Guidelines for compliance to

Quality requirements of eProcurement Systems

STQC Directorate
Department of Information Technology,
Ministry of Communications & Information Technology,
Electronics Niketan, 6 CGO Complex, Lodhi Road,
New Delhi – 110003

Dt: 05.08.2011

CONTENTS

1.0 Introduction

2.0 Operating Models of eProcurement System

3.0 Specific requirements of eProcurement System

4.0 Requirements of Conformity

5.0 Testing framework for Quality and Security Characteristics

6.0 Evaluation & Certification process

Annexures

Annexure-I : Risks of eProcurement Systems and related ISO 27001 controls
Annexure-II : Checklist for eSecurity Compliance (including CVC Guidelines)
Annexure-III : Checklist for compliance to GOI procurement procedures (GFR)
Annexure-IV : Checklist for legal compliance (IT Act – Amendment 2008)
Annexure-V : Definitions and Reference Documents

Reference documents:

1. eTendering Process
2. eTendering Glossary
3. eProcurement Integrity Matrix
4. OWASP (Open Web Application Security Project) Top10 Application Security Risks-2010
5. Business requirements specification- cross industry e-Tendering process (Source CWA 15666)

Forms & Templates:

Template I : Template for defining Usability Requirements Specifications of the Software product
Template II : Template for Performance Specification
Form I : Application form for applying for Testing to STQC

1.0 Introduction

1.1 Background

The public sector is one of the biggest purchasers of goods & services in the economy. The Government of India acknowledges that automating procurement process using electronic tools/techniques and enabling opportunities to suppliers fully supports the objective of non-discrimination, fair & open competition. eProcurement is identified as a mission mode project under national eGovernance plan. The objective is to transform public sector purchase activity from labor intensive paper based to efficient eProcurement process.

Electronic Procurement (eProcurement) is the use of Information and Communication Technology (specially the Internet) by the buyer (in this case Government) in conducting their procurement processes with supplier for the acquisition of goods (supplies), works and services. Use of Information Technology promotes the aims of open, non-discriminatory and efficient government procurement through transparent procedures.It is the technology-enabled acquisition of goods and services, required by an organisation, at the best value obtainable in the most efficient manner possible.

The factors driving the adoption of eProcurement are:

- Reduced purchasing cost and improved efficiency
- Standardized purchasing processes across the organization
- Reduced administrative costs with better effectiveness
- Significant reduction in the procurement cycle
- Reduced discretion

At the same time the inhibitors to adoption are:

- Lack of supplier readiness
- System integration issues (compatibility and interoperability)
- Confidence on the system (Security, Functionality and Performance)
- Insufficient skilled staff

eProcurement involves a set of technology solution which concentrate on different key areas of procurement such as

- e-Tendering,
- e-Auction or Reverse Auction,
- e-Catalogue/Purchasing,
- eMarket Place,
- e-Invocing etc.,.

The focus of the current Guidelines is mainly on e-Tendering, (i.e. tendering with encrypted bids, the equivalent of which in the manual context would be 'sealed bids').

This document provides the guideline for compliance to quality requirements of eProcurement systems. The essential quality characteristics of eProcurement system cover Security, Transparency & Functionality.

1.2 General Requirements of eProcurement System

The basic requirements of any eProcurement system are to achieve the goal of Government procurement, standardisation of procurement processes and information entities in an efficient and transparent way. Hence the key requirements are to:

- Address the requirement of GFR
  For public procurement of goods, services, works (e.g. construction) compliance with GFR rules, processes, roles (purchasing officer, local purchasing committee etc) are mandatory requirements. The GFR rules needs to be applied into the application workflow of e-tendering process. eProcurement System should be designed as per defined workflow with adequate security measures.

- Confidentiality and Integrity of Information
  The key requirement of procurement in public service organisation is to maintain the confidentiality & integrity of the information in procurement life cycle to protect the interest of buyer & supplier and to encourage the competitiveness in the business. The e-procurement platform transacts confidential procurement data and is exposed to several security threats. This requires employing a combination of security technologies and security best practices which result in reduced threat of data loss, leakage or manipulation.

- Address Vigilance Guidelines
  The system should meet the requirements of guidelines issued from time to time by Central Vigilance Commission.

- System Adaptability & customisation
  eTendering System need to have templates to offer flexibility in bidding methodologies as prevailing and followed currently in the manual process. Further, system should have templates to adopt bidding methodologies as may be prescribed by respective authorities.

The aim of this document is to provide guidelines that could be followed for designing/developing some critical functionality in an e-Procurement system as well as the necessary process for monitoring adherence to the security and transparency requirements of an e-procurement system during the implementation and post implementation by the e-procurement application developers, service providers and other stakeholders.

1.3 Objective

To provide Guidelines for assuring Quality and Security of an e-Procurement system so that confidence can be provided to its stakeholders that the system is secure, transparent, auditable & compliant with government procurement procedures.

1.4 Target Audience

- Purchase/ Head of Public Service Organization
- eProcurement Service Provider
- eProcurement Solution Provider/ Application Developer
- Third Party Testing and Audit Organization

1.5. Approach

To achieve the above objective the following approach is recommended.

- Evaluation of eProcurement System (including data, software, hardware, network, process) to ensure
  - Correct & complete implementation of organisation procurement policies & procedures
  - Compliance to GFR rules, CVC guidelines, IT Act (including amendments)
  - Assuring Security by Design & Development (ie some critical security and transparency related functionality has to be built into the e-procurement software application) , Implementation, Deployment & Use
  - Security of Data Storage and Communication
  - Performance
  - Usability
  - Interoperability
- Identification of risks and concerns of e-procurement system & providing the guidelines for mitigating the identified risks.

2.0 Operating Models of eProcurement System

There are four operating models for eProcurement **(Reference doc – 1)**

i) Dedicated e-Procurement System: the Government organization wishing to do e-Procurement, owns and controls the system infrastructure, and also controls all the procurement activities carried out.

ii) Outsourcing Model-1 (Partial Outsourcing – Managed Services): The Government organization procures and owns the system, which is managed by service provider with adequate security controls. There is a risk that service providers may get access to vendor data. Issues relating to Official Secrets Act shall be considered for this model.

iii) Outsourcing Model-2 (Partial Outsourcing – Infrastructure Support): The Government organization uses the eProcurement system of a Service Provider. The Service Provider also owns and controls the infrastructure. There is a risk that service providers may get access to vendor data & service provider start participating in core procurement process, Issues relating to Official Secrets Act shall be considered for this model.

iv) Outsourcing Model-3 (Full Outsourcing (ASP) Model): Multiple Government organizations can register and themselves use the ASP's portal for their various e-tendering/ e-auction activities with complete control of the all the 'core tendering activities' in their hands, without any intervention from the service provider. The registration/ deregistration activities, and the portal infrastructure is managed by the service provider with adequate security controls. In this case, essentially the Service Provider is only a platform-provider. The powers and responsibility of the tendering process remains in the hands of the duly authorized officers of the government organizations, and does not get transferred to third party service providers as in 'Outsourcing Model-2 (Full Outsourcing)'. So while there is some outsourcing in respect of infrastructure, there is no outsourcing of the actual tendering/ procurement activities by the concerned user-Government organizations.

All models of e-procurement system must incorporate functionality, processes and technologies outlined in (**Annexure I, II, III and IV**), and especially apply countermeasures to mitigate known risks (Annexure-I)

3.0 Specific requirement of eProcurement System

3.1 The service provider in consultation with the Purchase Officer shall establish the following process:

- Business Process Re-engineering switching from Manual Procurement to eProcurement. (Since Government tendering processes falls within a standard framework, only limited options should be given to the Purchase Officer. The service Provider/ Purchase Officer should not be able to reduce the essential security and transparency aspects of the system on the pretext of re-engineering and customization]).
- Implementation of Bid- Encryption at client-end (ie bidder's computer) using Symmetric Key, or Asymmetric Key (PKI-based) subject to issues raised in Annexure-I and II being suitably addressed
- Bids before transmission from the bidder's computer should be protected with SSL Encryption.
- Functionality/ Security/ Transparency related Requirements of a Manual Tendering System and Conformance its Availability in the Offered eProcurement system (functionality requirements of GFR & CVC guidelines)
- eProcurement System must have templates to offer flexibility in bidding methodology as prevailing and followed currently in the manner of processing. Further, the system should have templates to adopt bidding methodology as may be prescribed by the purchaser, as long as the methodology is a legally acceptable methodology.
- eProcurement System should deploy PKI based technologies for authenticating the bids, and opening electronic tender box. Secure methodology for decrypting bids should be deployed corresponding to the encryption methodology deployed (viz symmetric, or PKI-based asymmetric). The entire IT hardware infrastructure of E-Procurement System which includes application software, hardware, and system software be hardened as relevant. The system must deploy anti-spyware and anti-spam with a provision to update regularly. The updation of these software on the E-Procurement System be done using the offline updation mode. The E-Procurement System must have software tools to protect the operating system from injection of spyware. The entire infrastructure be protected and secured at the perimeter level by installing firewalls and Intrusion Prevention System. The system be configured properly so as to detect any kind of Intrusion into IT system.
- eProcurement System can be further secured by installing suitable security incident and event management mechanisms SIEM (Security Incident Event Management).
- eProcurement application should have audit trail facilities.
- The PKI Key Management System must specify the holder of private key and public key. The procedure in this case may be prescribed.
- eProcurement System should not provide read access to password to the Administrator. E-Procurement System further should not have forgot password feature which provides administrator-generated or system-generated temporary password.

3.2 The Purchase Officer of a Public Service Organisation (Government Department) must to ensure that e-Procurement system which he intends to use complies with all the applicable requirements listed in Sections 3 and 4.

3.3 The Purchase Officer must analyse the risk arising out of establishment of above mentioned processes and apply suitable controls. The annexure I,II,III and IV may be followed

3.4 Escrowing of Source Code

The source code of the e-procurement application software along with the modification/changes/patches which is implemented by the agency from time to time shall be escrowed with the agency nominated by the user organizations or government in case of dedicated portals.

An MOU would be entered between purchase officer/ purchase-organization and service provider

4.0 Requirements of Conformity

4.1 eProcurerement systems must address:

- E-procurement application should have provisions of ensuring validation of PKI signature through Certificate revocation list (CRL) and validity of certificate.
- Shall have mechanism for time synchronisation by using time synchronisation service (TSS) at hosting level, or synchronisation with master-server at the data-centre where the e-procurement system is hosted
- Time Stamping [facility should be there in the e-procurement application for time-stamping of all important events like – creation of tender notice, approval of tender notice/ tender documents, submission of bids and supplementary bids (like modification, substitution, alternatives), etc]
- The system must confirm to GFR rules, processes, roles (purchasing officer, local purchasing committee etc.), compliance to CVC guidelines and IT Act (including amendments).

4.2 Other Requirements for Quality and Security Evaluation

:

The following conditions shall be agreed in writing by service provider

- For Dedicated portal and ASP-Model, the e-procurement application should have facility for generating audit-logs, which should be accessible (in downloadable form) to a specially designated officer of the Purchase organization. For Outsourcing Models 1 and 3, e-procurement service provider shall submit all the logs of transaction created by the e-procurement solution including forensic image on quarterly basis or as prescribed by the user organization regularly and as and when demanded by the purchasers. The logs will be duly signed by the administration of the service provider by his electronic signature.
- The audit for certification of the entire e-procurement solution shall be undertaken after its deployment and prior to its usage.
- The e-procurement solution including the computer server shall be installed in India. No data as captured/stored in the e-procurement solution will be taken out of the country. The intent of this clause is to cover the data centre and the routing. Additionally, the foreign bidders should be able to quote.

- The audit of the ‘ complete e-procurement system’ shall be undertaken only on the request of the organization/agency who wish to use/install the system. Software application can be tested based on the request of the developer.
- The e-procurement solution shall need to be tested and audited again after it has been significantly modified (addition/ deletion of functions/ modules) or customized for a new organization whether stand alone or shared mode
- The traffic emanating to and from eProcurement systems will be scanned if required by the authorised body.

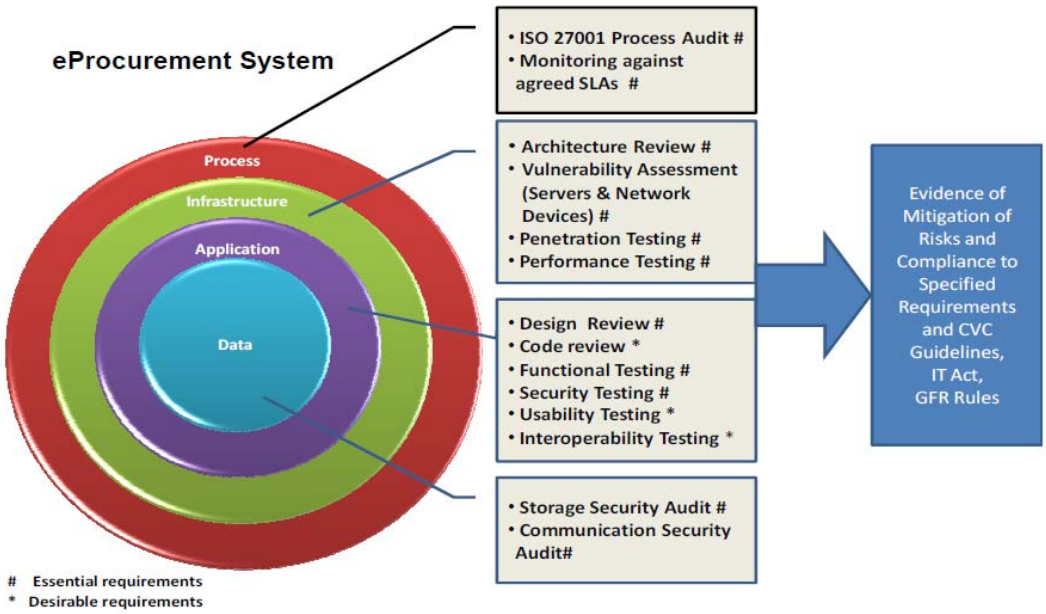
Storage of Electronic Invoices

- It is assumed that invoices transmitted electronically will be stored electronically. If public service organisation wish to store invoice in the paper form same shall be provisioned in local purchase procedure approved from competent authority
- For VAT purpose records must be retained for 6 years. 6 Years rule may cause serious storage problem or undue expense; competent authority may take a suitable decision for the retention period.
- The records may be stored anywhere State Data Centre/PSU own data center. The only requirement is that of security, strategic control and record must be made available to public service organisation on demand within a reasonable period.

5.0 Testing framework for Quality and Security Characteristics

5.1 eProcurement Quality and Security Assurance Model

A eProcurement Quality and Security Assurance Model is depicted below:



The Quality & Security evaluation model consist of four layers namely, Data, Application, Infrastructure and Process. Layer by layer assessment will ensure compliance with applicable requirements such as CVC, IT Act, GFR 2005 and concerns of other stakeholders.

5.2 Description of the model

Brief description of the layers (from outermost to inner) is given below.

- **Process-Layer**
  ISO 27001 Process Audit #
  Verification of the IT security processes to ensure that secure and best practices are followed in operation and maintenance of the e-Procurement System in line with international standard on Information Security Management System, ISO 27001/27002

  To supplement the functionality built into the e-procurement system, where some requirements of the e-procurement system and allied processes are being addressed through organizational procedures under ISO 27001/ 27002, these should be explicitly defined with satisfactory explanations. At the time of certification/ audit, such procedures as outlined by the e-procurement vendor / service provider in response to Annexure-I , II, III of these Guidelines, shall be reviewed and evaluated.

  Monitoring against agreed SLAs #
  SLA monitoring shall ensure that the e-procurement system is adhering to the agreed upon service related (i.e., user centric) as well as system related (i.e.,

technology centric) service quality requirements such as availability, performance, problem resolution, etc. While service related SLAs take care of the services delivery issues, the system related SLAs address IT technology (hardware, software and network) used in delivering the services.

- **Infrastructure Layer**

Architecture Review #

The review of e-procurement system shall be done to ensure that the defined architecture of the e-procurement system is adequate and suitable for meeting the various operational and service delivery requirements such as performance, security, availability, etc.

It is also recommended that once the e-procurement system is deployed, the deployed architecture should be audited to verify its compliance against the defined architecture. The audit should cover logical positioning of various system components such as firewall, IDS/IPS, servers, load balancer, etc. In addition, end-to-end transaction flows should be verified to ensure that they are going through the defined path by using dummy test transactions and analysis of logs at various layers. Certification body shall use standardized checklist for the criteria.

Vulnerability Assessment (Servers & Network Devices) #

System configuration checking or verification of hardening and vulnerability scanning shall be performed to find out weaknesses, vulnerabilities and mis-configuration in the target hosts (Servers, Routers, Firewalls, Switches etc.) which hosts the e-procurement application system. Certification body shall use standardized checklist for the criteria.

Penetration Testing of the System #

Penetration Testing (PT) shall be normally done remotely from public domain (Internet) and also can be done from internal network to find out exploitable vulnerabilities. Series of testing conducted like information gathering from public domain, port scanning, system fingerprinting, service probing, vulnerability scanning, manual testing, password cracking etc. using state-of-the-art tools (commercial and open source) and other techniques shall be used with the objective of unearthing vulnerabilities and weaknesses of the overall e-procurement system and its underlying IT infrastructure. Certification body shall use standardized checklist for the criteria.

Performance Testing of the System #

Performance testing of the e-procurement system shall be done to ensure that system is capable of handling defined user as well as transactional load. The performance testing of the e-procurement system essentially means measuring the response time of the system for defined scenarios. While measuring the response time it is important to record the resource (CPU, Memory, etc.) utilization. The capacity of the e-procurement system should be checked by systematically increasing the load on the system till performance degradation or system crash is encountered. Also the manner/ trend in which performance changes with load will determine the scalability of the e-procurement system.

- **Application Layer**

Application Design Review #

(Note: This would be applicable only where 'customized software development' is being done for a specific organization. Furthermore, it should be noted that this review would not be a substitute for the review and testing of critical security and functionality outlined in Annexures I, II and III of these Guidelines)

Design review covers the high level design and the low level (detailed) design of the e-procurement software application. It will ensure that software has been designed using best practices and design rules. The review will verify that the design has modularity, flexibility, low complexity, structural fan-in & fan-out and it is loosely coupled & highly cohesive. The correctness of logics and algorithms used in the detailed design should be verified including any zero day vulnerability in the algorithm.

Application Code review *

(Note: This would be applicable only where 'customized software development' is being done for a specific organization. Furthermore, it should be noted that this review would not be a substitute for the review and testing of critical security and functionality outlined in Annexures I, II and III of these Guidelines)

The code review (i.e., static analysis) of the software application source code shall be carried out using tool and measure metrics such as lines of Code, Code Complexity, Fan-in & fan-out, Application Call Graph, Dead Codes, Rule Violation, Memory leaks etc. It is also recommended to perform walk through of the source code with code developer to verify the logics and algorithms used for correctness and optimization.

Special focus should be given to identify any unwanted functions (not required by the e-procurement software application), as these 'not to have functionalities' can be potential security threats.

Application Functional Testing #

The functional testing of the e-procurement software application shall be carried out to validate the application meets the specified functional requirements covering the work flows, navigations, and business & data Validation rules for the defined user categories with access rights. The functional testing should be done following black box approach and using end-to-end user scenarios.

(Note: Detailed scenarios would be prepared for each application software to be tested. This would include all important steps and scenarios of Government Tendering , as well as, 'all issues' outlined in Annexures I, II and III of these Guidelines)

Application Security Testing #

The test is conducted to unearth various application security vulnerabilities, weaknesses and concerns related to Data /Input Validation, Authentication, Authorization /Access Control, Session Management, Error Handling, Use of Cryptography, etc. Typical issues which may be discovered in an application security testing include Cross-site scripting, Broken ACLs/Weak passwords, Weak session management, Buffer overflows, Forceful browsing, Form/hidden field manipulation, Command injection, SQL injection, Cookie poisoning, Insecure use of cryptography,,

Mis-configurations, Well-known platform vulnerabilities, Errors triggering sensitive information leak etc. OWASP (Open Web Application Security Project) guidelines are used for the testing.

