ENSURING 'UNQUESTIONABLE INTEGRITY' IN E-PROCUREMENT/ E-TENDERING SYSTEMS FOR PUBLIC-PROCUREMENT – A CHALLENGE FOR SUPREME AUDIT INSTITUTIONS

Jitendra Kohli

Jitendra Kohli, B.Tech (Electrical Engineering) from Indian Institute of Technology Delhi (IIT-Delhi, India), founder of ElectronicTender, has been researching in the 'Electronic-Government-Procurement (eGP)' field for over 24-years. Based on his pioneering work, his company, ElectronicTender, has developed an innovative e-procurement/ e-auction software with comprehensive security and transparency features which can be licensed for ready-deployment in any country. In public-interest, he has been sharing important aspects of his ground-breaking research in public domain through interaction with authorities in various countries (including India, and the European Union) and multi-lateral agencies, presentation of papers at international conferences, et al, so that the concerned authorities could take appropriate measures to check malpractices under the garb of e-procurement. In end-2011/ 2012, his services were commissioned by the Asian Development Bank for technical peer-review of the update of MDB's 'e-Procurement Toolkit'. Starting from IPPC5 at Seattle (USA), his papers relating to e-procurement have been published at all the IPPCs. In 2018, International Centre for Information Systems and Audit (iCISA), the International Training Centre of the 'Comptroller and Auditor General of India (India's Supreme Audit Institution)', invited him to write articles relating to e-procurement security/ audit aspects for being published in their biannual online journal on IT Audit named PursuIT. Both the 2018 issues of PursuIT published his articles under the section 'Audit Aids'.
(Jitendra Kohli can be contacted at – E-mail:
jkohli@electronictender.com; LinkedIn:
http://in.linkedin.com/in/jitendrakohli)

ABSTRACT:

Over the last decade or more, e-procurement/ e-tendering has become a popular methodology for conducting public-procurement in many countries. Technology being a dual-edged sword, malpractices that are prevalent in the traditional manual/ paper-based method of public procurement, such as compromising bid-confidentiality, bid rigging, non-transparent bid-opening, et al can continue even in the electronic versions,

unless the underlying web-application software has inbuilt functionality and checks to prevent such malpractices. Since e-procurement is relatively a new technology globally, it becomes a challenge for the Supreme Audit Institutions of a country to audit such systems, and to ensure that the systems being audited have -- foolproof bid-confidentiality, unquestionable transparency, accountability, supplemented with comprehensive audit-trails at various levels. The situation is compounded by the fact that e-procurement has variant forms, and one system may be different from another. The paper proposes a 'Model Framework for Auditing e-Procurement/ e-Tendering Systems to ensure Unquestionable Integrity in Public-Procurement'.

Key Words: e-procurement, e-tendering, public-procurement, eGP, e-procurement audit, audit-tools, supreme audit institution, CAG of India, iCISA, CVC of India.

INTRODUCTION

Objective of Government Auditing

It is the objective of the Supreme Audit Institution (SAI) of any country to supervise the management of public money. For example, the 'Mission' and 'Core values' statements of the Comptroller and Auditor General of India (CAG of India), which is the Supreme Audit Institution in India, read as follows –

"MISSION: Our mission enunciates our current role and describes what we are doing today: Mandated by the Constitution of India, we promote accountability, transparency and good governance through high quality auditing and accounting and provide independent assurance to our stakeholders, the Legislature, the Executive and the Public, that public funds are being used efficiently and for the intended purposes.

CORE VALUES: Our core values are the guiding beacons for all that we do and give us the benchmarks for assessing our performance, Independence, Objectivity, Integrity, Reliability, Professional Excellence, Transparency, Positive Approach" (CAG of India, 2016).

The Challenge of Auditing e-Procurement Systems

Typically, public-procurement constitutes 10% to 20% of the GDP of a country. Hence, in most countries, the need and importance for auditing systems and processes relating to public procurement would perhaps be the highest. For public-procurement done through manual/ paper-based methods in various countries, the auditing procedures and rules would generally be well established, based on historical best-practices that get fine-tuned with time.