(Note: Detailed scenarios would be prepared for each application software to be tested. This would tests to cover 'all' security related issues outlined in Annexures I, II and III of these Guidelines, especially aspects related to bid-encryption. In addition, standard security tests, viz – Cert-In, OWASP, FBI Top 20 (any other?) will be conducted)

Application Usability Testing *

Usability testing usually involves systematic observation under controlled conditions to determine how well people can use the product. e-procurement system is used by users of different levels of computer knowledge. User expectation varies with different types of user. Usability testing will ensure that the all types of users are comfortable to use the system. This shall be done by using defined international standards which recommend extensive user interaction and analysis of user behaviour for a defined task.

Application Interoperability and Compatibility Testing *

Interoperability Testing shall be done to check if the software can co-exist and interchange data with other supporting software in the system. Compatibility testing shall check if the software runs on different types of operating systems and other hardware/software/interface according to customer requirements

- **Data Layer**

Data Storage Security Audit #

This is done to ensure the use of standard and strong cryptography while storing the sensitive data and user credentials in the application or associated data base. It is also verified that the cryptography used is compliant with the Information Technology Act (ITACE) and the CVC guidelines

Data Communication Security Audit#

This is done to ensure that secure communication channel like SSL, TLS or equivalent is used for transmission of sensitive data and credentials by the e-procurement system. The cryptographic algorithms and the key size implemented by the system should be standard, strong and compliant with the IT ACT and the CVC guidelines.

It is recommended that the complete data transmission to and from the e-procurement website should be SSL/ TLS enabled.

6.0 Evaluation and Certification Process

6.1 The applicant shall submit the request to Testing and auditing agency (like STQC) to get eProcurement System assessed. The application should specify whether testing is required 'only for the e-procurement application', or for 'the complete e-procurement system, viz the application along with the server in a specific hosting environment'. Application for the former case can be made by the application software developer or licensor, and will cover only Part-1 of the two scenarios outlined below. The application for the latter case can be made by the service-

provider, or the organization which is procuring the system for its dedicated use, and will cover both Part-1 and 2 of the two scenarios outlined below.

6.2 Inputs & access required by Certification Body

[Scenario-A: Where 'Customized Software Development' of an e-Procurement System is undertaken]

(Part-1)

- Inputs required for Application Testing
  - RFP of the e-Procurement
  - Software Requirements Specification (SRS) addressing functional and non-functional requirements including business functions and applicable regulations, standards and policies.
  - User manual (operational instructions).
  - Software application related information such as – Work flows/ Navigations, Business logics/ Rules, Validation Rules, Screen shots and User categories with roles & access rights. Specifically for testing, application related information such as – Work flows/ Navigations for creating comprehensive 'System Test Cases' covering various tendering scenarios, User categories with roles & access rights would be required.
  - Software Design Document
  - Software Application Source Code (if the need is to assess to all desirable requirements)

The inputs should be available along with access to the application hosted in a staging environment with test data.

Note: Apart from review of the 'developmental aspects', detailed scenarios would be prepared for each application software to be tested. This would cover 'all' security related issues outlined in Annexures I, II and III of these Guidelines, especially aspects related to bid-encryption.

(Part-2)

- System Architecture
- Security Architecture for conducting VA&P
- ISMS of eProcurement Information System (eSecurity Manual)
- Access to e-procurement system/ test site with sample data (preferably field data).
- Access to hardware, software, Network & IT infrastructure to connect test tools on to the system, where required.

Non-disclosure Agreement (NDA) will be signed by STQC to cover the confidentiality of the information submitted by the applicant

[**Scenario-B: Where 'Ready-to-Use' e-Procurement Software License is to provided, or e-Procurement Services are made available through an ASP**]

Note: The focus Testing/ Certification here is on the 'Functionality'', 'Security' and 'Transparency' related aspects.

(Part-1)

- User Manual (operational instructions), or equivalent Guidelines for users provided online on the screens of the application
- Software application related information such as – Work flows/ Navigations for creating comprehensive 'System Test Cases' covering various tendering scenarios, User categories with roles & access rights.

The inputs should be available along with access to the application hosted in a staging environment with test data

Note: Detailed scenarios would be prepared for each application software to be tested. This would tests to cover 'all' security related issues outlined in Annexures I, II and III of these Guidelines, especially aspects related to bid-encryption.

(Part-2)

- System Architecture
- Security Architecture for conducting VA&PT
- Access to e-procurement system/ test site with sample data (preferably field data).
- Access to hardware, software, Network & IT infrastructure to connect test tools on to the system, where required.

Non-disclosure Agreement (NDA) will be signed by STQC to cover the confidentiality of the information submitted by the applicant.

6.3 Requirements of Compliance for demonstration

Testing and assessment as specified in Section 4.0 shall be carried out.

To demonstrate conformity to the **ESSENTIAL** Quality and eSecurity assurance requirements and minimum functionality compliance the following shall be complied:

- Evidence of compliance to implementation of ISO 27001 Information Security Management System with applicable controls in all concerned entities. The Security processes shall be audited as per controls defined in eSecurity Manual provided by the applicant, and/ or in the applicant's response to Annexure I, II, III, and IV.
- The risk analysis methodology used by the service provider shall adequately address the concerns raised in this document (**Annexure-I**). Mitigation methodology and techniques implemented should ensure eProcurement Information System is secure.
- While implementing the security controls the service provider shall demonstrate that the requirements of vigilance administration (CVC) **(Annexure-II)** are adequately addressed in the Information Security Management System. Also while implementing ISO 27001, the solution provider shall ensure that adequate controls have been implemented to ensure that security at design and operation level are addressed adequately
- The software shall be tested for functionality, workflow and other essential requirements **(like CVC Guidelines, GFR, IT Act – Annexure I, II, III, and IV).**
- The application hardening shall be assessed for Top 10 vulnerabilities defined by OWASP **(Reference doc – 3)**
- Network should be assessed for adequate security through penetration testing and vulnerability assessment as per **NIST 800-115**.To demonstrate that the

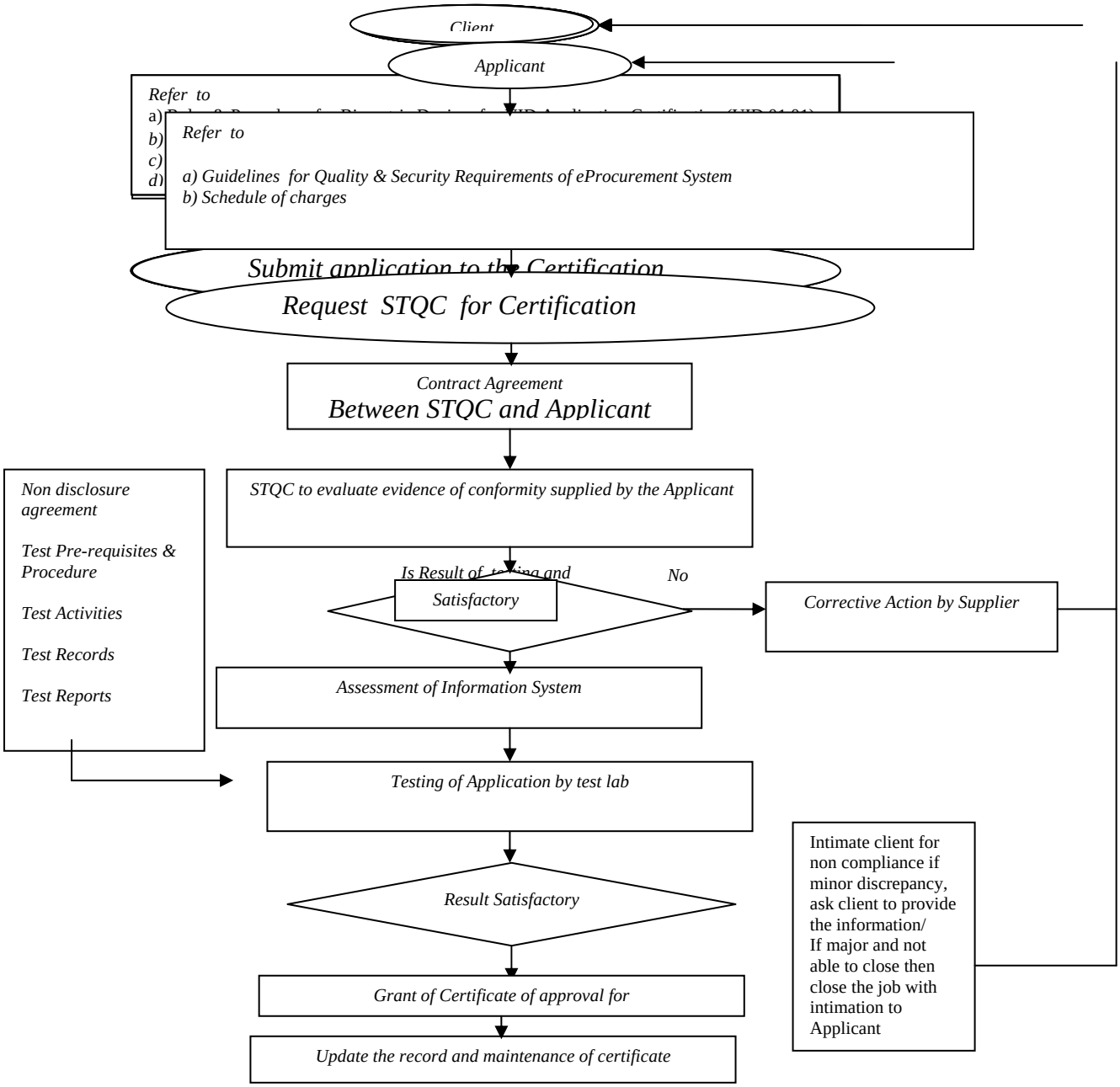
requirements are implemented and effective, the services of agencies empanelled by CERT-IN can be used (http://www.cert-in.org.in).

To demonstrate compliance to the **DESIRABLE** requirements following shall be complied, where applicable:

- The software source code shall be evaluated using white box test approach through code review/ inspection process for identifying malicious codes/ Trojan etc.
- Workflow shall be in line with the requirement of **CWA 15666** to standardized Business Processes and Information Entities using UML Version 1.4 and ebXML Core Components Technical Specification for Data Structure **(Reference doc - 4).** This will attain the objective of Interoperability and Compatibility of various solutions both at buyer and supplier end
- The solution shall be tested to Usability requirements as per Usability information defined in **Template I.**

6.4 If results are satisfactory and meet the requirements of this document, STQC shall issue a letter indicating Conformity with specified requirements.

Certification Process Flow Chart



Scope of Certification

eProcurement life cycle consist of following activities:

- Purchase to pay
    - Contract management
    - Content management
    - Selection/requisition
    - Workflow-approval
    - order
    - receive
    - invoice
    - payment
- eSourcing
    - management information
    - collaboration
    - specification/notice
    - expression of interest
    - invitation to tender
    - evaluate
    - negotiate/reverse auction
    - award

Generally, these activities are covered in different modules e.g.

- Supplier Registration
- E-tedenring
- eAuction
- ePayment
- Accounting
- Reverse Auction
- eCatalogue Management
- MIS
- Contract Management

The applicant can define any module as a part of scope of certification while the eTendering module is the essential requirement to obtain the certification. Depending on the complexity of the module and the scope identified by the applicant the Certification Body/Test Agency will charge for testing and certification.

Annexure-I - Risks of eProcurement Systems and related ISO 27001 controls

Sl. No.	Risks / Concerns	Control Identification	ISO 27001 Control Reference
1. Concerns related with Electronic vs. Manual Procurement			
1.1	While implementing eProcurement system the solution provider may do business process re-engineering to make the system efficient and effective. There is a risk of compromising basic principles of public procurement	Identification of applicable legislation compliance	A 15.1.1 "All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization".
	Guidance and recommended practices The underlying principle of e-tendering and manual tendering process should be same in respect of guidelines of CVC, GFR, Legal and transparency related requirements. While doing reengineering these requirements shall not be negotiated and compromised. Since section A15.1.1 of ISO 27001 demands **explicit definition** of the requirements, Annexures I, II, III of these Guidelines should be treated as a 'Checklist' for this purpose:		
1.2	Incorporation of multiple bidding methodologies in eProcurement solutions as provisioned in Manual Procurement System and the flexibility in the solution to the extent required	Identification of applicable legislation compliance	A 15.1.1 "All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization".
	Guidance and recommended practices- e Procurement System Depending upon the requirements of a tender any one of the multiple bidding methodologies as outlined below shall be provisioned in the application: • Single-stage, single- envelope • Single-stage, two- envelope • Two stage (with facility for 'technical conformance', and if required, 'revised tender documents') • Two-stage, two- envelope and requirement of Pre-qualification stage when required submission of one or more Alternative bids as applicable. • Each bid part (eg technical, financial) may be required to be submitted in a 'summary format' along with a 'detailed bid'. The latter could be a large file. There should be provision of appropriate file size (at least 10 MB) in the application with data encryption as outlined elsewhere in these Guidelines. • After having submitted the 'original' bid for each bid-part, a bidder has a right to submit: – 'Modification' bid		

	– 'Substitution' bid Or 'Withdrawal' bid for all his bid-submissions. The e-tendering system must effectively cater to all these possibilities without compromising security and transparency in any manner at any stage, for any bid part (such as Pre-qualification, Technical, and Financial). The e-tendering system need to have templates to offer flexibility in bidding methodologies as prevailing and followed currently in the manual process. Further, system should have templates to adopt bidding methodologies as may be prescribed by respective authorities.		
2.0 Concerns relating to Implementation of e-procurement systems using PKI based Bid-Encryption			
2.1	A system in which Public Key of a Tender-Opening Officer or of any other officer of the purchase department, or of any person from the service provider's organization is used for bid-encryption, and corresponding Private-Key used for Decryption Many time bids are encrypted at the bidder's computer with public-key as mentioned above, and the encrypted bids, with additional SSL encryption, reach the e-tendering server through file-upload and/ or filling of online-forms. There are risks related to integrity of persons in (a) purchase (buyer) organization & (b) e-Tendering Service Providers organization. As Typical implementation practices include • Private Key with which decryption is done, is available with the concerned officer before the Public Tender Opening Event • Public Key with which bid-encryption is done is available publicly. • Public Key algorithms are slow. • Copy of the decryption-key (ie private key of the encryption-certificate issued by a CA) is generally available (ie backed up) with the CA. Duplicate can generally be requested in case of loss, however, this can also be misused.	Cryptographic controls Regulation of cryptographic controls	A 12.3 *Objective:* To protect the confidentiality, authenticity or integrity of information by cryptographic means. A.12.3.1 : "A policy on the use of cryptographic controls for protection of information shall be developed and implemented". A.12.3.2 : "Key management shall be in place to support the organization's use of cryptographic techniques". A 15.1.6 "Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations".
	<u>Guidance and recommended practices- Use of PKI technique</u> If the e-procurement system uses PKI for bid-encryption, it has to satisfactorily address the above issues and consequent concerns (Ref 2.2 below) <u>through suitable functionality built into the e-procurement application</u>. Where, in addition, some issues are being further addressed through organizational procedures under ISO 27001, these should be explicitly defined with satisfactory explanations, otherwise certification process will become subjective. While doing this, the following can be kept in view:		

	Various techniques are available in market for improving implementation of PKI based encryption such as escrowing, splitting and repeated encryption to further strengthening the security of information and implementation. If the e-procurement system uses any of the above techniques, it will have to be explained how the related concerns (Ref 2.2 below) have been addressed. Furthermore, practical procedures will have to be put in place which can be implemented at the field level in diverse locations in the country in a user friendly manner.		
2.2	(i) While all efforts must be made to ensure that no spyware is put in the server which can make clandestine copies of a file or data being uploaded to the server, and then sending this clandestine copy to a secret destination, the possibility of such spyware being planted in the web-server cannot be totally ruled out. This undesirable eventuality could occur due to connivance of the administrators of the Service Provider, or even through remote injection. For secure & transparent functioning of the e-tendering system, it cannot be assumed that there will never be such a possibility of the spyware being planted in the e-tendering server. (ii) If the spyware is planted at the kernel level, there may not be any audit trail. (iii) Audit Trails (both application level, and Operating system level) are essentially reports. To that extent it is possible to fudge these. Also, other than application-level audit trail reports, the other audit trail reports can be quite complex and impractical to analyze for ongoing operations of this nature. In spite of this, audit trail-reports are useful and should be there as supporting evidence. However, in a sensitive application of this nature, audit trails cannot be depended upon as the sole protection against any mala-fide act.	Control of technical vulnerabilities Protection against malicious and mobile code OS Access Control Log monitoring	A 12.6.1 "Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk". A 10.4 A.10.4.1 "Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented". A.10.4.2 "Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing". A 11.5 A.11.5.1 Access to operating systems shall be controlled by a secure log-on procedure. A.11.5.2 All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to

			substantiate the claimed identity of a user. A.11.5.3 Systems for managing passwords shall be interactive and shall ensure quality passwords. A.11.5.4 The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. A.11.5.5 Inactive sessions shall shut down after a defined period of inactivity. A.11.5.6 Restrictions on connection times shall be used to provide additional security for high-risk applications. A10.10 A.10.10.1 Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. A.10.10.2 Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly. A.10.10.3 Logging facilities and log information shall be protected against tampering and unauthorized access. A.10.10.4 System administrator and system operator activities shall be logged. A.10.10.5 Faults shall be logged, analyzed, and appropriate action taken.

			A.10.10.6 The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source
	Guidance and recommended practices- Spyware/Trojan/BOTS It is important that even if a clandestine copy is made and stolen as above, the bid-encryption methodology should be such that it should not be possible to decrypt the bids in connivance with any officer of the Buyer organization or the Service Provider organization. While this issue becomes irrelevant if bid encryption is done at bidder-end with bidder created symmetric pass-phrase, in case PKI-based bid encryption is done, the software functionality has to be suitably augmented to mitigate this security threat. This threat has also been explicitly mentioned in CVC guidelines (refer security check-point No. 14 of Annexure-II) a) The controls should be placed to guard against the possibility of injecting spyware for making clandestine copies of a submitted bid and then sending this clandestine copy to a secret destination. The spyware are the malicious software codes which can be injected in to the system remotely. To protect the system from injection of spyware, the system needs to be secured. The system need to be secured and protected in the following manner; • Hardening of hardware and software of the entire Information Technology infrastructure (which include computer system, software, router etc.) • Installation of anti spyware, anti spam and antivirus software. • Installation of software tools to protect the operating system from injection of spyware. These software need to be upgraded on a continuous basis. The entire infrastructure needs to be secured at the perimeter level by installing Firewalls and intrusion Prevention System. After installation of software and protecting by devices as the entire IT infrastructure needs to be audited by the Information Technology Auditors. Indian Computer Emergency Response Team (CERT-IN), Department of Information Technology has empanelled auditors for auditing systems from the point of view of cyber security. It is always recommended that system should be audited at least once in a year and as and when the infrastructure (i.e hardware and software) is augmented by additions of new hardware and software. Further people operating these systems need to be trained in monitoring and detecting any intrusion in the system and network. b) The kernel of the operating system in the IT infrastructure should be secured first by hardening the operating system and installation of software which protects it from inject of spyware or any kind of intrusion. c) The e-procurement system should have audit trail facilities. These audit trails are complex but dependable. The audit trails reports provide useful information about the instructions which take place in the system both at operating system and		

	application software. This information is necessary to analyze nature of intrusion, vulnerabilities exploited and to track the perpetrators. It also helps in taking steps in preventing future intrusion. The analysis of audit trail requires appropriate expertise both in respect of application and operating system. Such expertise is available in the country at many places. CERT-In also facilitates the user organization in analyzing the audit trails.		
2.3	Private Key with which decryption is done, is available with the concerned officer before the Public Tender Opening Event a) If a clandestine copy of a bid is made as described above before the 'tender opening event (TOE)', and if the concerned tender-opening officer (TOE-officer) connives in decrypting the bid before the TOE, the confidentiality of the bid is compromised. b) The above concern with the difference that the copy of the bid is made with the connivance of the Database Administrator (DBA). c) If the concerned TOE-officer(s) is/ are absent during the TOE, how the bids will be decrypted especially keeping in view that the private-keys should not be handed over to anybody else.	Cryptographic controls Segregation of duties	A 12.3 A.12.3.1 "A policy on the use of cryptographic controls for protection of information shall be developed and implemented." A.12.3.2 "Key management shall be in place to support the organization's use of cryptographic techniques" A 10.1.3 "Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets."
	<u>Guidance and recommended practices</u> Note: While some guidance is provided below, it is the responsibility of the individual vendors to design and develop their applications in a manner that addresses the outlined concerns. They should first convincingly demonstrate the full methodology to DIT, and then DIT will transparently put this methodology on its website, so that bidders who use such e-procurement systems in future are fully assured against breach of confidentiality of their bid-data. A process needs to be established and followed in respect of key management of encryption keys particularly the key with which the bid would be decrypted at the time of opening of the bids. Such process should avoid compromising confidentiality and possibility of decrypting clandestine copy of the bid. In this regard the following three approaches may be adopted with proper checks while keeping in view the legality of the process for end-users. Furthermore, practical procedures will have to be put in place which can be implemented at the field level in diverse locations in the country in a user friendly manner. • Splitting of Keys: A bidder would submit the bid document after encrypting it with the public key of the tendering organization, so that the contents are encrypted and are decrypted by the authorized officials at the tendering organization. To minimize the risks associated with "person of dubious integrity" or collusion, private key decryption should be split into `M' parts with the requirement of minimum `N'		

	splits being required for its use. (`N' should be more than 1 and less than or equal to M). `N' and `M' will be decided by the tendering organization and suitably configured on the system. • Multiple encryption of the bid document with multiple public keys and decryption of document with the multiple corresponding private keys of the tendering organization. Application of multiple encryption of the bid document could be prescribed in a predefined order by authorized officials of the tendering organization. Decryption will have to be carried out in the reverse order. The multiple decryption keys (i.e. private) may be held by different officials of the tender organization. Encrypting the bid document first with public key of the bidder and then by the public key of tendering organization. The bid document may then be decrypted by the private key of the authorized official of tendering organization and then by the private key of bidder. It may be noted that the decryption keys are applied in reverse order in application of encryption keys. The implementation of this system, however, would require physical presence of the bidder who encrypted the bid at the time of submission of bid. Preferably the person of bidding organization should be same who has signed the bid by digital signature. There are logistic issues with this approach.		
2.4	Public Key with which bid-encryption is done is available publicly. The easy availability of the public key makes the data encrypted with it vulnerable to 'Chosen Plaintext Attack'	Cryptographic controls Regulation of cryptographic controls	A 12.3 A.12.3.1 A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A.12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques A 15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
	<u>Guidance and recommended practices</u> Note: While some guidance is provided below, it is the responsibility of the individual vendors to design and develop their applications in a manner that addresses the outlined concerns. They should first convincingly demonstrate the full methodology to DIT, and then DIT will transparently put this methodology on its website, so that bidders who use such e-procurement systems in future are fully assured against breach of confidentiality of their bid-data.		
2.5	Public Key algorithms are slow. As a result many e-tendering systems which use PKI for bid-encryption, use mainly an encrypted online-form for bid submission, and do not have facility for an encrypted detailed bid (eg detailed technical bid as a file), along with the online form. As a result, the detailed bid is either not submitted, or it is submitted in	Capacity management	A 10.3.1 The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

	unencrypted form.		
	<u>Guidance and recommended practices</u> Note: While some guidance is provided below, it is the responsibility of the individual vendors to design and develop their applications in a manner that addresses the outlined concerns. They should first convincingly demonstrate the full methodology to DIT, and then DIT will transparently put this methodology on its website, so that bidders who use such e-procurement systems in future are fully assured against breach of confidentiality of their bid-data.		
2.6	A system in which Public Key of a bidder's representative is used for bid-encryption at bidder's office, and where decryption will be done by the bidder's representative himself using his private key during the Online Public TOE. <u>Concerns</u>: **a)** Concerns outlined in 2.4 and 2.5 outlined above are applicable here also, and should be suitably addressed. **b)** How would the bids be opened if the bidder's representative with whose key bids have been encrypted is not available during the Online Public TOE ? The non-availability could be due to leave, termination or any other reason. **c)** Copy of the decryption-key (ie private key of the encryption-certificate issued by a CA) is generally available (ie backed up) with the CA. Duplicate can generally be requested in case of loss, however, this can also be misused. <u>Note</u>: Private key cannot be transmitted by the bidder over the internet. Furthermore, during the Online Public TOE, bids cannot be allowed to be downloaded from the server to the bidder's computer. This would tantamount to the bids being taken away from the tender-box back to the bidder's office for opening. This cannot be allowed. Therefore the bidder will have to be physically present during the Public TOE, and such a system will never be able to have a proper Online Public TOE. This would immediately remove one of the biggest benefits of e-procurement. Assuming that all other concerns are satisfactorily addressed, this would at best be a PARTIAL e-procurement system.		
3. Concerns relating to situations where bids before being transmitted from the bidder's			

computer are protected with only SSL Encryption and Database level Encryption is done before the bid is stored in the Database Server			
3.1	i) For secure and transparent functioning of the e-tendering system, it cannot be assumed that there will never be any "persons of dubious integrity" in the Purchase organization ii) For secure and transparent functioning of the e-tendering system, it cannot be assumed that there will never be any "persons of dubious integrity" in the e-tendering Service Provider's organization iii) While all efforts must be made to ensure that no spyware is put in the server which can make clandestine copies of a file or data being uploaded to the server, and then sending this clandestine copy to a secret destination, the possibility of such spyware being planted in the web-server cannot be totally ruled out. This undesirable eventuality could occur due to connivance of the administrators of the Service Provider, or even through remote injection. For secure and transparent functioning of the e-tendering system, it cannot be assumed that there will never be such a possibility of the spyware being planted in the e-tendering server. iv) If the spyware is planted at the kernel level, there may not be any audit trail. v) Audit Trails (both application level and Operating system level) are essentially reports. To that extent it is possible to fudge these. Also, other than application- level audit trail reports, the other audit trail reports can be quite complex and impractical to analyze for ongoing operations of this nature. In spite of this, audit trail-reports are useful and should be there as supporting evidence. However, in a sensitive application of this nature, audit trails cannot be depended upon as the sole protection against any malafide act.	Cryptographic controls Regulation of cryptographic controls	A 12.3 A.12.3.1 A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A.12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques A 15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
	<u>Guidance and recommended practices</u> Secure submission of bid from bidder's computer to the server should be done after the bid file/ data is encrypted (with symmetric or asymmetric encryption) at the bidder's computer and further submitted to the e-procurement server through SSL encryption. Only the encrypted file submitted by the bidder should be stored and should be decrypted at the Tender Opening Event (TOE).		
3.2	Assuming that 'only SSL encryption' is applied to a bid while it is being transmitted from the bidder's computer to the server, it is a fact the	Cryptographic controls	A 12.3 A.12.3.1 A policy on the use of

	role of SSL encryption is limited to the transmission phase (ie transportation to the server), and that on reaching the server the SSL encryption is removed. The bid is now presumably encrypted again with PKI or Symmetric Key. Albeit small, there is an 'interim period' before the bid is encrypted again. In the interim period the bid is actually in an unencrypted state and to that extent vulnerable. Irrespective of whether PKI or Symmetric Key is used for encryption at Database-level, the encrypting key is available/ accessible to some officer of the purchase organization, or an administrator of the e-tendering Service Provider, or the DBA. The above issues exist irrespective of whether only select data is encrypted, or the entire database is encrypted. If a clandestine copy of a bid is made as described above in the interim period which would be before the 'tender opening event (TOE)', and if the administrator connives, the confidentiality of the bid is compromised. 1b. The above concern with the difference that the copy of the bid is made with the connivance of the Database Administrator (DBA) and decryption done in connivance with the person holding the decryption key.	Regulation of cryptographic controls	cryptographic controls for protection of information shall be developed and implemented. A.12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques A 15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
	<u>Guidance and recommended practices</u> Secure submission of bid from bidder's computer to the server should be done after the bid file is encrypted (with symmetric or asymmetric encryption) at the bidder's computer and further submitted to the e-procurement server through SSL encryption. Only the encrypted file submitted by the bidder should be stored and should be decrypted at the Tender Opening Event (TOE). The two-way process as suggested may be followed strictly. This will address the concerns raised. The information on reaching the server where e-procurement software is deployed through SSL mode will remain encrypted even after the SSL encryption is removed. Information will lie encrypted in the system hosting e-procurement software. Data Base Administrator (DBA) will not be able to decrypt the information as he will not be having the decryption keys. It may be mentioned here that at no point of time the System Administrator or Data Base Administrator should be authorized to hold the private (decryption) key. The organization shall have a procedure which can include three different approaches to address three different scenarios.		
4. Concern about Symmetric key based Bid-Encryption done at the Bidder's computer			
4.1	a) While bidders' representatives should be welcome during Online Public TOE, it should	Cryptographic controls	A 12.3 A.12.3.1

	not be mandatory for them to be present if their bids are to be opened. b) How the security of the symmetric key (i.e. the key used for encryption of each bid-part) is ensured, between the period of bid-submission and the Online Public TOE, keeping in view the concerns outlined above. c) It should be allowed for a bidder to have different keys for bid-encryption of each bid-part (such as Pre-qualification, Technical, and Financial) he submits.	Regulation of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A.12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques A 15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
	<u>Guidance and recommended practices</u> The organization shall have procedure to address above. E-Procurement system should have functionality such that the physical presence of bidders should not be mandatory during Online Public TOE.		
5. Concerns/ clarifications based on s42(1) of the IT Act 2000 relating to Digital Signatures, a User Organization's Administrative Hierarchy, and some related aspects			
5.1	In any large Government or PSU Purchase organization, there can be multiple indenting departments, multiple tendering authorities (ie entities which can invite tenders in their name), and tens (and sometimes hundreds) of officers involved with different activities relating to various tenders. A situation should not arise in the e-tendering system where due to limitation of the e-tendering system, these departments and officers are not able to themselves execute their duly assigned roles as in the manual process, and are constrained to re-assign/ abdicate their roles and responsibilities to a few tech-savvy technicians or the personnel of the service-provider of the e-tendering system. The concern<u>s</u> in this regard are : a) No such limitations exist in the offered e-tendering system, and the system supports multiple departments and a comprehensive hierarchy of officers which is such that each officer can continue to perform his/ her tendering related role in a secure manner with full accountability, and with no need for any re-assigning of responsibilities. It is being clarified that the objective here is not to provide a full-	Cryptographic controls Regulation of cryptographic controls	A 12.3 A.12.3.1 A policy on the use of cryptographic controls for protection of Information shall be developed and implemented. A.12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques A 15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

	fledged virtual office to the officers, but to provide adequate facilities within the application for multiple officers of multiple departments to carry out their respective tendering related activities with proper security and full accountability. Roles relating to various tendering activities within each department, and which could vary from tender to tender, would inter alia include – deciding methodology and rules pertaining to a particular tender, creation of tender notice, approval/ rejection of tender notice, creation of corrigendum, approval of corrigendum, creation tender document forms, approval of tender document forms, overall approval/ rejection of tender documents, providing responses to clarification of tender documents, uploading minutes of pre-bid meeting, one or more officers conducting public online tender opening event (TOE), approving minutes of the public online TOE, short-listing responsive bidders for the next stage (where applicable), managing roles of various personnel, and assigning alternative personnel in case the original assignees are absent, etc. b) The offered e-tendering system has facility, such that roles with conflict of interest can be offered to different persons within the organization, so that conflict of interest is avoided. c) There should be one authorized person as an overall coordinator and representative of that organization in the e-tendering system, with powers to delegate different roles to different users from time to time, and all such role-changes must be audit-trailed in the application. The credentials of this overall coordinator must be verified. d) There should be provision for having separate authorized user (at the corporate level of each Buyer organization, i.e. external to its tendering departments) who can access the application-level audit-trail (ie audit-log) reports. Other users of the organization should not have access to these reports. e) Under no circumstances will it be required for any officer to hand over his/ her		

	private-key (used for digital-signing, or bid-decryption if applicable in the offered system) to anyone else – within the organization, or to anyone in the service provider's organization, or to anybody else. f) There could be occasions when an authorized officer of a Purchase/Buyer organization is on leave, gets transferred, resigns or his/ her services are terminated. One example where such an eventuality may arise is if the public key of the tender opening officer is used for bid encryption, and his private key required for bid decryption during the online tender opening event. There should no limitation in the e-tendering system which may necessitate that the private key of such an officer be handed over to anybody else for the scheduled tendering processes to continue uninterrupted. Note: The above is necessary for compliance with s-42(1) of the IT Act 2000.		
	<u>Guidance and recommended practices</u> The e-procurement system should have the features to address above. Under the IT Act, 2000 any holder of a Digital Signature, who's Digital Signature Certificate has been issued by a licensed CA, is responsible for protecting the corresponding private key. Unless the certificate validity has expired or the certificate has been revoked by the issuing CA, any digital signature will be legally valid and will be attributed to the person listed in the Digital Signature Certificate. Similar mechanism measures should be evolved for encryption key pair as well. Handing over of private (decryption) key by one officer to another officer both in case of digital signature as well as in case of encryption should not be allowed In case of digital signature, private key should be one of the two factor authentication method which must be implemented. The other could be Personal Identification Number (PIN) or biometric etc., so that nobody else can use the private key for signing the document. Further, it is the responsibility of the e-procurement system to reject the Digital Signature (except for verification) in case the corresponding Digital Signature Certificate has expired. It is suggested that e-procurement tendering system must have signing interface which can keep track of corresponding certificate particularly relating to expiry aspect of digital signature. There should also be a clause in the tender document stating that tender will not be considered for evaluation if the digital signature certificate has expired (except for verification).		
5.2	In any large Supplier/ Vendor organization, there can be multiple sales departments which can bid for different tenders. Also within each such department there can be	Cryptographic controls Regulation of	A 12.3 A.12.3.1 A policy on the use of cryptographic

	many executives involved with different activities relating to various tenders. A situation should not arise in the e-tendering system where due to limitation of the e-tendering system, these departments and executives are not able to themselves execute their duly assigned roles as in the manual process, and are constrained to re-assign/ abdicate their roles and responsibilities to a few tech-savvy technicians or the personnel of the service-provider of the e-tendering system.	cryptographic controls	controls for protection of information shall be developed and implemented. A.12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques A 15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
	<u>Guidance and recommended practices</u> This has implication on process and technology. There would be scenarios regarding multiple tendering within organization. e-Procurement software must have features to address such suggested issues' viz – multiple sales departments within a bidder/ supplier organization, multiple executives (each with his own digital signature certificate) for performing various e-procurement related tasks within each such department; system for managing roles and authorizations of such executives in case of transfer, leave, termination etc; independent executive within each bidder/ supplier organization for accessing audit trails relating to that organization. Apart from from ensuring security within a supplier/ bidder organization, such functionality is necessary to ensure that users within a supplier/ bidder organization do not handover their private keys to each other for completing an ongoing tendering process. If these concerns are not addressed, it would result in violation of s-42(1) of the IT Act. Further, it is suggested that organizations implementing e-procurement system should conduct training programmes for persons who have been assigned roles and are using the system on functional aspect related to process and technical aspects of the system. The training programme should also cover dos and don'ts for using the system.		
6. Some other functionality/ Security/ Transparency related requirements of a Manual Tendering System and Conformance its Availability in the offered e-tendering system			
6.1	<u>Concern</u> (Manual System)A Tender Notice is issued after internal clearance. Once a Tender Notice is published in a newspaper, it becomes an authentic record. (Electronic System) a) At a higher level, there should be clearance (which is audit-trailed within the application and digitally signed) before a Tender Notice is issued. b) For authenticity and for assurance that it has not been tampered, the electronic Tender	Cryptographic controls Regulation of cryptographic controls	A 12.3 A.12.3.1 A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A.12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques A 15.1.6 Cryptographic controls shall be used in compliance with all

	Notice (which is an electronic record), should have an audit-trail within the application of its creation/ approval/ posting. Also, the tender notice should be digitally signed by an authorized officer of the Purchase/ Buyer organization. <u>Concern</u> (Manual System) A Corrigendum is issued after internal clearance/ approval. Once a Corrigendum to a Tender Notice is published in a newspaper, it becomes an authentic record. (Electronic System) a) At a higher level, there should be clearance (which is audit-trailed within the application and digitally signed) before a Corrigendum is issued. b) For authenticity and for assurance that it has not been tampered, the electronic Corrigendum (which is an electronic record), should have an audit-trail within the application of its creation/ approval / posting. Also, the Corrigendum should be digitally signed by an authorized officer of the Purchase/ Buyer organization. <u>Concern</u> (Manual System) Once Tender Documents are published, and sold with official receipt and serial no. for each copy sold, these become an authentic record. (Electronic System) a) For authenticity and for assurance that it has not been tampered, the electronic Tender Documents (which is an electronic record), should have an audit-trail within the application of its posting. Also, the Tender Documents should be digitally signed by an authorized officer of the Purchase/ Buyer organization. b) At the time of online sale/ downloading of the tender documents, official serial number should be given along with the receipt. <u>Concern</u> (Manual System) An Addendum is issued after internal clearance/ approval. Once Addendum to Tender Documents are published, and		relevant agreements, laws, and regulations.

	distributed, these become an authentic record. (Electronic System) a) At a higher level, there should be clearance (which is audit-trailed within the application and digitally signed) before an Addendum is issued. b) For authenticity and for assurance that it has not been tampered, the electronic Addendum (which is an electronic record), should have an audit-trail within the application of its approval/ posting. Also, the Addendum should be digitally signed by an authorized officer of the Purchase/ Buyer organization. <u>Concern</u> (Manual System) Clarification of Tender Documents. In response to a bidder's query, an authorized officer of the Purchase/ Buyer organization responds to the querist with a copy to all other prospective bidders who have purchased tender documents (without revealing the identity of the querist). The response is signed by the concerned officer for authenticity. (Electronic System) The e-tendering system should also have such a facility with all the functionality as described in the previous column. For authenticity and for assurance that it has not been tampered, the response from the authorized officer of the Purchase/ Buyer organization should be digitally signed by him. <u>Concern</u> (Manual System) Pre-Bid meeting. The minutes of the Pre-bid meeting are signed for authenticity by an authorized officer of the Purchaser/ Buyer organization and made available to the prospective bidders. (Electronic System) The e-tendering system should also have such a facility with all the functionality as described in the previous column. For authenticity and for assurance that it has not been tampered, the Minutes should be digitally signed by an authorized officer of the Purchaser/ Buyer		

	organization. <u>Concern</u> (Manual System) Bid Methodologies/ Formats: Depending on the circumstances and nature of a tender, one of the many bidding methodologies may be prescribed by a Buyer, and the bidder would have to respond accordingly. • Single-stage, single- envelope • Single-stage, two- envelope • Two stage (with facility for 'technical conformance', and if required, 'revised tender documents') • Two-stage, two- envelope • Where required, the above may be combined with a Pre-qualification stage • In some cases, the Purchaser may allow submission of one or more Alternative bids • Each bid part (eg technical, financial) may be required to be submitted in a 'summary format' along with a 'detailed bid'. The latter could be a large file. • After having submitted the 'original' bid for each bid-part, a bidder has a right to submit: 'Modification' bid 'Substitution' bid Or 'Withdrawal' bid for all his bid-submissions. (Electronic System) The e-tendering system should support all the bidding methodologies/ formats as outlined above without sacrificing any aspect of security and transparency including those listed elsewhere in this document.		
	<u>Guidance and recommended practices</u> CVC Circular No. Office Order No.43/7/04 dated 2nd July 2004 had also required that tender documents posted on an e-tendering/ e-procurement website should be digitally signed by an officer of the tendering organization, and for the assurance of the bidder who is viewing or downloading the tender documents, the CVC circular required that facility be provided to verify the digital signature to ensure the authenticity and integrity of the tender documents. The e-procurement system should have functionality as outlined above under '(Electronic System)', and the Buyer organization should have related procedures to implement this.		
6.2	<u>Concern</u>	Cryptographic	A 12.3