However, e-procurement/ e-tendering is relatively new. It was around the year 2000 that e-procurement started getting promoted as an alternative methodology for conducting public-procurement. Initially, the emphasis of governments and multilateral agencies promoting e-procurement was mainly on transparent display of 'tender-notices and tender-documents'. The focus gradually shifted to 'e-bid-submission and opening', which is the electronic equivalent of sealed-bid tendering and its public-opening, and other forms of e-procurement. Hence, there is a **need to develop a new set of working procedures and rules to audit such e-procurement/ e-tendering systems** and related practices. This entails an understanding of the technical peculiarities of such systems, especially how the sacrosanct principles of public-procurement, namely Integrity, Transparency, Fairness, and Accountability have been achieved (or not achieved) in these electronic systems.

While discussing the subject of e-Procurement, it is important to appreciate the difference between its various forms. The broad categories are –

- **e-Catalog or e-Marketplace**, which is essentially for purchase of standardised low-value commonly-used items;
- **e-Procurement or e-Tendering**, which is generally referred to in the context of the electronic equivalent of the traditional sealed-bid tendering;
- **e-Reverse Auction**, which is a form of bidding where the bids are not sealed, and is typically used for creating an open competition on 'price' for commoditized items, or where technical and other criteria have been separately evaluated through sealed-bid e-tendering.

In terms of the 'value of public-procurement' and its consequent 'sensitivity from audit perspective', the highest importance has to be given to e-tendering/e-procurement. Further, even amongst e-tendering/ e-procurement systems deployed in various countries, the variation in functionalities, degree of robustness and methods of encryption, and levels

of transparency is so enormous as to be almost mind-boggling from audit perspective.

Apart from enhancement in efficiency, an important underlying assumption for the promotion of e-procurement/ e-tendering has been that technology will reduce malpractices. However, technology is a dual-edged sword. Malpractices prevalent in the traditional manual/ paper-based method of public procurement, such as compromising bid-confidentiality, bid rigging, non-transparent bid-opening, et al can continue with greater degree of sophistication in the electronic versions, unless the underlying web-application software has inbuilt technical features and checks to prevent such malpractices. **In the absence of adoption of appropriate precautionary measures, technology-enabled malpractices in e-procurement can be worse than in manual-tendering**. For example,

- Bid-Confidentiality can be compromised by stealing bid-data through clandestine bid-decryption, and sharing it with a conniving vendor;
- Transparency related established practices for 'public bid-opening' can be compromised, by not having an 'Online Public Tender Opening Event', which is conducted transparently in the interactive/ simultaneous online presence of authorized representatives of bidders, as well as, the authorised officers of the buyer organization. Transparency is further compromised by not sharing with the bidders 'instantly and automatically' the salient points of each opened bid as soon as that bid is opened, in the form of a comparative chart;

  et al.

Importantly, the reality on the ground is that most such technology-enabled malpractices may **neither get discovered nor reported**. So, a sensitive application like e-procurement should be designed and developed keeping in view the adage, "**Prevention is better than Cure**". It would be incumbent on the regulatory authorities of a country to ensure that technical features/ checks that make such malpractices unfeasible, are incorporated in the e-procurement systems being deployed in that country (eTEG, 2013; iCISA, 2018a; Kohli, 2012, 2015, 2016; STQC, 2011).

The following excerpts from a report of the EUROSAI IT Working Group, reinforce this view*:*

QUOTE:

- Digital systems controls must often be activated earlier – be preventative instead of detective/corrective – due to the rapid electronic and automated information flow
- IT security policy should include both internal and external threats (risks) against the systems and data indispensable for a public body's mission and development UNQUOTE (EUROSAI, 2004)

Due to the relative newness of e-procurement/ e-tendering as a methodology for public-procurement, and a general lack of awareness of its technical nuances, it becomes a challenge for the Supreme Audit Institutions of a country to audit such systems. The audit team is confronted with the task of ascertaining whether an e-procurement system being audited has been providing during its usage -- foolproof bid-confidentiality, unquestionable transparency, accountability, supplemented with comprehensive audit-trails at various levels to allow ex post verification of electronic transactions. This challenge is somewhat akin to the challenge in the story most people would have read at kindergarten level in school, "How to bell the cat?" The transposed challenge would be – how to have practical procedures and rules to achieve in e-procurement, transparency, integrity and other stated noble objectives of public-procurement.