	(Manual System) Signing of each page of each bid part (pre-qualification, technical, financial) especially the 'summary format' and the 'detailed' bid including modification, substitution, withdrawal. The sealed bids are deposited securely in a locked tender box, and stored securely till the box is opened during the public tender opening event. (Electronic System) The e-tendering system should have the corresponding facilities without sacrificing any aspect of security and transparency including those listed elsewhere in these Guidelines. • It should not be possible to open the 'e-tender boxes' till the specified time has occurred or elapsed, and till all the authorized Tender-Opening Officers have formally instructed the system to do so with PKI-based Digital Signatures • Till the Public Tender Opening Event, security related features should be such that the contents of the bids which are being stored cannot be 'accessed and decrypted' by even the authorized officers of the Purchaser/ Buyer or the Administrators of the Service Provider (even if they wish to do so with mala-fide intentions).	controls Regulation of cryptographic controls	A.12.3.1 A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A.12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques A 15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
	<u>Guidance and recommended practices</u> The e-procurement system should have features to address the suggestions made in this document. Any e-procurement/e-tendering services must provide the facility of Time Stamping which is critical for establishing data and time of document submission and its acknowledgement. Time Stamping feature should be built within the application and synchronisation of e-tendering/ e-procurement server should be done with master-server at the data-center where the e-procurement system is hosted (as mentioned in section 4.1 of these Guidelines). Alternatively, the e-procurement service provider can take Time Stamping services being provided by licensed CAs.		
6.3	(Manual System) Public Tender Opening Event(s) [Public TOEs] For Transparency, there is an elaborate procedure for opening of bids in the presence of authorized bidders. A few salient aspects of	Cryptographic controls Regulation of cryptographic controls	A 12.3 A.12.3.1 A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A.12.3.2

	this are: Authorized representatives of bidder organizations a) Who have submitted their bids are entitled to be present and have to sign in their attendance. b) Each bid is opened one at a time in front of the participating bidders, and the concerned bidder is entitled to satisfy himself that his bid packet is intact and has not been tampered with. c) If Bid security [earnest money deposit (EMD)] is applicable for a tender, then details of the EMD submitted, or exemption claimed with basis thereof is disclosed to the participants. d) Salient points of each opened bid are read out aloud for the benefit of the participating bidders, and to ensure that no change is made in the bid contents later on with connivance. e) Clarifications may be sought from a bidder whose bid has been opened and record is made of the query and the response. f) Each page of the opened bid is countersigned during the TOE itself (by each tender opening officer (typically up to 3) to ensure that no change is made in the bid contents later on with connivance. g) After all the bids are opened and countersigned by the TOE-officers, the minutes of the meeting (ie TOE) are to be recorded. h) Each bid part may be opened in a separate tender opening event in which only the authorized bidders are allowed. This is supposed to be done in a very transparent manner with proper scheduling of events and proper information to the concerned bidders. i) Bid parts which are due for opening in a subsequent tender opening event are securely stored till that event. j) If in a particular TOE, if it is decided not to open the bid of a bidder, then such bids are returned opened. (Electronic System) Facility for the authorized personnel to conduct Public Online Tender Opening Event with Bidders attending from remote		Key management shall be in place to support the organization's use of cryptographic techniques A 15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

	locations electronically with full security procedures. Tender-Opening Event should be simultaneously viewable by all attendees from their respective locations The e-tendering system should support all the salient aspects,viz a, b, c, d, e, f, g, h, i as listed in the previous column without sacrificing any aspect of security and transparency including those listed elsewhere in this matrix/ questionnaire. As soon as a bid is opened, participating bidders should be able to simultaneously download the salient points (ie the summary information) of the opened bid. For (j) keeping in view the nature of the internet, such bids may be archived unopened. Note: In addition, in cases where some bidders have bid offline (ie manually), and this has been allowed, then the following should be ensured: - That the offline bids are opened first and their salient points entered into the system before the online bids are opened. This is all done in the presence of the online bidders who are simultaneously witnessing this exercise. The compiled/ integrated data of the both the online and offline bidders should be made available in the form of an online comparison chart to all the participants.		
	<u>Guidance and recommended practices</u> The GFR requires that tenders be opened in public in the presence of the authorized representatives of the bidders. The Finance Ministry Manual on procurement procedures outlines in details the requirements of a transparently conducted Public Tender Opening Event. CVC Guidelines on security aspects of e-procurement also stae the requirement of 'Online Public Tender Opening Event'. Merely opening bids 'online', and then separately making them available for display to the bidders subsequently, and/ or from a different location/ screen (ie user interface) without the simultaneous online presence of bidders, does not fulfill the requirements of a proper and transparent online Public TOE. A comprehensive and transparent Public Tender Opening Event is the 'backbone of transparency and fairness' of the Public Procurement process, manual or electronic. This has an impact on technical as well as procedural aspects. It must be ensured that e-tendering/ e-procurement has comprehensive functionality for a transparent Public Online Tender Opening Event (Public OTOE). Well established practices of manual tender opening (with legal and transparency related significance) should have corresponding electronic equivalents for transparent e-tendering/ e-procurement. Some relevant processes of a fair and transparent online public TOE should include:		

	i. Opening of the bids in the simultaneous online presence of the bidders with proper online attendance record of the authorized representatives of the bidders. Merely opening bids online, and then subsequently displaying some results to the bidders does not fulfill the requirements of a transparent Online Public Tender Opening Event ii. Security Checks to assure bidders of non-tampering of their bids, et al during the online TOE itself iii. One-by-one opening of the sealed bids in the simultaneous online presence of the bidders iv. Online verification of the digital signatures of bidders affixed to their respective bids v. Reading out, ie allowing bidders to download the electronic version of the salient points of each opened bid (opened in the simultaneous online presence of the bidders) vi. There should be a procedure for seeking clarifications by the TOE officers during online Public TOE from a bidder in the online presence of other bidders, and recording such clarifications vii. Digital counter-signing (by all the tender opening officers) of each opened bid, in the simultaneous online presence of all participating bidders viii. Preparation of the 'Minutes of the Tender Opening Event' and its signing by the concerned officers in the simultaneous online presence of the bidders While bidders should be welcome to be present physically during the TOE, it should not be mandatory for them to do so. All the above should be achieved online in a user-friendly manner. The e-procurement system has to satisfactorily address the above requirements through suitable functionality built into the e-procurement application. Where, in addition, some issues are being further addressed through organizational procedures under ISO 27001, these should be explicitly defined with satisfactory explanations.		
7. Concerns/clarifications relating to preventing other Bidders from Bidding in the e-Tendering Scenario, and Miscellaneous Concerns/ Clarifications			
7.1	Can the e-tendering prevent competitors/ tender mafia from locking the accounts (target accounts) of other users/ bidders by deliberately entering incorrect authentication information against user-names (which are not secret) of such bidders/ users?	Control of technical vulnerabilities Cryptographic controls Regulation of cryptographic controls	A 12.6.1 Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. A 12.3 A.12.3.1 A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A.12.3.2 Key management shall be in place to support the

			organization's use of cryptographic techniques A 15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
	Guidance and recommended practices Generally any system are designed in such a manner that it gets locked/denied permission after repeated login attempts based on wrong passwords and user IDs. Such a scenario, if it exists, in e-procurement system may be exploited by the competitors/tender mafia to prevent the genuine bidders. To avoid such a situation the e-procurement system should not have features for locking the system on account of repetitive login attempts based on wrong passwords and user IDs and digital signatures. It is also suggested that login to the e-procurement system should be based on digital signatures. It has also been suggested that e-procurement system should have interface software to check the validity of digital signature/certificate. Other innovative methods may also be developed to address this concern.		
7.2	For security reasons, Administrators of the e-tendering application/ portal should not have any access to the passwords of the various users. Neither should the Administrators be able to generate passwords for the users.	Control of technical vulnerabilities Cryptographic controls Regulation of cryptographic controls	A 12.6.1 Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. A 12.3 A.12.3.1 A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A.12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques A 15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
	Guidance and recommended practices The Administrators of the e-tendering application/portal should not have any access to the passwords of the various users. Neither the software should allow the Administrator to generate password for the users. The designer/developer should factor this at the design stage/development stage, ie the e-procurement system has to satisfactorily address the above requirements through suitable functionality built into the e-procurement application.		

7.3	The Forgot Password feature should not be based on some questions and answers which can be guessed by a competitor/ hacker. Please explain how this is achieved.	Control of technical vulnerabilities Cryptographic controls Regulation of cryptographic controls	A 12.6.1 Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. A 12.3 A.12.3.1 A policy on the use of cryptographic controls for protection of information shall be developed and implemented. A.12.3.2 Key management shall be in place to support the organization's use of cryptographic techniques A 15.1.6 Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
	<u>Guidance and recommended practices</u> If the e-procurement system has "Forgot Passwords feature", it should address these concerns.		
7.4	There should be facility for Comprehensive Electronic Audit-Trail (ie Audit-Log, or Vigilance Reports) within the application with provision for Archiving. Specifically: i) There should be audit trail reports for -- each tender of each Buyer organization, as well as, non-tender specific activities (like creation of user-hierarchy and role authorization), which is viewable only to the authorized user of that Buyer organization. Other users of the organization should not have access to these audit trail reports. ii) Similarly, there should be audit trail reports for -- each tender of each Supplier/ Bidder organization, as well as, non-tender specific activities (like creation of user-hierarchy and role authorization), which is viewable only to the authorized user of that Supplier organization. Other users of the organization should not have access to audit trail reports.	Log monitoring	A 10.10 A.10.10.1 Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. A.10.10.2 Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly. A.10.10.3 Logging facilities and log information shall be protected against tampering and unauthorized access. A.10.10.4 System administrator and system operator activities shall be logged. A.10.10.5 Faults shall be logged, analyzed, and appropriate

	iii) As backup, and as protection against tampering of audit-trail reports saved by an individual organization at its end, facility should be available for the authorized e-procurement application administrator to have parallel access to such reports of both Buyer organizations, as well as, Supplier organizations. Furthermore, information pertaining content of bids and Bid Submission [which is sensitive till the Tender-Opening Event (TOE)], should not be accessible to the e-procurement application administrator till the start of the TOE. iv) The authorized administrator of the e-procurement/ e-tendering application should also have access to audit trail reports of other administrators within the application. v) The application should not provide any facility to modify or delete audit logs, or suspend logging operations		action taken. A.10.10.6 The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source
	Guidance and recommended practices The e-procurement system and software should have the facility and functionality. There should be facility for Reports relating to Tendering-Activities, and corresponding MIS Reports which are accessible to the relevant authorized users of that organization.		
7.5	As required in a CVC order, the e-tendering system should have facility for displaying 'Award of Contracts'	CVC Order	NA
	Guidance and recommended practices The application shall have this functionality. Furthermore, this information should be digitally signed by the concerned user of the Buyer organization with facility for verification by the viewer.		
7.6	It is important that officers of a Buyer organization involved in procurement related activities continue to perform their related roles without re-assigning or abdicating responsibilities. A pre-requisite to enable officers to perform their roles is the existence of comprehensive virtual hierarchy and role-authorization as outlined above. Another requirement to enable this is that e-Tendering Systems must design their user interfaces to be "user friendly", and that all information that the user needs to perform each transaction is available easily and clearly from the screen Concern	Control of technical vulnerabilities	A 12.6.1 Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

	The e-Tendering application must be designed, developed and deployed using reputed and secure platforms such as -- .DotNet, J2EE etc, that minimize defects like bugs and vulnerabilities. It is important to ensure that during deployment; only compiled codes of the e-tendering application software are used, with further protection to prevent run-time modifications in the code. Please clarify how this is achieved. Concern It should not be possible to compromise the security of the e-tendering application, even with knowledge of its architecture, design and encryption algorithm used.		
	Guidance and recommended practices The application shall be architectured, designed and developed (ie the required functionality should be inbuilt in the application) to address above concerns. The best practices and processes to develop secure software shall be followed.		
8. Concerns relating to Bidders making false assertions based on non-existing functionality in their e-tendering software (Important Eligibility/ Qualifying Criteria)			
	References may be given of various clients who have used the e-tendering/ e-procurement software before the date of submission of bids. Such references should state whether or not the e-Tendering software supplied to each reference client was capable of handling each of the following requirements: composite technical & financial bids (single stage- single envelope); technical and financial bids in separate envelopes (single stage- two envelope); single stage two envelope preceded by pre-qualification; and various security and transparency related concerns outlined in this Annexure-I, Annexure-II (which is based on CVC Guidelines).	• Quality assessment of solution • Publically available capability • No monopolization	NA
	Guidance and recommended practices The solution should be assessed in respect of various security and transparency related concerns outline in these Guidelines, and its scope of Capability should be in public domain, ie the functionality claimed should have references. This will discourage monopolizing a particular vendor and solution and will encourage new entrants from offering such systems thereby affecting the competitiveness of procurement of systems. To encourage new entrants, while there should be no compromise on security, transparency and crucial functionality related concerns highlighted herein, the eligibility criteria in respect of 'number of tenders', 'revenue criteria from e-procurement', etc should be minimum.		

Summary- Analysis of Risk of eProcurement Systems

Security Risks	
Security	Compromise through potential weaknesses in the system
Availability	The need for services to be `on' all the time
Authentication	Masquerading identity or repudiation of message Any purchasing system must support authentication of users so that individual transaction can be traced back to the relevant person. Generally, this is by user name and password. Alternatively, the authentication mechanism could be network login or other directory services, while higher security requirement may demand token based method such as digital certificate, smart card or biometrics devices.
Access	To ensure users only have access to the functions required to do their jobs, an eProcurement system should incorporate "roles – based" access control mechanism. This should allow a particular role to be assigned to each user of the application, and to determine which function areas this role incorporates.
Audit Trail	A robust eProcurement solution should incorporate a comprehensive audit trail, with recording of who did what and when at various key stages of the purchasing process. The system should also allow rules to be incorporated, example the person who approves a requisition must be different from the requisition originator. Setting such principles within the purchasing application can be a useful counter major against possible fraud.
Liability	Through employment or legal contractual obligations
Computer Fraud	Internal abuse and misuse
Breach by external party	External attack by various parties, whether corporate espionage or terrorists
Virus affecting the system	Email viruses such as NIMDA or Melissa which have capability of crippling systems
Denial of service	Flooding a computer's internet connection with requests to disrupt traffic flow
Intellectual property	Misappropriation or release of intellectual property
Software Risks	
Switching Cost and compliance with Rules of Government Procurement	Control of spending to specific suppliers as part of e-Commerce
Applets, scripting and punch-out	Some applications which only require users to have access to the internet via a web browser may also require additional software to be installed and run on the local machine, such as ActiveX components, Java Applets, browser script and cookies. Security policy should allow these software components to be installed and run.
Interoperability	Lack of interoperability between the system of the bidder and system of the procurement body System interoperability is the smooth transition of data between systems internally within an organisation, example between an

	eProcurement system and a finance system and externally example between a buyers eProcurement system and suppliers eCommerce System. The preferred method of data flow today is eXtensible Mark-Up Language (XML). XML is accepted a core standard for data exchange between the Government and Business.
Project Risks	
Competitive information	Risk to customer and supplier data, as well as other commercially sensitive information
Lack of required skills	Staff not being properly equipped with the correct skill set. Repercussion of not adhering to roles & responsibilities while handling private key/ user secret of personnel involved in e procurement life cycle.
Wrong technology choice	Investing in the wrong technology, this may lead to greater costs than initially projected, or being stuck with a vendor
Complexity and Management of electronic records	Increasing complexity of organisation, systems and models The increasing electronic delivery of public services to business and citizens, in turn, producing more electronic records. Electronic records unlock content previously difficult to assess in paper form, enable more effective sharing of information and contribute to knowledge exchange. However, they need to be retained and maintained over the medium to long term as the records also demonstrate accountability. Privacy and excess issues and particularly right to information act, VAT and other taxation act required that electronic records be managed constantly within regulatory environment.
Reputational Risk	The risk of damaging goodwill or brand equity as a result of e-Commerce mishap
Business Continuity	To protect historic data in the event of a system failure, or to allow a purchase department to continue off-site in the event of disaster, security arrangement should also include a business continuity plan. This should detail : • **Precautions** to prevent disaster from occurring such as virus checking • **Physical security** in the premises where the application is held and • **Duplication of data** onto multiple storage devices • **Procedures** to follow in the event of an unrecoverable disaster e.g. retrieval of off-site back-ups or relocating to a "warm recovery" server which contains all historical data. Finally, it is important to test any continuity plans on a regular basis. The time to discover that not all relevant files are backed up is during a test drill, not when trying to recover after a catastrophic failure.
Environmental Risks	
Natural hazard	Because of involvement of remotely located additional body
Changing technology	Rate of change of technology progressing ahead of the ability to secure it
Maverick Spend/compliance	Procurement risk, describing employee's expenditure via non-preferred suppliers, resulting in a blow-out in costs.

Annexure-II - Checklist for eSecurity Compliance (including CVC Guidelines)

Table 1: General Security Issues

Sl. No.	Issues to be Checked	Means of Checking
1	Whether the application is secure from making any temporary distortion in the electronic posing of tender notice, just to mislead certain vendors?	Functionality Verification/Testing (Application level)
2	If yes at 2 above, then whether any automatic systems alert is provided in the form of daily exception report in the application in this regards?	Functionality Verification/Testing (Application level)
3	Whether application ensures that the tender documents issued to/downloaded by bidders are complete in shape as per the approved tender documents including all its corrigendum?	Functionality Verification/Testing (Application level)
4	Is there any check available in the application to detect and alert about the missing pages to the tenderer, if any?	Functionality Verification/Testing (Application level)
5	Whether application ensures that all the corrigendum issued by the Competent Authority are being fully communicated in proper fashion to all bidders including those who had already purchased/downloaded the bid documents well ahead of the due date and before uploading the corrigendum?	Functionality Verification/Testing (Application level)
6	Whether system is safe from sending discriminatory communication to different bidders about the same e-tendering process?	Functionality Verification/Testing (Application level)
7	Whether e-procurement solution has also been customized to process all type of tenders viz Limited/Open/Global Tenders?	Functionality Verification/Testing (Application level)
8	Whether online Public Tender opening events feature are available in the application?	Functionality Verification/Testing (Application level)
9	Whether facilities for evaluation/loading of bids, strictly in terms of criteria laid down in bid documents are available in the application?	Functionality Verification/Testing
10	Whether sufficient safeguards have been provided in the application to deal with failed attempt blocking?	Functionality Verification/Testing (Application level)
11	Whether application is safe from submission of fake bids?	Functionality Verification/Testing to check that a bid can be submitted only by a duly authorized user of the bidder organization, and that all bidder organizations are authenticated. (Application level) • Application Vulnerability

		Assessment (Test for OWASP Top 10 and other known vulnerabilities) • (Application level)
12	Whether encryptions of bids are done at clients end?	Functionality Verification/Testing (Application level)
13	Whether safety against tampering and stealing information of submitted bid, during storage before its opening is ensured?	• Functionality Verification/Testing of related 'features' and 'explanations' given by the e-procurement/ e-tendering software/ service provider against relevant sections and points of Annexure-I, viz sections 2, 3 and 4 of Annexure-I. (Application level, as well as, Network level) • Application Vulnerability Assessment (Test for OWASP Top 10 and other known vulnerabilities) (Application level, as well as, Network level)
14	Whether application is safe from siphoning off and decrypting the clandestine copy of a bid encrypted with Public key of tender opening officer?	• Functionality Verification/Testing of related 'features' and 'explanations' given by the e-procurement/ e-tendering software/ service provider against relevant sections and points of Annexure-I, viz sections 2, 3 and 4 of Annexure-I. (Application level) • Application Vulnerability Assessment (Test for OWASP Top 10 and other known vulnerabilities)

		(Application level)
15	Whether application is safe from mutilation/sabotage of otherwise rendering the encrypted bid in the e-tender box during storage, to make it unreadable/invalid in any form, before opening of the bids?	• Functionality Verification/Testing of related 'features' and 'explanations' given by the e-procurement/ e-tendering software/ service provider against relevant sections and points of Annexure-I, viz sections 2, 3 and 4 of Annexure-I. (Application level, as well as, Network level) • Application Vulnerability Assessment (Test for OWASP Top 10 and other known vulnerabilities) (Application level, as well as, Network level)
16	Whether introduction of special characters/executable files etc by users are restricted in the application?	Testing of Input Validation (Refer OWASP Testing Guide) (Application level)
17	Whether validity check of DSC is being done at server end?	Verification of the implementation (Application level)
18	Whether system supports the feature that even though if a published tender is being deleted from the application, does not allow permanent deletion of the published tender from the Database?	Verification of the implementation (Application level)
19	Whether sufficient security features are provided in the application for authentication procedure of the system administrator like ID, password, digital signature, biometric etc.	Review of the authentication mechanism implemented. (Application level, as well as, Network level)
20	Whether audit trails are being captured in the application on media not prone to tampering, such as optical write once?	Verification of the implementation (Application level, as well as, Network level)
21	Whether log shipping featuring available, where a separate dedicated server receives the logs from the application over web service in real time?	Verification of the implementation (Network level)
22	Whether integrity and non-tampering is ensured in maintaining the server clock synchronization and time stamping?	Verification of the implementation (Network level)
23	Whether application generates any exception	Functionality

	report/system alerts etc to indicate the resetting of the clock, in case the application for time stamping is killing at the server level and time is manipulated?	Verification/Testing (Network level)
24.	Whether application ensures that the quotes from various bidders with their name are not being displayed to anyone including to the organization during carrying out of the e-reverse auctioning process?	Functionality Verification/Testing (Application level)
25	Whether application is fit for usage complying with the requirements of tender processing viz authenticity of tender, non-repudiation and secrecy of information till the actual opening of tenders	Functionality Verification/Testing (Refer GFR for the requirements) (Application level)
26	Whether any comprehensive third party audit (as per statutory requirement and also as per the requirements of e-tender processing (compliance to IT Act 2000) was got conducted before first putting it to public use?	Verification of records/reports/certificates (Application level, as well as, Network level)
27	Whether application complies with the Commission/s Guidelines dated 17.9.2009 on Security consideration for e-procurement systems	Covered below

Table 2: Infrastructure Security Issues

Sl. No.	Issues to be Checked	Means of Checking
1	Perimeter Defence: Deployment of routers, firewalls. IPS/IDS, Remote Access and network segmentation.	• Network Architecture Review • Assessment of vulnerabilities and hardening/configuration of network and security devices e.g. routers, switches, firewalls, IPS/IDS etc. (Network level)
2	Authentication: Network authentication through deployment of password policy for accessing the network resources. To minimize unauthorised access to the e-procurement system, at system level.	Review of authentication policies and mechanisms (Network level)
3	Monitoring: Deployment of logging at OS/ network level and monitoring the same.	Review of logging and monitoring policies, procedures & mechanisms (Network level)
4	Secure configuration of network host: The security of individual servers & workstations is a critical factor in the defence of any environment, especially when remote access is allowed workstations should have Safeguards in place to resist common attacks.	Assessment of vulnerabilities and hardening/configuration of the hosts (servers, client work stations etc.) (Network level)
5	System patching:	• Review of Patch

	As the vulnerability of the system is discovered almost regularly and the system vendors are also releasing the patches, It is expected that the host are patched with latest security updates.	Management Procedure • Verification of the system patching status (Network level)
6	Control of Malware: Suitable control like anti-virus, anti spyware ext. should be deployed on the host associated with e-procurement system. However, option for running the services at non-privileged user profile may be looked for. Otherwise suitable operating system which is immune to virus, Trojan and malware may be deployed.	Review of Malware Control policies, procedures and mechanisms (Network level)
7	Structured cabling: The availability of the network services is critically dependent on the quality of interconnection between the hosts through structured including termination & marking. It is expected the e-procurement system has implemented structured cabling and other controls related with network and interconnection.	Verification of the cabling (Network level)

Table 3: Application Security Issues at Design Level

Sl. No.	Issues to be Checked	Means of Checking
1	Authentication: The authentication mechanism of the e-procurement application should ensure that the credentials are submitted on the pages that are served under SSL	Functionality Verification of the implementation (Application level, and SSL verification at Network Level)
2	Access Control: The application shall enforce proper access control model to ensure that the parameter available to the user cannot be used for launching any attack.	Assessment/Testing (Refer OWASP Testing Guide) (Application level)
3	Session management: The design should ensure that session tokens are adequately protected from guessing during an authenticated session.	Assessment/Testing (Refer OWASP Testing Guide) (Application level)
4	Error handling: The design should ensure that the application does not present user error messages to the outside world which can be used for attacking the application.	Assessment/Testing (Refer OWASP Testing Guide) (Application level)
5	Input validation: The application may accept input at multiple points from external sources, such as users, client applications, and data feeds. It should perform validation checks of the syntactic and semantic validity of the input. It should also check that input data does not violate limitations of underlying or dependent components, particularly string length and character set.	Assessment/Testing (Refer OWASP Testing Guide) (Application level)

	All user-supplied fields should be validated at the server side.	
6	Application logging and monitoring: Logging should be enabled across all applications in the environment. Log file data is important for incident and trend analysis as well as for auditing purposes. The application should log failed and successful authentication attempts, changes to application data including user accounts, serve application errors, and failed and successful access to resources	Functionality Verification of the implementation (Application level)

Table 4: Application Security Issues During Deployment & Use

Sl. No.	Issues to be Checked	Means of Checking
1	Availability /Clustering /Load balancing: Depending on the number of expected hits and access the option for clustering of servers and load balancing of the web application shall be implemented	Verification of the implementation (Network level)
2	Application and data recovery: Suitable management procedure shall be deployed for regular back-up of application and data. The regularity of data backup shall be in commensurate with the nature of transaction/ business translated into the e-procurement system.	Review of backup policies, procedures and the backup and restoration records. (Network level)
3	Integrity of the Application, Control of source code. Configuration management: Suitable management control shall be implemented on availability of updated source code and its deployment. Strict configuration control is recommended to ensure that the latest software in the production system.	Review of the configuration management procedure, mechanism and its implementation (Network level)

Table 5: Application Security Issues during Data Storage & Communication

Sl. No.	Issues to be Checked	Means of Checking
1	Encryption for data storage: Sensitive data should be encrypted or hashed in the database and file system. The application should differentiate between data that is sensitive to disclosure and must be encrypted, data that is sensitive only to tampering and for which a keyed hash value (HMAC) must be generated, and data that can be irreversibly transformed (hashed) without loss of functionality (such as passwords). The application should store keys used for decryption separately from the encrypted data.	Verification of the implementation (Application level)
2	Data transfer security: Sensitive data should be encrypted prior to transmission to other components. Verify that	Verification of the implementation (Application level, as well as,

	intermediate components that handle the data in clear-text form, prior to transmission or subsequent to receipt, do not present an undue threat to the data. The application should take advantage of authentication features available within the transport security mechanism. Specially, encryption methodology like SSL must be deployed while communicating with the payment gateway over public network.	Network level)
3	Access control: Applications should enforce an authorization mechanism that provides access to sensitive data and functionality only to suitably permitted users or clients. Role-based access controls should be enforced at the database level as well as at the application interface. This will protect the database in the event that the client application is exploited. Authorization checks should require prior successful authentication to have occurred. All attempts to obtain access, without proper authorization should be logged Conduct regular testing of key applications that process sensitive data and of the interfaces available to users from the Internet include both "black box" informed" testing against the application. Determine if users can gain access to data from other accounts.	Testing/Assessment of the access control implementation as per defined policies. (Application level)

Annexure-III – Checklist for Compliance to GOI procurement procedures
GFR 2005, Government of India, Ministry of Finance, Department of Expenditure

The contents of GFR 2005 are as follows:

Chapter	Name of the Chapter
1.	Introduction
2.	General System of Financial Management I. General Principles relating to expenditure & payment of money II. Defalcation and losses III. Submission of records & information
3.	Budget formulation and implementation
4.	Government Accounts
5.	Works
6.	Procurement of Goods and Services I. Procurement of Goods II. Procurement of Services
7.	Inventory Management
8.	Contract Management
9.	Grants-in-aid and Loans
10.	Budgeting and Accounting for Externally Aided Projects
11.	Government Guarantees
12.	Miscellaneous Subjects I. Establishment II. Refund of revenue III. Debt and misc. obligations of Govt. IV. Security deposits V. Transfer of land and buildings VI. Charitable endowments and other trusts VII. Local bodies VIII. Destruction of records connected with Accounts IX. Contingent and Miscellaneous Expenditure.

Chapter-6, Procurement of Good & Services is applicable for e-Procurement System (EPS).

The list of GFR requirements given below provides general guidelines about the applicability of the requirements in the EPS and the verification mechanism. The assumption has been made that in an ideal situation, all the GFR requirements will be applicable to the EPS. However, in actual situation, depending on the client's (buyer organization) requirements, all the GFR requirements may not be applicable and hence not addressed by the EPS. Therefore, it is recommended that the EPS solution/ service provider uses this list as a guideline and prepares similar list for the EPS being developed as per the applicability of the GFR requirements.

The compliance to applicable GFR requirements may be verified as follows:

- In case of manual procurement system, compliance verification may be done through process audit of the policy & procedures of the client's (buyer organization). It is up to the client to perform the process audit to ensure compliance.
- In case of e-procurement system, compliance verification shall be done through **testing and audit of the functionalities in the EPS solution**. It is recommended; that internal verification may be done by the EPS solution provider and also be externally verified by Third Party Agency for client's acceptance.

Rule	Description	To Be Addressed By	Compliance Verification
	General		
	GFR covers Rules relating to – Tenders relating to Works, Goods and Services. The e-procurement system should have functionality to cover all kinds of tenders, whether the tenders relate to Works, Goods or Services. While some specific rules relating to procurement of Goods and Services are outlined below, corresponding functionality for Works tenders should also be implemented in the e-procurement system.		

Chapter 6: Procurement of Goods and Services - Guidelines

Rule	Description	To Be Addressed By	Compliance Verification
	A) Procurement of Goods: Rule 135 to 162		
135	This chapter contains the general rules applicable to all Ministries or Departments, regarding procurement of goods required for use in the public service. Detailed instructions relating to procurement of goods may be issued by the procuring departments broadly in conformity with the general rules contained in this Chapter.	-	-
136	**Definition of Goods** The term 'goods' used in this chapter includes all articles, material, commodities, livestock, furniture, fixtures, raw material, spares, instruments, machinery, equipment, industrial plant etc. purchased or otherwise acquired for the use of Government but excludes books, publications, periodicals, etc. for a library.	-	-
137	**Fundamental principles of public buying:** Every authority delegated with the financial powers of procuring goods in public interest shall have the responsibility and accountability to bring efficiency, economy, and transparency in matters relating to public procurement and for fair and equitable treatment of suppliers and promotion of competition in public procurement. The procedure to be followed in making public procurement must conform to the following yardsticks: (i) The specifications in terms of quality, type etc., as also quantity of goods to be procured, should be clearly spelt out keeping in view the specific needs of the procuring organisations. The specifications so worked out should meet the	e-procurement System should have functionality to ensure transparency, accountability, fairness and equitable treatment of suppliers. This should be ensured by e-procurement system strictly and satisfactorily addressing the various issues especially outlined in Annexure-I of these Guidelines. Specifically for fairness it must be ensured that the e-procurement system	Functionality Verification/Testing of related 'features' and 'explanations' given by the e-procurement/ e-tendering software/ service provider against relevant sections and points of Annexure-I of these Guidelines

	basic needs of the organisation without including superfluous and non-essential features, which may result in unwarranted expenditure. Care should also be taken to avoid purchasing quantities in excess of requirement to avoid inventory carrying costs; (ii) Offers should be invited following a fair, transparent and reasonable procedure; (iii) The procuring authority should be satisfied that the selected offer adequately meets the requirement in all respects; (iv) The procuring authority should satisfy itself that the price of the selected offer is reasonable and consistent with the quality required; (v) At each stage of procurement the concerned procuring authority must place on record, in precise terms, the considerations which weighed with it while taking the procurement decision.	supports all legitimate processes and methodologies for inviting bids in a transparent manner, and under no circumstances should the confidentiality of the bid be compromised before the Online Public Tender Opening Event. Importantly, a properly conducted Public Tender Opening Event is the backbone of transparency in public procurement. The e-procurement system must have a very transparent and comprehensive Online Public Tender Opening Event. For accountability, there should be a comprehensive Hierarchy and Role Authorization of officers with detailed Audit Trails as outlined in Annexure-I of these Guidelines. Where required, functionality of the e-procurement system should be supplemented with Procurement Policy & Procedures internal to the Buyer organization.	
138	**Authorities competent to purchase goods:** An authority which is competent to incur contingent expenditure may sanction the purchase of goods required for use in public service in accordance with Schedule V of the Delegation of Financial Powers Rules, 1978, following the general procedure contained in the following rules.	e-procurement System should have functionality for Requisition Management (ie Indent Management) with digital signatures.	Functionality Verification/Testing & Audit
139	**Procurement of goods required on mobilisation:** Procurement of goods required on mobilisation and/ or during the continuance of Military operations shall be regulated by special rules and orders issued by the Government on this behalf from time to time.	Procurement Policy & Procedures internal to the Buyer organization Note: Generally no specific requirements for e-procurement.	Process Audit

140	**Powers for procurement of goods:** The Ministries or Departments have been delegated full powers to make their own arrangements for procurement of goods. In case however, a Ministry or Department does not have the required expertise, it may project its indent to the Central Purchase Organisation (e.g. DGS&D) with the approval of competent authority. The indent form to be utilised for this purpose will be as per the standard form evolved by the Central Purchase Organisation.	Procurement Policy & Procedures internal to the Buyer organization Note: Generally no specific requirements for e-procurement.	Process Audit
141	**Rate contract:** The Central Purchase Organisation (e.g. DGS&D) shall conclude rate contracts with the registered suppliers, for goods and items of standard types, which are identified as common user items and are needed on recurring basis by various Central Government Ministries or Departments. Definition of Registered suppliers is given in **Rule 142 below.** The Central Purchase Organisation will furnish and update all the relevant details of the rate contracts in its web site. The Ministries or Departments shall follow those rate contracts to the maximum extent possible.	Procurement Policy & Procedures internal to the Buyer organization Note: Generally no specific requirements for e-procurement.	Process Audit
142	**Registration of suppliers:** With a view to establishing reliable sources for procurement of goods commonly required for Government use, the Central Purchase Organisation (e.g. DGS&D) will prepare and maintain item-wise lists of eligible and capable suppliers. Such approved suppliers will be known as "Registered Suppliers". All Ministries or Departments may utilise these lists as and when necessary. Such registered suppliers are prima facie eligible for consideration for procurement of goods through Limited Tender Enquiry. They are also ordinarily exempted from furnishing bid security along with their bids. A Head of Department may also register suppliers of goods which are specifically required by that Department or Office. (ii) Credentials, manufacturing capability, quality control systems, past performance, after-sales service, financial background etc. of the supplier(s) should be carefully verified before registration. (iii) The supplier(s) will be registered for a fixed period (between 1 to 3 years) depending on the nature of the goods. At the end of this period, the registered supplier(s) willing to continue with registration are to apply afresh for renewal of registration. New supplier(s) may also be	Procurement Policy & Procedures internal to the Buyer organization Note: Generally no specific requirements for e-procurement.	Process Audit Functionality Verification/Testing

	considered for registration at any time, provided they fulfil all the required conditions. (iv) Performance and conduct of every registered supplier is to be watched by the concerned Ministry or Department. The registered supplier(s) are liable to be removed from the list of approved suppliers if they fail to abide by the terms and conditions of the registration or fail to supply the goods on time or supply substandard goods or make any false declaration to any Government agency or for any ground which, in the opinion of the Government, is not in public interest.		
143	**Enlistment of Indian agents:** As per the Compulsory Enlistment Scheme of the Department of Expenditure, Ministry of Finance, it is compulsory for Indian agents, who desire to quote directly on behalf of their foreign principals, to get themselves enlisted with the Central Purchase Organisation (eg. DGS&D). However, such enlistment is not equivalent to registration of suppliers as mentioned under **Rule 142 above**.	e-procurement System should have feature for bidder (Indian Agent) to be able to furnish details of their enlisting with the concerned Central Purchase Organization in the bid.	Functionality Verification/Testing & Audit
144	**Reserved items:** The Central Government, through administrative instructions, has reserved all items of handspun and handwoven textiles (khadi goods) for exclusive purchase from Khadi Village Industries Commission (KVIC). It has also reserved all items of handloom textiles required by Central Government departments for exclusive purchase from KVIC and/or the notified handloom units of ACASH (Association of Corporations and Apex Societies of Handlooms). The Central Government has also reserved some items for purchase from registered Small Scale Industrial Units. The Central Departments or Ministries are to make their purchases for such reserved goods and items from such units as per the instructions issued by the Central Government in this regard.	e-procurement System should have feature for Tender Notice to highlight such special reservations.	Functionality Verification/ Testing
145	**Purchase of goods without quotation (Upto Rs.15,000/-):** Purchase of goods upto the value of Rs. 15,000/- (Rupees Fifteen Thousand) only on each occasion may be made without inviting quotations or bids on the basis of a certificate to be recorded by the competent authority in the following format. "I, _____, am personally satisfied that these goods purchased are of the requisite quality and specification and have been purchased from a reliable supplier at a reasonable price."	Procurement Policy & Procedures internal to the Buyer organization Note: Generally no specific requirements for e-procurement.	Process Audit

146	**Purchase of goods by purchase committee (Above Rs.15,000/- & upto Rs.1,00,000/-):** Purchase of goods costing above Rs. 15,000/- (Rupees Fifteen Thousand) only and upto Rs. 1,00,000/- (Rupees One lakh) only on each occasion may be made on the recommendations of a duly constituted Local Purchase Committee consisting of three members of an appropriate level as decided by the Head of the Department. The committee will survey the market to ascertain the reasonableness of rate, quality and specifications and identify the appropriate supplier. Before recommending placement of the purchase order, the members of the committee will jointly record a certificate as under. "Certified that we _____, members of the purchase committee are jointly and individually satisfied that the goods recommended for purchase are of the requisite specification and quality, priced at the prevailing market rate and the supplier recommended is reliable and competent to supply the goods in question."	Procurement Policy & Procedures internal to the Buyer organization Note: Generally no specific requirements for e-procurement.	Process Audit
147	**Purchase of goods directly under rate contract:** **(1)** In case a Ministry or Department directly procures Central Purchase Organisation (e.g. DGS&D) rate contracted goods from suppliers, the prices to be paid for such goods shall not exceed those stipulated in the rate contract and the other salient terms and conditions of the purchase should be in line with those specified in the rate contract. The Ministry or Department shall make its own arrangement for inspection and testing of such goods where required. **(2)** The Central Purchase Organisation (e.g. DGS&D) should host the specifications, prices and other salient details of different rate contracted items, appropriately updated, on the web site for use by the procuring Ministry or Department.	Procurement Policy & Procedures internal to the Buyer organization Note: Generally no specific requirements for e-procurement.	Process Audit
148	A demand for goods should not be divided into small quantities to make piece meal purchases to avoid the necessity of obtaining the sanction of higher authority required with reference to the estimated value of the total demand.	Procurement Policy & Procedures internal to the Buyer organization Note: Generally no specific requirements for e-procurement.	Process Audit
149	**Purchase of goods by obtaining bids:** Except in cases covered under **Rule 145, 146 and 147(1),** Ministries or Departments shall procure goods under the powers referred to in **Rule 140** above by following the standard method of obtaining bids in:	Procurement Policy & Procedures e-procurement system should have functionality for creating and	Process Audit Functionality Verification/Testing of related

	(i) Advertised Tender Enquiry; (ii) Limited Tender Enquiry; (iii) Single Tender Enquiry.	managing Tender Notices, Corrigenda, Tender Documents, Addenda; floating Open Tenders, as well as, Limited Tenders (Single Tenders being a special case of Limited Tenders); and functionality for other associated processes	'features' and 'explanations' given by the e-procurement/ e-tendering software/ service provider against relevant sections and points of Annexure-I
150	**Advertised tender enquiry:** (i) Subject to exceptions incorporated under **Rules 151 and 154**, invitation to tenders by advertisement should be used for procurement of goods of estimated value Rs. 25 lakh (Rupees Twenty Five Lakh) and above. Advertisement in such case should be given in the Indian Trade Journal (ITJ), published by the Director General of Commercial Intelligence and Statistics, Kolkata and at least in one national daily having wide circulation. (ii) An organisation having its own web site should also publish all its advertised tender enquiries on the web site and provide a link with NIC web site. It should also give its web site address in the advertisements in ITJ and newspapers. (iii) The organisation should also post the complete bidding document in its web site and permit prospective bidders to make use of the document downloaded from the web site. If such a downloaded bidding document is priced, there should be clear instructions for the bidder to pay the amount by demand draft etc. along with the bid. (iv) Where the Ministry or Department feels that the goods of the required quality, specifications etc., may not be available in the country and it is necessary to also look for suitable competitive offers from abroad, the Ministry or Department may send copies of the tender notice to the Indian embassies abroad as well as to the foreign embassies in India. The selection of the embassies will depend on the possibility of availability of the required goods in such countries. (v) Ordinarily, the minimum time to be allowed for submission of bids should be three weeks from the date of publication of the tender notice or availability of the bidding document for sale, whichever is later. Where the department also contemplates obtaining bids from abroad, the minimum period should be kept as four weeks for	e-procurement System should have functionality for creating and managing Tender Notices, Corrigenda, Tender Documents, Addenda; floating Open Tenders with functionality for other associated processes. Cost of priced Tender Documents should be payable online at the time of downloading tender documents, or payable offline parallel to the online bid-submission before the bid-submission deadline. In the latter case, provision should be there to take the offline payment on record during the Public TOE. In addition, the concerned Buyer organization should have Procurement Policy & Procedures to implement the other requirements	Functionality Verification/Testing of related 'features' and 'explanations' given by the e-procurement/ e-tendering software/ service provider against relevant sections and points of Annexure-I. In addition, audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.