Prerequisite for Auditing e-Procurement Systems

Generically, an e-procurement/ e-tendering system would come in the category of 'Information Technology (IT) systems'. To that extent, general rules and procedures applicable to audit of IT systems would also be applicable to e-procurement/ e-tendering systems. However, e-procurement/ e-tendering has its own peculiarities, and special criticalities that require special domain knowledge. This necessitates application of special auditing techniques/ tools that are over and above the general auditing procedures of IT systems.

In this context, the following excerpt from the report of EUROSAI IT Working Group is relevant:

QUOTE: Authorities that run e-government services are under the obligation to make technical and organisational arrangements allowing the ex post verification of electronic transactions enabling supervisors or auditors to find out who entered or conveyed which data at which time. The arrangements made must also be adequate to detect and investigate any unauthorised attempts to access or tamper with data. Examples of risks

and potential damage caused by non-compliance with these requirements are:

- introduction into IT networks of malicious software (e.g. viruses; Trojan horses; logical bombs or worms);
- tampering with/ damaging / destruction of operating systems or application
- tampering by 'internal offenders' (e.g. administrators or users); …
- (Audit Trails)… organization should therefore create new audit trails in the automated information systems, to ensure that transactions can always be audited. Nonexistent or inadequate audit trails bring the risk that unauthorized changes of data go unnoticed …UNQUOTE (EUROSAI, 2004).

Without going further into various aspects of 'Audit of IT Systems', the minimum that the audit team is expected to check in this regard would be,

- Whether the e-procurement system has undergone a 'certification' process to meet legal, security, technical/ conformity assurance levels as may be required by the regulatory framework of that country.
- Whether the e-procurement system being audited is 'compliant' with the relevant Governing/ Regulatory Framework of that country.
- Notwithstanding the certification, this independent check by the audit team is important, as on the ground enforcement may not be satisfactory. Further, just as the 'Volkswagen Emissions Scandal' in September 2015 had exposed, even certification/ testing processes can be defeated by delivering in the real-world a product which is different from what was offered for certification (Kohli, 2016).

Needless to state, the existence a governing/ regulatory framework and allied processes within a country becomes a 'prerequisite' for auditing of e-procurement systems deployed in that country. Allowing e-procurement within a country, without having such a regulatory framework would be similar to having aircraft flying in the sky without any civil aviation framework and air-traffic control. The result would be unmitigated disaster. **In case of unregulated civil aviation, it will lead to frequent collisions of aircraft in the sky, which will of course be noticed and tears shed. In case of unregulated e-procurement, bid-manipulation**

will become a norm, and no tears will be shed because as stated earlier, such malpractices will normally neither get discovered, nor reported.

METHODS AND DISCUSSION

Since having a relevant regulatory framework is a prerequisite for a consistent and proper audit, for rest of the discussion on this subject, **reference will be made to the regulatory framework for e-procurement applicable in India** (STQC, 2011). **Based on available information, at present the framework in India is perhaps the most comprehensive in the world**. In addition, where relevant, reference will also be made to final report issued in 2013 by the e-Tendering Expert Group (**e-TEG**) appointed by the European Commission (e-TEG, 2013).

Countries that do not have a similar regulatory framework for e-procurement, but are keen to have e-procurement systems deployed in their respective country, could consider borrowing the framework from India. From an applicability perspective, this should be quite justified as broadly **the fundamental principles of public-procurement are similar for most countries**.

Regulatory Framework for e-Procurement/ e-Tendering in India

In the context of India, the most important document relating to the governing framework for e-procurement/ e-tendering is the 'Quality Requirements of e-Procurement Systems dated 31st August 2011' (earlier popularly referred to as DIT-Guidelines, and now **DeitY-Guidelines**) issued by 'Standardisation Testing & Quality Certification (STQC)' Directorate, Ministry of Electronics and Information Technology (MeitY), Government of India. These DeitY-Guidelines encompass relevant guidelines of the Central Vigilance Commission (CVC) of India as Annexure-II of the guidelines; the General Financial Rules (GFR) of the Finance Ministry of India as Annexure-III of the guidelines; the Information Technology Act 2000 (and its Amendment 2008) of India as Annexure-IV of the guidelines (STQC, 2011).