	both domestic and foreign bidders.		
151	**Limited tender enquiry:** (i) This method may be adopted when estimated value of the goods to be procured is up to Rupees Twenty-five Lakhs. Copies of the bidding document should be sent directly by speed post/ registered post/courier/ e-mail to firms which are borne on the list of registered suppliers for the goods in question as referred under **Rule 142 above**. The number of supplier firms in Limited Tender Enquiry should be more than three. Further, web based publicity should be given for limited tenders. Efforts should be made to identify a higher number of approved suppliers to obtain more responsive bids on competitive basis. (ii) Purchase through Limited Tender Enquiry may be adopted even where the estimated value of the procurement is more than Rupees twenty five Lakhs, in the following circumstances. (a) The competent authority in the Ministry or Department certifies that the demand is urgent and any additional expenditure involved by not procuring through advertised tender enquiry is justified in view of urgency. The Ministry or Department should also put on record the nature of the urgency and reasons why the procurement could not be anticipated. (b) There are sufficient reasons, to be recorded in writing by the competent authority, indicating that it will not be in public interest to procure the goods through advertised tender enquiry. (c) The sources of supply are definitely known and possibility of fresh source(s) beyond those being tapped is remote. (iii) Sufficient time should be allowed for submission of bids in Limited Tender Enquiry cases.	e-procurement System should have functionality for inviting Limited Tenders (Domestic, as well as, Global) with all related features such as -- creating and managing Tender Notices, Corrigenda, Tender Documents, Addenda, sending Invitation Letters**,** etc. Relevant Supplier organizations registered by the Buyer under Rule 142 should be sent Invitation Letters. For web-publicity Tender Notices of such Limited Tenders (or Short-Term tenders) should be posted on the e-procurement website for general publicity. This is also a CVC requirement. In addition, the concerned Buyer organization should have Procurement Policy & Procedures to implement the other requirements	Functionality Verification/Testing of related 'features' and 'explanations' given by the e-procurement/ e-tendering software/ service provider against relevant sections and points of Annexure-I. In addition, audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.
152	**Two bid system:** For purchasing high value plant, machinery etc. of a complex and technical nature, bids may be obtained in two parts as under :- (a) Technical bid consisting of all technical details alongwith commercial terms and conditions; and (b) Financial bid indicating item-wise price for the items mentioned in the technical bid. The technical bid and the financial bid should be sealed by the bidder in separate covers duly superscribed and both these sealed covers are to be put in a bigger cover which should also be sealed and duly superscribed. The technical bids are to be opened by the purchasing Ministry or	e-procurement System should have functionality for inviting 'Single Stage Two Envelope' tenders or Two-Stage tenders (as mentioned in CVC guidelines), with secure methodology for sealing bids (ie data encryption of both the 'Technical', as well as, 'Financial' bid parts by the bidder himself before bid-submission. In addition,	Functionality Verification/Testing of related 'features' and 'explanations' given by the e-procurement/ e-tendering software/ service provider against relevant sections and points of Annexure-I.

	Department at the first instance and evaluated by a competent committee or authority. At the second stage financial bids of only the technically acceptable offers should be opened for further evaluation and ranking before awarding the contract.	there should be functionality for opening only the technical bids first; functionality for creating a short-list of technically responsive bidders; functionality for a second tender opening event for opening the financial bids of the technically responsive bidders	
153	**Late bids:** In the case of advertised tender enquiry or limited tender enquiry, late bids (i.e. bids received after the specified date and time for receipt of bids) should not be considered.	e-procurement System should have functionality for 'Not Accepting Late Bids'	Functionality Verification/Testing
154	**Single tender enquiry:** Procurement from a single source may be resorted to in the following circumstances: (i) It is in the knowledge of the user department that only a particular firm is the manufacturer of the required goods. (ii) In a case of emergency, the required goods are necessarily to be purchased from a particular source and the reason for such decision is to be recorded and approval of competent authority obtained. (iii) For standardisation of machinery or spare parts to be compatible to the existing sets of equipment (on the advice of a competent technical expert and approved by the competent authority), the required item is to be purchased only from a selected firm. Note: Proprietary Article Certificate in the following form is to be provided by the Ministry / Department before procuring the goods from a single source under the provision of sub **Rule 154 (i) and 154 (iii)** as applicable. (i) The indented goods are manufactured by M/s…….. (ii) No other make or model is acceptable for the following reasons: …….. (iii) Concurrence of finance wing to the proposal vide: …….. (iv) Approval of the competent authority vide: …… _____ (Signature with date and designation of the procuring officer)'	e-procurement System should have functionality for inviting bid from only one specified Supplier organization with all features applicable for Limited Tenders as highlighted above. In addition, the concerned Buyer organization should have Procurement Policy & Procedures to implement the other requirements	Functionality Verification/Testing In addition, audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.
155	**Contents of bidding document:** All the terms, conditions, stipulations and	e-procurement System should have functionality	Functionality Verification/Testing

	information to be incorporated in the bidding document are to be shown in the appropriate chapters as below: Chapter–1: Instructions to Bidders. Chapter–2: Conditions of Contract. Chapter–3: Schedule of Requirements. Chapter–4: Specifications and allied Technical Details. Chapter–5: Price Schedule (to be utilised by the bidders for quoting their prices). Chapter–6: Contract Form. Chapter–7: Other Standard Forms, if any, to be utilised by the purchaser and the bidders.	for – General Terms and Conditions, Special Terms and Conditions, Detailed Tender Documents and Electronic Form (for Technical details) and Electronic Form (for Financial details). In addition, the concerned Buyer organization should have Procurement Policy & Procedures to implement the other requirements	In addition, audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.
156	**Maintenance contract:** Depending on the cost and nature of the goods to be purchased, it may also be necessary to enter into maintenance contract(s) of suitable period either with the supplier of the goods or with any other competent firm, not necessarily the supplier of the subject goods. Such maintenance contracts are especially needed for sophisticated and costly equipment and machinery. It may however be kept in mind that the equipment or machinery is maintained free of charge by the supplier during its warranty period or such other extended periods as the contract terms may provide and the paid maintenance should commence only thereafter.	e-procurement System should have functionality for inviting bids for such Maintenance contracts. In addition, the concerned Buyer organization should have Procurement Policy & Procedures to implement the other requirements	Functionality Verification/Testing In addition, audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.
157	**Bid security:** (i) To safeguard against a bidder's withdrawing or altering its bid during the bid validity period in the case of advertised or limited tender enquiry, Bid Security (also known as Earnest Money) is to be obtained from the bidders except those who are registered with the Central Purchase Organisation, National Small Industries Corporation (NSIC) or the concerned Ministry or Department. The bidders should be asked to furnish bid security along with their bids. Amount of bid security should ordinarily range between two percent to five percent of the estimated value of the goods to be procured. The exact amount of bid security should be determined accordingly by the Ministry or Department and indicated in the bidding documents. The bid security may be accepted in the form of Account Payee Demand Draft, Fixed Deposit Receipt, Banker's Cheque or Bank Guarantee from any of the commercial banks in an acceptable form, safeguarding the purchaser's interest in all	e-procurement System should have functionality for payment of Bid Security (ie Earnest Money Deposit) as per instructions of the Buyer, either online at the time of online bid-submission (subject to the payment limits of the Payment Gateway), or payable offline parallel to the online bid-submission before the bid-submission deadline. In the latter case, provision should be there to take the offline payment on record during the Public TOE. In addition, the concerned Buyer	Functionality Verification/Testing In addition, audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.

	respects. The bid security is normally to remain valid for a period of forty-five days beyond the final bid validity period. (ii) Bid securities of the unsuccessful bidders should be returned to them at the earliest after expiry of the final bid validity and latest on or before the 30th day after the award of the contract.	organization should have Procurement Policy & Procedures to implement the other requirements	
158	**Performance security:** (i) To ensure due performance of the contract, Performance Security is to be obtained from the successful bidder awarded the contract. Performance Security is to be obtained from every successful bidder irrespective of its registration status etc. Performance Security should be for an amount of five to ten per cent. of the value of the contract. Performance Security may be furnished in the form of an Account payee Demand Draft, Fixed Deposit Receipt from a Commercial bank, Bank Guarantee from a Commercial bank in an acceptable form safeguarding the purchasers' interest in all respects. (ii) Performance Security should remain valid for a period of sixty days beyond the date of completion of all contractual obligations of the supplier including warranty obligations. (iii) Bid security should be refunded to the successful bidder on receipt of Performance Security.	e-procurement System should have functionality for recording important milestones of Contract Execution which would include submission of Performance Security by the successful bidder(s) In addition, the concerned Buyer organization should have Procurement Policy & Procedures to implement the other requirements	Functionality Verification/Testing In addition, audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.
159	**(1) Advance payment to supplier:** Ordinarily, payments for services rendered or supplies made should be released only after the services have been rendered or supplies made. However, it may become necessary to make advance payments in the following types of cases: (i) Advance payment demanded by firms holding maintenance contracts for servicing of Air-conditioners, computers, other costly equipment, etc. (ii) Advance payment demanded by firms against fabrication contracts, turn-key contracts etc. Such advance payments should not exceed the following limits: (i) Thirty per cent. of the contract value to private firms; (ii) Forty per cent. of the contract value to a State or Central Government agency or a Public Sector Undertaking; or (iii) In case of maintenance contract, the amount should not exceed the amount payable for six months under the contract.	e-procurement System should have functionality for recording important milestones of Contract Execution which would include Advance Payments and other payments made to the successful bidder(s)/ suppliers. In addition, the concerned Buyer organization should have Procurement Policy & Procedures to implement the other requirements	Functionality Verification/Testing In addition, audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.

	Ministries or Departments of the Central Government may relax, in consultation with their Financial Advisers concerned, the ceilings (including percentage laid down for advance payment for private firms) mentioned above. While making any advance payment as above, adequate safeguards in the form of bank guarantee etc. should be obtained from the firm. **(2) Part payment to suppliers:** Depending on the terms of delivery incorporated in a contract, part payment to the supplier may be released after it dispatches the goods from its premises in terms of the contract.		
160	**Transparency, competition, fairness and elimination of arbitrariness in the procurement process:** All government purchases should be made in a transparent, competitive and fair manner, to secure best value for money. This will also enable the prospective bidders to formulate and send their competitive bids with confidence. Some of the measures for ensuring the above are as follows: (i) The text of the bidding document should be self-contained and comprehensive without any ambiguities. All essential information, which a bidder needs for sending responsive bid, should be clearly spelt out in the bidding document in simple language. The bidding document should contain, inter alia; (a) The criteria for eligibility and qualifications to be met by the bidders such as minimum level of experience, past performance, technical capability, manufacturing facilities and financial position etc.; (b) Eligibility criteria for goods indicating any legal restrictions or conditions about the origin of goods etc. which may be required to be met by the successful bidder; (c) The procedure as well as date, time and place for sending the bids; (d) Date, time and place of opening of the bid; (e) Terms of delivery; (f) Special terms affecting performance, if any. (ii) Suitable provision should be kept in the bidding document to enable a bidder to question the bidding conditions, bidding process and/ or rejection of its bid. (iii) Suitable provision for settlement of disputes, if any, emanating from the resultant contract, should be kept in the bidding document. (iv) The bidding document should indicate clearly	e-procurement System should have functionality to ensure transparency, accountability, fairness and elimination of arbitrariness in the procurement process. This should be ensured by e-procurement system strictly and satisfactorily addressing the various issues especially outlined in Annexure-I of these Guidelines. Specifically for fairness it must be ensured that the e-procurement system supports all legitimate processes and methodologies for inviting bids in a transparent manner, and under no circumstances should the confidentiality of the bid be compromised before the Online Public Tender Opening Event. Importantly, a properly conducted Public Tender Opening Event is the backbone of transparency in public procurement. The e-procurement system must have a very transparent and comprehensive Online Public Tender Opening Event with simultaneous	Functionality Verification/Testing In addition, Audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.

	that the resultant contract will be interpreted under Indian Laws. (v) The bidders should be given reasonable time to send their bids. (vi) The bids should be opened in public and authorised representatives of the bidders should be permitted to attend the bid opening. (vii) The specifications of the required goods should be clearly stated without any ambiguity so that the prospective bidders can send meaningful bids. In order to attract sufficient number of bidders, the specification should be broad based to the extent feasible. Efforts should also be made to use standard specifications which are widely known to the industry. (viii) Pre-bid conference: In case of turn-key contract(s) or contract(s) of special nature for procurement of sophisticated and costly equipment, a suitable provision is to be kept in the bidding documents for a pre-bid conference for clarifying issues and clearing doubts, if any, about the specifications and other allied technical details of the plant, equipment and machinery projected in the bidding document. The date, time and place of pre-bid conference should be indicated in the bidding document. This date should be sufficiently ahead of bid opening date. (ix) Criteria for determining responsiveness of bids, criteria as well as factors to be taken into account for evaluating the bids on a common platform and the criteria for awarding the contract to the responsive lowest bidder should be clearly indicated in the bidding documents. (x) Bids received should be evaluated in terms of the conditions already incorporated in the bidding documents; no new condition which was not incorporated in the bidding documents should be brought in for evaluation of the bids. Determination of a bid's responsiveness should be based on the contents of the bid itself without recourse to extrinsic evidence. (xi) Bidders should not be permitted to alter or modify their bids after expiry of the deadline for receipt of bids. (xii) Negotiation with bidders after bid opening must be severely discouraged. However, in exceptional circumstances where price negotiation against an ad-hoc procurement is necessary due to some unavoidable circumstances, the same may be resorted to only with the lowest evaluated responsive bidder. (xiii) In the rate contract system, where a number	online presence of authorized representatives of bidders, and to eliminate arbitrariness each opened bid should be countersigned by the TOE-officers in the simultaneous online presence of the authorized bidders. In addition, authorized representatives of bidders may also be present offline during a TOE. However, to eliminate any arbitrariness and any doubt about tampering, the simultaneous online presence of bidders during TOE is important. Bidders may have doubts about the transparency of the process if the bids are opened by the Buyer independently in the backend (ie without the simultaneous online presence of bidders), and then subsequently displayed to the bidders. For comparison, this would tantamount to bids being opened by the Buyer in another room (where the bidders are not present), and then brought to a second room where the bidders are waiting. This is obviously not a transparent public opening, and so it is not acceptable. Furthermore, e-procurement system should allow submission of Modification/ Substitution/ Withdrawal of bids only till the bid-	

	of firms are brought on rate contract for the same item, negotiation as well as counter offering of rates are permitted with the bidders in view and for this purpose special permission has been given to the Directorate General of Supplies and Disposals (DGS&D). (xiv) Contract should ordinarily be awarded to the lowest evaluated bidder whose bid has been found to be responsive and who is eligible and qualified to perform the contract satisfactorily as per the terms and conditions incorporated in the corresponding bidding document. However, where the lowest acceptable bidder against ad-hoc requirement is not in a position to supply the full quantity required, the remaining quantity, as far as possible, be ordered from the next higher responsive bidder at the rates offered by the lowest responsive bidder. (xv) The name of the successful bidder awarded the contract should be mentioned in the Ministries or Departments notice board or bulletin or web site	submission deadline. To further eliminate arbitrariness, the e-procurement system should have comprehensive electronic-forms for capturing specific data requirements of each tender, and detailed response from each bidder to General Terms & Conditions (GTC) and Special Terms & Conditions (STC). Where required, functionality of the e-procurement system should be supplemented with Procurement Policy & Procedures internal to the Buyer organization.	
161	**Efficiency, Economy and Accountability in public procurement system:** Public procurement procedure is also to ensure efficiency, economy and accountability in the system. To achieve the same, the following keys areas should be addressed: (i) To reduce delay, appropriate time frame for each stage of procurement should be prescribed by the Ministry or Department. Such a time frame will also make the concerned purchase officials more alert. (ii) To minimise the time needed for decision making and placement of contract, every Ministry/ Department, with the approval of the competent authority, may delegate, wherever necessary, appropriate purchasing powers to the lower functionaries. (iii) The Ministries or Departments should ensure placement of contract within the original validity of the bids. Extension of bid validity must be discouraged and resorted to only in exceptional circumstances. (iv) The Central Purchase Organisation (e.g. DGS&D) should bring into the rate contract system more and more common user items which are frequently needed in bulk by various Central Government departments. The Central Purchase Organisation (e.g. DGS&D) should also ensure	For accountability, e-procurement system should have a comprehensive Hierarchy and Role Authorization of officers with detailed Audit Trails as outlined in Annexure-I of these Guidelines. Where required, functionality of the e-procurement system should be supplemented with Procurement Policy & Procedures internal to the Buyer organization.	Functionality Verification/Testing In addition, Audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.

	that the rate contracts remain available without any break.		
162	**Buy-back offer:** When it is decided with the approval of the competent authority to replace an existing old item(s) with a new and better version, the department may trade the existing old item while purchasing the new one. For this purpose, a suitable clause is to be incorporated in the bidding document so that the prospective and interested bidders formulate their bids accordingly. Depending on the value and condition of the old item to be traded, the time as well as the mode of handing over the old item to the successful bidder should be decided and relevant details in this regard suitably incorporated in the bidding document. Further, suitable provision should also be kept in the bidding document to enable the purchaser either to trade or not to trade the item while purchasing the new one.	e-procurement System should have functionality where 'Buy Back Price' should also be captured in the Financial-Bid and provision should be there for 'Net Procurement Price' after taking into account the 'Buy Back Price'	Functionality Verification/Testing
	B) Procurement of Services Rule 163 to 177		
163	The Ministries or Departments may hire external professionals, consultancy firms or consultants for a specific job, which is well defined in terms of content and time frame for its completion or outsource certain services.	Procurement Policy & Procedures internal to the Buyer organization Note: Generally no specific requirements for e-procurement.	Process Audit
164	This chapter contains the fundamental principles applicable to all Ministries or Departments regarding engagement of consultant(s) and outsourcing of services.	-	-
165	**Identification of Work/ Services required to be performed by Consultants:** Engagement of consultants may be resorted to in situations requiring high quality services for which the concerned Ministry/ Department does not have requisite expertise. Approval of the competent authority should be obtained before engaging consultant(s).	e-procurement System should functionality for obtaining approval of an Indent or Requisition Note for engagement of consultants with provision for recording relevant justification.	Functionality Verification/Testing
166	**Preparation of scope of the required work/ service:** The Ministries/ Departments should prepare in simple and concise language the requirement, objectives and the scope of the assignment. The eligibility and pre-qualification criteria to be met by the consultants should also be clearly identified at this stage.	e-procurement System should functionality for obtaining approval of an Indent or Requisition Note for engagement of consultants with provision for recording relevant justification.	Functionality Verification/Testing
167	**Estimating reasonable expenditure:** Ministry or Department proposing to engage	e-procurement System should functionality for	Functionality Verification/Testing

	consultant(s) should estimate reasonable expenditure for the same by ascertaining the prevalent market conditions and consulting other organisations engaged in similar activities.	obtaining approval of an Indent or Requisition Note for engagement of consultants with provision for recording relevant justification with estimated expenditure.	
168	**Identification of likely sources:** (i) Where the estimated cost of the work or service is upto Rupees twenty-five lakhs, preparation of a long list of potential consultants may be done on the basis of formal or informal enquiries from other Ministries or Departments or Organisations involved in similar activities, Chambers of Commerce & Industry, Association of consultancy firms etc. (ii) Where the estimated cost of the work or service is above Rupees twenty-five lakhs, in addition to (i) above, an enquiry for seeking 'Expression of Interest' from consultants should be published in at least one national daily and the Ministry's web site. The web site address should also be given in the advertisements. Enquiry for seeking Expression of Interest should include in brief, the broad scope of work or service, inputs to be provided by the Ministry or Department, eligibility and the pre-qualification criteria to be met by the consultant(s) and consultant's past experience in similar work or service. The consultants may also be asked to send their comments on the objectives and scope of the work or service projected in the enquiry. Adequate time should be allowed for getting responses from interested consultants	e-procurement System should have functionality for inviting 'Expression of Interest (EOI)' through Limited or Open Invitation, with other functionality as applicable for Limited and Open Tenders. This could be done through first Inviting Applications for Pre-qualification followed by Bidding, or directly inviting Bids in one or two envelopes. Where required, functionality of the e-procurement system should be supplemented with Procurement Policy & Procedures internal to the Buyer organization.	Functionality Verification/Testing of related 'features' and 'explanations' given by the e-procurement/ e-tendering software/ service provider against relevant sections and points of Annexure-I. In addition, Audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.
169	**Short listing of consultants:** On the basis of responses received from the interested parties as per **Rule 168 above**, consultants meeting the requirements should be short listed for further consideration. The number of short listed consultants should not be less than three.	e-procurement System should have functionality for short listing consultants who have been found to be eligible after the first round/ pre-qualification. Where required, functionality of the e-procurement system should be supplemented with Procurement Policy & Procedures internal to the Buyer organization.	Functionality Verification/Testing In addition, Audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.
170	**Preparation of Terms of Reference (TOR):** The TOR should include: 1. Precise statement of objectives; 2. Outline of the tasks to be carried out;	e-procurement System should have functionality for including in the Request for Proposal (RFP)	Functionality Verification/Testing