Further, the CVC vide its circular dated 12th January 2012, and the Finance Ministry vide its Office-Memorandum dated 3rd September 2012, had directed that all e-procurement systems used by government entities in

India should be certified for compliance with DeitY-Guidelines by STQC only.

The regulatory frameworks outlined above, **along with problems and malpractices observed on the ground**, have been considered to propose an 'Audit Framework for e-Procurement'.

AUDIT FRAMEWORK FOR E-PROCUREMENT

Sample Checklist for Audit of 'Overall/ General Aspects'

1. **It is mandatory for "the complete e-procurement system, viz the application along with the server in a specific hosting environment" to be certified by STQC for compliance with DeitY-Guidelines**.

   In other words, if an e-procurement service provider has set up four separate e-procurement portals for four different government organizations, then each of these four portals has to be independently certified by STQC for compliance with DeitY-Guidelines (even if the same version of the application software has been claimed to be deployed on all the four portals).

[Relevant regulatory references: CVC Circular dtd 12th January 2012; Finance Ministry's Office Memorandum dtd 3rd September 2012; section 6.0 of DeitY-Guidelines (STQC, 2011)]

Some Audit Points:

(a) Check whether there is a 'valid STQC certificate for compliance with DeitY-Guidelines' for the specific e-procurement system being audited. If not, it is a 'Red-Flag'.

Needless to state, the following scenarios could be straightaway 'Red-Flagged':

(i) E-procurement portal that has not been certified by STQC

(ii) A different STQC certificate, ie not specifically for compliance with DeitY-Guidelines, is being presented to mislead the auditors and users.

(Note: Apart from certification for compliance with DeitY-Guidelines, STQC does many other types of testing

and certification of many other types, such as OWASP, etc.)

Further, if the following 'checks' are 'not true', it is a 'Red-Flag' --

(b) Whether the URL of the portal given in the STQC certificate is the same as that of the portal being audited.

(Note: There are instances where unscrupulous vendors have got one portal certified, and are flaunting that certificate for all their other portals)

(c) Whether 'version reference' of the software solution of the portal is the same as that given on the related STQC certificate.

(d) Whether the 'portal is owned and operated' by the same entity with which the government buyer (ie purchasing-entity or contracting-authority) has signed the contract for e-procurement services.

(For example, a government buyer may have been misled into believing that the government entity with which they are signing the contract is the 'owner and/ or operator' of the portal and is responsible for the 'security of the database', while in reality the actual physical portal may be 'owned and/ or operated' by a private entity', and the government entity is only a front)

2. To prevent misuse by the e-Procurement service provider, **the service provider 'should not have access to the source code' of the e-procurement software/ solution**.

(Note: Service provider should carry out its activities with compiled code) [Relevant regulatory references: page-17 of DeitY-Guidelines]

3. To prevent misuse by the e-Procurement service provider, **the e-procurement service provider or the portal operator should not be selling or providing PKI encryption and decryption certificates/ keys** to the users of the portal.

[Relevant regulatory references: Annexure-I (section 2.1) of DeitY-Guidelines. On page-19, 25 it is stated, "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."]. Note: In this para, CA refers to a certifying authority that issues a digital signature certificate.

Sample Checklist for Audit of some Critical Functionalities

As stated earlier, even a 'valid STQC certificate for compliance with DeitY-Guidelines' may only be a 'fig-leaf', and the actual functionalities of the software deployed on the e-procurement portal may be different from the functionalities prescribed in the DeitY-Guidelines.

Cautionary Note: To get at the truth, the auditing team could themselves conduct some 'functionality checks' on the actual portal deployed in the field (and not on some demo portal of the concerned service-provider). The user-manuals (for both Buyers and Suppliers) should also be independently procured and studied by the auditing team. Only then there is a reasonable chance for the truth to be revealed. Due to constraint of space, only some critical functionalities are being discussed here.