	3. Schedule for completion of tasks; 4. The support or inputs to be provided by the Ministry or Department to facilitate the consultancy; 5. The final outputs that will be required of the Consultant.	documents, the detailed Terms of Reference (TOR)	
171	**Preparation and issue of Request for Proposal (RFP):** RFP is the document to be used by the Ministry/ Department for obtaining offers from the consultants for the required work/ service. The RFP should be issued to the shortlisted consultants to seek their technical and financial proposals. The RFP should contain: 1. A letter of Invitation 2. Information to Consultants regarding the procedure for submission of proposal 3. Terms of Reference (TOR) 4. Eligibility and pre-qualification criteria in case the same has not been ascertained through Enquiry for Expression of Interest (EOI) 5. List of key position whose CV and experience would be evaluated 6. Bid evaluation criteria and selection procedure 7. Standard formats for technical and financial proposal 8. Proposed contract terms 9. Procedure proposed to be followed for midterm review of the progress of the work and review of the final draft report	e-procurement System should have functionality for creating detailed Request for Proposal (RFP) and posting this on the e-procurement system website with allied functionality for Corrigenda and Addenda to RFP. The functionality should also include creation of Electronic Forms to capture precise data in the application/ bid submitted by each consultant. Where required, functionality of the e-procurement system should be supplemented with Procurement Policy & Procedures internal to the Buyer organization.	Functionality Verification/Testing of related 'features' and 'explanations' given by the e-procurement/ e-tendering software/ service provider against relevant sections and points of Annexure-I. In addition, Audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.
172	**Receipt and opening of proposals**: Proposals should ordinarily be asked for from consultants in 'Two-bid' system with technical and financial bids sealed separately. The bidder should put these two sealed envelopes in a bigger envelop duly sealed and submit the same to the Ministry or Department by the specified date and time at the specified place. On receipt, the technical proposals should be opened first by the Ministry or Department at the specified date, time and place.	e-procurement System should have functionality for inviting 'Single Stage Two Envelope' tenders, or Two-Stage tenders (as mentioned in CVC guidelines), with secure methodology for sealing bids (ie data encryption of both the 'Technical', as well as, 'Financial' bid parts by the bidder himself before bid-submission. In addition, there should be functionality for opening only the technical bids first; functionality for creating a short-list of technically responsive	Functionality Verification/Testing of related 'features' and 'explanations' given by the e-procurement/ e-tendering software/ service provider against relevant sections and points of Annexure-I.

		bidders; functionality for a second tender opening event for opening the financial bids of the technically responsive bidders	
173	**Late bids:** Late bids i.e. bids received after the specified date and time of receipt should not be considered.	e-procurement System should have functionality for 'Not Accepting Late Bids'	Functionality Verification/ Testing
174	**Evaluation of technical bids:** Technical bids should be analysed and evaluated by a Consultancy Evaluation Committee (CEC) constituted by the Ministry or Department. The CEC shall record in detail the reasons for acceptance or rejection of the technical proposals analysed and evaluated by it.	In the e-procurement System after the TOE in which the Technical-Bids are opened, functionality should exist for members of Consultancy Evaluation Committee (CEC) to access the Technical-Bids for evaluation with provision to record recommendations.	Functionality Verification/ Testing
175	**Evaluation of financial bids of the technically qualified bidders:** The Ministry or Department shall open the financial bids of only those bidders who have been declared technically qualified by the Consultancy Evaluation 69 Committee as per **Rule 174** above for further analysis or evaluation and ranking and selecting the successful bidder for placement of the consultancy contract.	In the e-procurement System after the TOE in which the Financial-Bids of the technically qualified bidders are opened, functionality should exist for members of Consultancy Evaluation Committee (CEC) to access the Financial-Bids for evaluation with provision to record recommendations.	Functionality Verification/ Testing
176	**Consultancy by nomination:** Under some special circumstances, it may become necessary to select a particular consultant where adequate justification is available for such single-source selection in the context of the overall interest of the Ministry or Department. Full justification for single source selection should be recorded in the file and approval of the competent authority obtained before resorting to such single-source selection.	Procurement Policy & Procedures internal to the Buyer organization Note: Generally no specific requirements for e-procurement.	Process Audit
177	**Monitoring the contract:** The Ministry/ Department should be involved throughout in the conduct of consultancy, preferably by taking a task force approach and continuously monitoring the performance of the consultant(s) so that the output of the consultancy is in line with the Ministry	e-procurement System should have functionality for monitoring performance of a consultant, which would include recording of important parameters/	Functionality Verification/Testing In addition, audit of the Procurement Policy & Procedures of the

	/Department's objectives.	mile-stones relating the consultant's performance. In addition, the concerned Buyer organization should have Procurement Policy & Procedures to implement the other requirements	concerned Buyer organization can be carried out.
	C) Outsourcing of Services: Rule 178 to 185		
178	**Outsourcing of Services:** A Ministry or Department may outsource certain services in the interest of economy and efficiency and it may prescribe detailed instructions and procedures for this purpose without, however, contravening the following basic guidelines.	Procurement Policy & Procedures internal to the Buyer organization Note: Generally no specific requirements for e-procurement.	Process Audit
179	**Identification of likely contractors:** The Ministry or Department should prepare a list of likely and potential contractors on the basis of formal or informal enquiries from other Ministries or Departments and Organisations involved in similar activities, scrutiny of 'Yellow pages', and trade journals, if available, web site etc.	e-procurement System should have functionality for creating Classified Lists of likely and potential contractors. Also functionality should exist for a Buyer organization to Create/ Manage Contractor organizations under different Heads and Grades	Functionality Verification/Testing
180	**Preparation of Tender enquiry:** Ministry or Department should prepare a tender enquiry containing, inter alia : (i) The details of the work or service to be performed by the contractor; (ii) The facilities and the inputs which will be provided to the contractor by the Ministry or Department; (iii) Eligibility and qualification criteria to be met by the contractor for performing the required work / service; and (iv) The statutory and contractual obligations to be complied with by the contractor.	e-procurement System should have functionality for creating and managing Tender Notices, Corrigenda, Tender Documents, Addenda; floating Open Tenders, as well as, Limited Tenders; and functionality for other associated processes In addition, the concerned Buyer organization should have Procurement Policy & Procedures to implement the other requirements	Functionality Verification/Testing of related 'features' and 'explanations' given by the e-procurement/ e-tendering software/ service provider against relevant sections and points of Annexure-I In addition, Audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.
181	**Invitation of Bids:** (a) For estimated value of the work or service upto Rupees ten lakhs or less: The Ministry or Department should scrutinise the preliminary list of likely contractors as identified as per **Rule 179** above, decide the	e-procurement System should have functionality for creating and managing Tender Notices, Corrigenda, Tender Documents, Addenda;	Functionality Verification/Testing of related 'features' and 'explanations' given by the e-procurement/ e-

	prima facie eligible and capable contractors and issue limited tender enquiry to them asking for their offers by a specified date and time etc. as per standard practice. The number of the contractors so identified for issuing limited tender enquiry should not be less than six. **(b)** For estimated value of the work or service above Rupees ten lakhs: The Ministry or Department should issue advertised tender enquiry asking for the offers by a specified date and time etc. in at least one popular largely circulated national newspaper and web site of the Ministry or Department.	floating Open Tenders, as well as, Limited Tenders; and functionality for other associated processes In addition, the concerned Buyer organization should have Procurement Policy & Procedures to implement the other requirements	tendering software/ service provider against relevant sections and points of Annexure-I In addition, Audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.
182	**Late Bids:** Late bids i.e. bids received after the specified date and time of receipt should not be considered.	e-procurement System should have functionality for 'Not Accepting Late Bids'	Functionality Verification/Testing
183	**Evaluation of Bids Received:** The Ministry or Department should evaluate, segregate, rank the responsive bids and select the successful bidder for placement of the contract.	In the e-procurement System after the TOE in which the Bids are opened, functionality should exist for members of the Evaluation Committee (EC) to access the Bids for evaluation with provision to record recommendations.	Functionality Verification/ Testing
184	**Outsourcing by Choice:** Should it become necessary, in an exceptional situation to outsource a job to a specifically chosen contractor, the Competent Authority in the Ministry or Department may do so in consultation with the Financial Adviser. In such cases the detailed justification, the circumstances leading to the outsourcing by choice and the special interest or purpose it shall serve shall form an integral part of the proposal.	Procurement Policy & Procedures internal to the Buyer organization Note: Generally no specific requirements for e-procurement.	Testing & Audit
185	**Monitoring the Contract:** The Ministry or Department should be involved throughout in the conduct of the contract and continuously monitor the performance of the contractor.	e-procurement System should have functionality for recording important milestones of Contract Execution. In addition, the concerned Buyer organization should have Procurement Policy & Procedures to implement the other requirements	Functionality Verification/Testing In addition, audit of the Procurement Policy & Procedures of the concerned Buyer organization can be carried out.

Annexure-IV - Checklist for Compliance with IT ACT (IT ACT 2000 and Amendment 2008)

Sl. No.	Issues to be Checked	IT ACT Reference	Means of Checking
1	Electronic Signature Implementation: i) ESC (Electronic Signature Certificate) used for the e-Procurement System by the users are Issued by CC(Certifying Authority) recognized by Govt. of India CCA(Controller of Certifying Authority). ii) The private key or the signature creation data should not be stored in the e-Procurement System or kept under the control of the e-Procurement Service Provider. iii) By the use of a public key of the subscriber/ signer, it should be possible to verify the electronic record. This may be read in conjunction with Sch-2, 13 85B(2)(b) "except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature". (*Explanation*: This implies that important electronic records of an e-procurement application, like – Tender Notice, Corrigenda, Tender Documents, Addenda, Clarifications to Tender Documents, Bids, etc should not only be electronically signed, there should also be provision in the e-procurement application to verify the electronic signatures). iv) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure (*Explanation*: There should be no limitation in the functionality of the e-procurement system which may necessitate for the tendering processes to continue uninterrupted that the private key of any officer be handed over to anybody else (who may be absent or unavailable), or where a private key is shared by multiple users due to any reason such as – absence of detailed hierarchy within a user organization, or multiple users of a group using a common key. v) Similarly, functionality of the e-procurement system should cover other aspects outlined in various sections (specified in the adjacent	3, 3A, 5, 6, 15, 42, Ch-VI; Sch-2, 13	Verification of Implementation/ Functionality and the ESC used.

	column) of the IT Act.		
2	Electronic Document & Record Control: Suitable controls are established for electronic documents /records generated, processed, stored, disposed of by the e-Procurement System to comply i) The information contained in e-Documents/e-Records remains accessible/usable for subsequent reference; ii) The e-Records are retained in the original format, it was generated, to accurately demonstrate how it was generated/sent/received. iii) The e-Records should be maintained with identification of origin, destination, date and time of dispatch or receipt. iv) The retention period of the e-Records should be compliant with the legal and contractual requirements.	7	Verification of policies, procedures, mechanisms and relevant records, and functionality of the e-procurement system.
3	Data Protection: i) Adequate and reasonable security practices and procedures are in place to protect confidentiality and integrity of the users data and credentials ii) The e-procurement system has to satisfactorily address the above) through suitable functionality built into the e-procurement application. Where, in addition, some issues are being further addressed through organizational procedures, these should be explicitly defined with satisfactory explanations. The reasonable security practices and procedures followed should be documented in line with the international standard ISO/IEC 27001.	43A, Draft rule under Section 43A	Verification of policies, procedures, mechanisms and relevant records, and functionality of the e-procurement system. (Some checks are covered in Annexure-I, II and III)
4	Due diligence exercise: i) The Service Provider shall publish the terms and conditions of use of its e-Procurement System, user agreement, privacy policy etc. ii) The Service Provider shall notify users not to use, display, upload, modify, publish, transmit, update, share or store any information that: (a) belongs to another person; (b) is harmful, threatening, abusive, harassing, blasphemous, objectionable, defamatory, vulgar, obscene, pornographic, pedophilic, libelous,	79, Draft rule under Section 79	Verification of the terms and conditions of use of the e-Procurement System, user agreement, privacy policy, and other notifications as mentioned.

	invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever; (c) harm minors in any way; (d) infringes any patent, trademark, copyright or other proprietary rights; (e) violates any law for the time being in force; (f) discloses sensitive personal information of other person or to which the user does not have any right to; (g) causes annoyance or inconvenience or deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature; (h) impersonate another person; (i) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource; (j) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any other nation. iii) The Service Provider shall not itself host or publish or edit or store any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in (ii) above. iv) The Service Provider shall inform its users that in case of non-compliance with terms of use of the services and privacy policy provided by the Service Provider, it has the right to immediately terminate the access rights of the users to the e-Procurement System. v) The Service Provider shall publish on the e-Procurement website about the designated agent to receive notification of claimed infringements.		

Reference Documents

Reference Document – 1
eTendering Processes

e-tendering portal

- an e-tendering portal, or an e-tendering website, refers to an internet-based portal on which an e-tendering application software is hosted in a secure manner. One or more Government organizations register on the portal (as Buyer organizations). Various vendors also register on the portal (as Supplier organizations). A Buyer organization floats (i.e. invites) a tender on the portal, and Supplier organizations respond to such tenders. Depending on the functionality offered by an e-tendering portal, all the tendering related activities, from 'Indent Management (or Requisition Management)' to 'Award of Contract' can be carried out 'Online' over the Internet by a Buyer organization, and related activities by Supplier organizations.

Non-negotiable founding principles of Public Procurement like transparency, encouraging competitiveness and fair treatment to all etc.

- Switchover from manual system of tendering to electronic tendering or e-tendering is major change. Some 'process re-engineering' (i.e. change or improvement in the methodology of conducting various activities) becomes inevitable when changeover is made to a new technology, or a new method of working is adopted. However, while switching over to e-tendering, no compromise should be made by the Government organization on `Security and Transparency' related aspects of the Government Tendering Policy and Rules on the pretext of re-engineering.
- While switching over to e-tendering, a Government organization (in the role of a Buyer) which urges its Suppliers/Vendors to changeover to e-tendering, should ensure that the e-tendering portal also takes care of the Supplier organizations needs for security and transparency, and that suppliers are given reasonable time to change-over in a phased manner.

core activities related to tendering

- From a Buyer's perspective, `core activities related to tendering' refers to activities like-raising indents (or requisitions) for procuring some item or service, approving such requisitions, configuring the e-tendering system to act as per that organisation's tendering policy, creating a hierarchy of officers with specific authorizations to manage and control activities related to e-tendering for various tenders, configuring the e-tendering system to act as per specific rules for a given tender, creating a list of bidders to be invited for a `limited tender', creating a tender notice, approving a tender notice, authorizing issue of corrigenda , creating corrigenda, approving tender documents, authorizing issue of addenda, approving addenda, furnishing clarifications to tender documents, conducing online public tender opening event(s) and sharing salient points of each bid with all participating bidders, counter-signing each opened bid during tender opening event, evaluating the bids which have been opened, creating a list of bidders for the next stage (where applicable). From a Supplier's (or Vendor's perspective), `core tendering activities' or `core activities related to tendering' refers to activities relating to responding to various tenders. These include-creating a hierarchy of executives with specific authorizations to manage and control activities related to e-tendering for various tenders, procuring tender documents for a tender, seeking clarifications to tender documents, preparing a bid in multiple parts(as required by the Buyer) and required), attending online public tender opening event(s).

Operating Models for e-Tendering

A variety of `Operating Models' have emerged through which e-tendering services are currently being offered. Some prominent models are - `Dedicated e-Tendering Portals' (also referred to as Captive e-Tendering Portals), `Shared e-Tendering Portals' [ where services are offered in ASP (Application Service Provider) mode/SaaS (Software as a Service) mode, and different types of `Outsourcing Models'. Also, it is important to differentiate between the concepts of the portal. In view of the emphasis on Security and Transparency in Public-Procurement, the acceptability of these models varies. Guidelines are as follows:

A) (Dedicated e-Tendering Portals)- where the Government organization wishing to do e-tendering, owns and controls the portal infrastructure, and also controls all the core tendering activities carried out on the portal.

- A Government organization wishing to set up a dedicated e-tendering portal for its tendering requirements should float an `Open Tender' for selecting a suitable vendor. It should not resort to by-passing of the tendering process on the grounds, that as a Buyer organization it has been offered the service free of charge or at nominal charge, and only Suppliers or Vendors have to pay to the Service Provider or the Supplier of the e-tendering software, as the case may be. In situations like this, as in the case of infrastructure projects, the total revenue which accrues to the Service provider of the e-tendering portal should be considered, viz revenue from the Buyer organization(s), revenue from registration of Supplier organizations which will register on the portal at the behest of that Buyer organization, and any other sources of revenue.

B) (Use of a Shared e-Tendering Portal)- where the Government organization wishing to do e-tendering controls all the core tendering activities of its organization carried out on the portal, but where ownership and control of the portal infrastructure is with the Service Provider.

- A Government organization wishing to use an existing e-tendering portal on shared basis for its tendering requirements may float a tender for the purpose of selecting a suitable Service Provider. In such situations, the nomination route may be used if both the following conditions are satisfied.
  - i) The total annual revenue which accrues to the Service Provider from that Government organization and its Suppliers who register specifically at the behest of that Government organization is less than Rs. Five/ten lakhs a year. (Note: Limit to be defined by the appropriate Govt body keeping in view Finance Ministry's current limit of Rs. Ten lakhs for consultancy service through the nomination route). For this purpose, revenue should include registration and portal usage charges of the Buyer organization, registration charges of supplier organizations which register at the behest of that buyer organization, and portal-usage charges of the aforesaid supplier organizations specifically in respect of responding to tenders of that Buyer organization.
  - ii) The arrangement of that Government organization with the Service Provider is on a `non-exclusive' basis.

C) (Outsourcing Model-1): The Government organization outsources its tendering activities to a Service Provider. The control of all or most of the core tendering activities is in the hands of the Service Provider. The Service Provider also owns and controls the portal infrastructure.

(Outsourcing Model 2): The government organization procures and owns partially or fully the portal infrastructure, but does not manage it. Furthermore, the Government organization outsources the management and control of its tendering activities to a Service Provider.

It is important to note that `Outsourcing' as outlines above is substantively distinct from `Use of a Shared e-Tendering Portal' as outlined in (ii) B above. In case of the `Shared e-Tendering Portal, the Government organization wishing to so e-tendering controls all the core tendering activities of its organization carried out on the portal.

In case of `outsourcing' since `complete control is in the hands of a third party Service Provider', number of `legal' and `security' related issues arise. Some of these issues are:

i) `Tendering' is a sensitive activity, where integrity and transparency of the procurement process is on paramount importance. Can such a sensitive activity be outsourced to a third party Service Provider (who in turn may be a public sector entity, or a private entity) where `complete control is in the hands of the third party Service Provider'?

ii) In case of a Government organization, the officers authorized for `tendering' are legally accountable under the official Secrets Act'. Certain Standards of propriety, integrity and confidentiality are expected of Government officers and Government departments. How will this be ensured from personnel of a third party private Service Provider, who would gain complete control of the tendering activities under the outsourcing-contract?

iii) Guidelines pertaining Access to the e-Tendering Portal:

- Access shall be provided to the general public for viewing `tendering opportunities' (i.e. Tender Notices) posted on the e-tendering portal for all `Open Tenders', as well as `Limited Tenders' (the exception in case of Limited Tenders is where due to reasons of national security it is expedient not to do so). Access shall imply-viewing a Tender Notice, searching a Tender Notice with its reference number, or name of the Buyer organization.
- Access shall be provided to the general public for accessing any other `Public Information' sections of the e-tendering portal, such as – Information pertaining to forthcoming Tendering Opportunities, Information pertaining to `Award of Contracts i.e. Purchase Orders'.

iv) Guidelines pertaining use of Digital Signatures, IT Act 2000 and Phased Approach:

- Any e-tendering portal to be used by a Government organization must allow the users of the portal to use any one Digital Certificate (Digital Signature) issued by any Certifying Authority licensed by the CCA subject to other conditions of the Digital Certificate issuing authority.

- The Digital Signature (i.e. Private Key) cannot be handed over by the owner of that key to any other person. (It has been observed that in some e-tendering portals, the private digital keys of the authorized officers are handed over to the staff of the service provider, or the keys are freely exchanged amongst the users. This practice should be stopped forthwith).
- No technology should be forced on the users suddenly. A phased approach must be adopted. Specifically in case of e-tendering, unless a large number of users are comfortable with use of Digital Signatures, there is no point forcing them to deal with more sophisticated features like online bid-submission involving encryption of bids etc. (It has been observed that in some e-tendering portals that the staff of the Service Provider have been encrypting bids on behalf of the bidders and conducting the Tender Opening Events on behalf of the authorized Government officers.
- All Digital Signature Certificates should be PKI based and issued by a Certifying Authority duly licensed by the CCA.
- Compliance with IT Act 2000: Vendors of e-tendering portals, or-tendering software, should be specifically instructed to keep in view s-42 (1), and s-85B2(b) of the IT Act 2000 while giving a `confirmation of compliance with the IT Act 2000'.
- To avoid compromise of security (i.e. compromise of private key in this context), users of an e-tendering portal should not obtain `pre-prepared' digital certificates' through the service provider or any other source. The digital certificate should be generated by the concerned user (i.e. the applicant of the digital certificate) himself, preferably on his own computer, and securely stored under a password

Reference Document – 2
Electronic Tendering Glossary

Information Entity	Definition
Goods	The supply of Goods with minimal Labour
Invitation to Tender	A request by procuring entity to contractors of commercial offer for the entity to appoint a contractor to execute the works
Open Tender	All interested suppliers may submit a tender
Opening of tenders	Tenders shall be opened under procedures and conditions guaranteeing the regularity of the openings
Optional Contract	Procuring entity identifies a tenderer who has suitable assets, repute and ability and then contracts with it as its discretion
Registration	A system to ensure that tenders are sought only from contracts whom the procuring entity has already established as having the requisite resources and experience to perform the intended work satisfactorily.
Public Invitation	An invitation to participate in intended procurement published by procuring entities. The notice shall be published in the appropriate publication
Selective Tender	Suppliers invited to do so by the procuring entity may submit a tender
Services	The supply of Services, mainly Intellectually based Labour
Tender	The letter of Tender and all other documents which the Contractor submitted with the Letter of Tender, as included in the Contract.
Tender Documents	Documents which should be issued by the procuring entity to those firms who have been selected to tender, or who wish to tender in case of an Open tender
Tenderer	Firm answering an invitation to tender
Tender Result Notice	Procuring entity creates tender result notice, issues it to tenders
Contract Award Publication	Procuring entity publishes the contract award
Qualification	Procuring entity verifies tender participation qualification of tenders
Works	The supply of Labour, Materials and associated Plant.

Reference Document – 3

OWASP(Open Web Application Security Project) Top 10 Application Security Risks-2010

A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted 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.
A2-Cross Site Scripting (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.
A3-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.
A4-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.
A5-Cross Site Request Forgery (CSRF)	A 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 the vulnerable application thinks are legitimate requests from the victim.
A6-Security Misconfiguration	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.
A7-Insecure Cryptographic Storage	Many web applications 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.
A8-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.
A9-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.
A10-Unvalidated 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.

Reference document – 4

Business requirements specification- cross industry e-Tendering process (Source CWA 15666)

To attain the objective of interoperability and compatibility of various solutions, both at buyer and supplier end it is required that processes and information entities shall be standardized across industrial electronic tendering. Following are the business requirements for the same.

Business Process Elaboration

- E-Tendering
- Registration
- Public Invitation
- Tender/Opening of Tenders
- Publication of Award

Business Information Flow Definition

- Submit Registration Application
- Issue Examination Result Notification
- Publish prior information notice
- Publish invitation to tender
- Submit pre-qualification application
- Issue letter of invitation to tender
- Request Tender Information
- Issue tender information
- Issue tender guaranty
- Submit the response of tender guaranty
- Submit tender
- Submit qualification and application
- Issue qualification result notice
- Issue tender result notice

Following are the process details:

Registration

Preconditions	None
Begins When	Tenderers apply for registration
Definitions	Tenderers apply for registration Procuring entity receives registration application Procuring entity examines registration application Procuring entity notifies tenderers of examination result Tenderers receive examination result

Public Invitation

Preconditions	Procuring entity has a tendering subject release invitation to tender
Begins When	Procuring entity establishes project strategy
Definition	Procuring entity establishes project strategy Procuring entity publishes invitation to tender If necessary, tenderers should be pre-qualified If necessary,procuring entity selects tenders

	When tenderers have intention to submit tenders • Tenderers request detailed information of the tendering subject • Procuring entity receives request for detailed information of the tendering subject • Procuring entity issues detailed information of the tendering subject to tenders • Tenders receive detailed information of the tendering subject
Ends When	Tenderers receive detailed information of the tendering subject
Exceptions	Procuring entity does not receive request for detailed information of the tendering subject by tenderers Tenderers do not receive detailed information of the tendering subject from procuring entity Tenderers have no intention to participate in tender
Post conditions	Tenderers get detailed information of the tendering subject

Tender/Opening of Tenders

Preconditions	Targeted tendering subject is within submission period of tenders Tenderers receive detailed information of the tendering subject
Begins When	Tenderers submit tenders
Definitions	Tenderers submit tenders Procuring entity receives tenders Procuring entity opens tenders If necessary, procuring entity verifies qualification of the tenderer Procuring entity notifies tender result Tenders receive tender result
Ends When	Tenderers receive tender result
Exceptions	Procuring entity does not receive tenders from tenderers Tenderers do not receive tender result from procuring entity
Post conditions	Tenderers get details of tender result.

Publication of Award

Preconditions	Procuring entity notifies tender result to tenderers
Begins when	Procuring entity publishes tender result
Definitions	Procuring entity publishes tender result Note: This definitions are example of executing business collaborations within this business process
Ends When	Procuring entity publishes tender result
Exceptions	None
Postconditions	Procuring entity proves that the tender has been performed without injustice.

Templates & Forms

Template 1 : Defining Usability Requirement Specifications of the Software Product

USABILITY REQUIREMENTS SPECIFICATIONS OF < > SOFTWARE PRODUCT

1. **NAME AND PURPOSE OF THE PRODUCT :**

   < > is a web based eGovernance solution designed and developed for complete automation of the tendering/ procurement of materials, components, contracts, works and services.

   This specification defines the Usability requirements for < >software application

2. **CONTEXT OF USE**

   < >has the capability to support the complete tendering process which includes placing of on-line technical bids, commercial bids, facility for e-payment and secure opening of vendor bids with provision for interface to e-payment gateways and incorporating PKI enabled digital signatures.

   Fine details of tendering like creation of vendor database, tender announcement and corrigendum; tender offer processing, opening, negotiation, dynamic pricing mechanism, automatic generation of comparative statement of bids received tender awarding and management of tender contract operation and re-tendering are supported in a real time interactive environment. This system enables both procurers and vendors to interact with each other and transact business.

   a. Specification of users:

   Based on the analysis of the product, the main classes of users are

   - Department users (ie Buyers or Purchasers)
   - Portal/ e-Procurement Application Administrators (for Dedicated Portal of a Buyer)
   - Registered suppliers/ contractors/vendors
   - Portal/ e-Procurement Application Administrators (for Service Providers)

   Registered suppliers/ contractors/vendors

   i. Skills & knowledge –
      - Should be computer literate and in the habit of surfing the net
      - Should have Knowledge about tendering process

   ii. Training on the usage of software mandatory

   iii. Product Experience – Nil

   iv. Organizational experience – Nil

   v. Physical attributes – Normal

   Department Users (ie Buyers or Purchasers)

   i. Skills & knowledge –
      - Should be computer literate and in the habit of surfing the net
      - Should have Knowledge about tendering process

   ii. Training on the usage of software mandatory

   iii. Product Experience – Nil

   iv. Organizational experience – Required

   v. Physical attributes - Normal

b. Broad Specification of tasks

The major work flows analysed in terms of severity, criticality and frequency of use for the respective users are as given below :

Department Users

1. **Vendor Registration** specific to a particular Buyer/ Department- Any person who wants to bid for any tender of that Buyer/ Department, has first to register with the department (after having registered on the portal) . Where required, Department Administrator can create vendors
    a. They receive filled in application with credentials of the vendors , and then register them for a particular classification and grade
2. **The Tendering Creation** : Creation ,Uploading of tender and Authorizing the tender

3. **Tender Opening** - Tender Opening in the simultaneous online presence of authorized bidder representatives with additional optional offline presence, EMD Authorisation , countersigning of each opened bid in the simultaneous online presence of authorized bidder representatives, Downloading of submitted vendor documents , Disqualification of a vendor (i.e. archiving a bid unopened) and Comparative statement generation

    Sub activities: verification of documents and EMD/Bank Guarantee

Suppliers/ contractors/vendors

a. Self Registration on the e-procurement by the first user of an organization, and submission his Public Key

    Sub activities:

    i. Where required, registration by an authorized user for particular Department/ Buyer for a particular classification of trade, region and vendor class for a particular duration
    ii. Attachment of supporting documents required for the registration

b. PKI based login and Request/ Procurement of tender documents
c. Pre-qualification based on projects/tenders
d. Download tender documents/ addenda
e. Upload filled tender documents (ie bids, in envelopes and stages as instructed in the tender documents)

    Sub activities:

    i. Attachment of supporting documents required for the tender
    ii. Submission

c. Specification of environment

As this application is generally used in an office environment , testing can be done in an office ambience .

So the Usability Lab at < > can be used for carrying out the user tests .

3. SPECIFICATION OF MEASURES OF USABILITY FOR PARTICULAR CONTEXTS

Department Users

1. Vendor Registration
    a. **Effectiveness** (Accuracy & Completeness): All Vendor Registrations have been completed successfully .

b. **Efficiency**: Registration to be completed by the user within <10 minutes>.
c. **Satisfaction**: Less than 10% of users report dissatisfaction with the vendor registration procedures.

2. Generation of a tender- Creation
   a. **Effectiveness** (Accuracy & Completeness); All Tenders have been completed correctly and successfully .
   b. **Efficiency**: Tender Creation to be completed by the user within 10 minutes.
   c. **Satisfaction**: Less than 10% of users report dissatisfaction with the tender generation process.

3. Uploading of tender
   a. **Effectiveness** (Accuracy & Completeness): All tenders have been uploaded successfully.
   b. **Efficiency**: Uploading to be completed by the user within 3 minutes.
   c. **Satisfaction**: Less than 10% of users report dissatisfaction with the uploading procedures.

4. Opening of Tenders
   a. **Effectiveness** (Accuracy & Completeness): The opening of all tenders have been completed successfully .
   b. **Efficiency**: Opening of tenders to be completed by the user within 5 minutes.
   c. **Satisfaction**: Less than 10% of users report dissatisfaction with the tender opening procedures.

5. EMD Authorisation ,
   a. **Effectiveness** (Accuracy & Completeness): The EMD Authorisation of all tenders has been completed successfully.
   b. **Efficiency**: EMD Authorisation to be completed by the user within 1 minute
   c. **Satisfaction**: Less than 10% of users report dissatisfaction with the EMD Authorisation procedures.

6. Downloading of submitted vendor documents ,
   a. **Effectiveness** (Accuracy & Completeness) : The downloading of all submitted tenders have been completed successfully.
   b. **Efficiency**: Downloading of submitted vendor documents to be completed by the user within 5 minutes.
   c. **Satisfaction**: Less than 10% of users report dissatisfaction with the Downloading procedures.

7. Disqualification of one vendor
   a. **Effectiveness** (Accuracy & Completeness) Vendor Disqualification has been completed successfully.
   b. **Efficiency**: Disqualification of one vendor to be completed by the user within 3 minutes.
   c. **Satisfaction**: Less than 10% of users report dissatisfaction with the disqualification procedures.

8. Comparative statement generation
    a. **Effectiveness** (Accuracy & Completeness) Generation of Comparative statement has been completed successfully .
    b. **Efficiency**: Comparative statement generation to be completed by the user within 2 minutes.
    c. **Satisfaction**: Less than 10% of users report dissatisfaction with the Comparative statement procedures.

Suppliers/ contractors/vendors

1. Self Registration with PKI
    a. **Effectiveness** (Accuracy & Completeness) Self Registration with PKI has been completed successfully.
    b. **Efficiency**: Registration to be completed by the user within 12 minutes.
    c. **Satisfaction**: Less than 10% of users report dissatisfaction with the PKI registration procedures.
2. PKI based login and Request for tender documentation
    a. **Effectiveness** (Accuracy & Completeness) All Vendor requests have been completed successfully .
    b. **Efficiency**: Tender request to be completed by the user within 5 minutes.
    c. **Satisfaction**: Less than 10% of users report dissatisfaction with the Tender request procedures.
3. Downloading of tender documents
    a. **Effectiveness** (Accuracy & Completeness) All the tender documents have been downloaded successfully .
    b. **Efficiency**: Downloading of tender documents to be completed by the user within 3 minutes.
    c. **Satisfaction**: Less than 10% of users report dissatisfaction with the downloading procedures.
4. Upload filled tender documents, Supporting documents and Submission of tender
    a. **Effectiveness** (Accuracy & Completeness) All the tender documents have been uploaded and submitted successfully .
    b. **Efficiency**: Tender Submission to be completed by the user within 15 minutes.
    c. **Satisfaction**: Less than 10% of users report dissatisfaction with the whole tender submission procedures.

4. **Usability objective : Overall usability**

1. Effectiveness measures

    a. Percentage of goals achieved - 100%
    b. Percentage of users successfully completing task- 100%

2. Efficiency measures

    a. Average time to complete a task - less than 40 mts
    b. Average no of tasks completed per unit time - 0ne per 10 mts

3. Satisfaction measures

    a. Rating scale for satisfaction - more than 90%
    b. No of complaints - less than 10%

Template 2: - Defining Performance Specifications

To be provided by developer/user

- The application < Brief about application >
- The data model < Use of Data base and Data Architecture>
- The technology <Use of Technology e.g. Net, Oracle, SQL, Soft etc)
- The user profiles Type of User (Internal, External etc)
- The business requirements

Sl. No.	Characteristic/requirement	Supplied Data Value
1.	Type of user's (e.g. administrator/power user/user/guest etc. on the basis of access rights & frequency of use.	
2.	Type of activities to be performed by the users (Identify each activity/function)	
3.	No. of user's for each activity/function/scenario (with concurrent users/activities)	
4.	Response time for each activity/scenario (a) At normal load (b) At max. load	
5.	Total no. of Task (identify & list each task)	
6.	Response time for each task (c) At normal load (d) At max. load	
7.	Throughput (for each activity) in terms of Bytes/second or task/second or no. of tasks to be completed within a specified period (a) At normal load (b) At max. load	
8.	Turn-Around Time(activity wise) (a) At normal load (b) At max. load	
9.	I/O Devices (e.g. printer, Keyboard, Mouse, scanner, Modem etc.) (a) Utilization time for I/O devices (b) I/O error messages /warning /failure messages at max. load (c) Waiting time for I/O utilization at max. load	
10.	Memory Utilization (a) Memory utilization at max. load (b) Memory related error messages/warning/failure messages at max. load	
11	Transmission resources utilization (a) Specify the followings: i) Data transfer speed of network cable ii) NIC card iii) Modem iv) Hub, Switch and Router (b) Internet Service provider(e.g. ISDN dial-up/lease line with 64/128 KBPS) (c) No. of error messages at max. load (d) Transmission capacity at max. load	
12.	Compliance: Identify the activities /functions requiring conformance to standard (Organization specific/national/international), rules & regulations.	
	Signature of supplier/user: Place: Dated:	

Annexure V

Definitions and Reference Documents

- **E-Procurement**:- Electronic procurement (e-procurement) is use of electronic tools and systems to increase efficiency and reduce costs during each stage of the purchasing process
- **E-Sourcing**:- Electronic sourcing (esourcing) is the use of internet technology to establish, manage and monitor contracts. It includes:
  *eTendering
  * eEvaluation
  * eCollaboration, and
  * eContract Management
- **Public Service Organization (PSO)**:- An organization which provides service (s) to public at large and/or whose activities influences influence public interest.
  eg: Government ministries and departments, Regulatory bodies, Public utility service providers, etc.
- **Purchase Officer**:- A Purchase officer is an employee within Public service organization(Govt. Department/ Public Service Undertaking) who is responsible at some level for buying or approving the acquisition of goods and services needed by the organization. A Purchase Officer may oversee the acquisition of materials, general supplies for offices and facilities or equipment. The term Purchase Officer is also known as "Procurement Manager". They are overall responsible for building and managing their organization supply chains.
- **Service Provider**: - A service provider is an entity that provides services to other entities. In the context of this document Service Provider refers to a business that provides e-procurement services to the Public service organization (Govt. Department/ Public Sector Undertaking).
- **Solution Provider**:- A solution provider is a vendor, a service provider or a value-added reseller (VAR) that comprehensively handles the project needs of their client from concept to installation through support. This process normally involves studying the client's current infrastructure, evaluating the client's needs, specifying the mix of manufacturers' hardware and software required to meet project goals, installing the hardware and software at the client's site(s). In many cases, the "solution" also includes ongoing service and support from the VAR.
- **Senior Administrators**: Employee within Public service organization charged with improving their company's profits, responsiveness, and standing in the market.
  They are also termed as (Executive Director, Material Management or Chief Executive Officer) depending on the size of the organization.
- **Financial Advisor (CFO):-** Employee of Public service organization focused on controlling costs and optimizing their organization resources. They are also designated as Chief financial Advisors (CFO).
- **Head IT:**-Employee of Public Service Organization involved in selecting and implementing e-Governance in the P.S.O also Known as chief information officer. He is also responsible for managing consultants and system integrators (SI) tasked with identifying leading e-Procurement solutions.
- **Facility Management Partner (FMP):**- In some cases PSO's take services of Front end FMP's for implementation, operation, management and training of eProcurement Solution. PSO's outsourced the operation of the e-procurement solution through front end facility management partner

2.0 Reference Standards and Normative documents

- Application Security : OWASP-10, 2010
- Network Security as per NIST 800-115 Technical Guide to Information Security Testing and Assessment
- CWA (CEN Workshop Agreement 15994- e-Tendering Process)
- CWA (CEN Workshop Agreement 15666- Business requirements specification- Cross Industry e-Tendering Process)
- eProcurement Integrity Matrix from Transparency International India
- ISO / IEC 27001 Information Security Management System Requirements
- ISO/TS 15000 Electronic business eXtensible Markup Language (ebXML)
- IT Act 2000 with amendments 2008
- General Financial Rules, 2005
- Relevant CVC Guidelines