1. **Bid-Encryption Methodology**:

   This is the most critical functionality to be checked, as any compromise in bid-confidentiality before the 'online public tender opening event' will make a mockery of the public-procurement process. Section 3.1 of DeitY-Guidelines requires that 'bid-encryption' should be done at client-end (ie bidder's computer) using symmetric-key, or asymmetric-key (PKI-based) subject to issues raised in Annexure-I and II of DeitY-Guidelines being suitably addressed. In addition, bids before transmission from the bidder's computer should be protected with SSL (now called TLS) encryption. Further, as prescribed in Annexure-I (section 3.2) of DeitY-Guidelines, "… at no point of time the System Administrator or Data Base Administrator should be authorized to hold the private (decryption) key."

	Functionality to be Checked	**Inference/ Conclusion**
	Is the main bid encryption being done at the client-end or database-level (ie server end) Note: A scenario, where bids before being transmitted from the bidder's computer are protected with only SSL/TLS Encryption, and Database-level Encryption is done	*If the main bid encryption is not being done at the client-end, it is a 'Red-Flag' as per DeitY-Guidelines -- section 3.1; Annexure-I*

	before the bid is stored in the Database Server, is covered by Annexure-I (Section 3) of DeitY-Guidelines on pages 25-27. As per section 3.1 and Annexure-I (section 3) of DeitY-Guidelines, this method of database-level encryption (irrespective of whether symmetric or asymmetric key is used) is not acceptable as it violates the requirement of bid-encryption at client-end (ie bidder's computer) followed by SSL/ TLS encryption before transmission from the bidder's computer.	*(sections 3.1, 3.2); Annexure-II (12);*
	Assuming that Bid-Encryption is being done at 'Client-end', we have the following Scenarios:	
	Scenario-1: Where asymmetric encryption methodology using Public-Key/ DSC or Encryption Certificate of an officer of the Buyer organization, or any other Public-Key specified by the Buyer organization is used for bid-encryption	
	Security vulnerabilities of this form of bid-encryption are explained in Annexure-I (Section 2.0) of DeitY-Guidelines on pages 19-25. To mitigate the security risks mentioned in DeitY-Guidelines, it should be checked as to which of the following <u>remedial measures</u> (as given on pages 23-24 of DeitY-Guidelines) have been adopted in the portal being audited: i) Key-Splitting ii) Repeated/ Multiple encryption iii) Any other Detailed information should be sought from the service provider as to how the security risks mentioned in section 2.0 of Annexure-I of DeitY-Guidelines have been satisfactorily addressed. Further, even if these measures have been adopted, 'field-level practicability efficacy' of the measure should be checked by the audit team.	*If neither key-splitting, nor multiple repeated encryption, nor a better measure has been adopted, then this is a very serious 'Red-Flag'.* *If some of the remedial measures have been implemented, then decision has to be taken based on the 'field-level practicability and efficacy' of the measure.*

	For example, if key-splitting has been done, then keeping in view the IT Act and other aspects -- • In how many parts has the key been split? • How is the key split done? • Even after the key is split into 'N' parts, will at least one original copy remain in un-split form? (If so, can it not be misused?) • How and where is the 'Original' key 'securely' stored/escrowed? • How and where are the split key parts 'securely' stored/ escrowed? • How many split key parts are required to be put together for Bid-decryption? et al. Similarly, if some measure such as 'multiple encryption' has been adopted, and three copies of the same bid have been independently encrypted using a different key each time, then it is actually making the situation worse as far as ensuring security is concerned, as connivance of any one of the three key-owners can compromise Bid-Confidentiality. In contrast, if 'repeated multiple encryption' has been done sequentially, then while the security situation improves to some extent, the dependency on the presence of 'all the three key owners' during the public tender opening becomes necessary, thus worsening the situation from a practical angle.	
	Scenario-2: Where asymmetric encryption methodology (Public key of a user of the Bidder organization) is used for bid encryption	

	Security vulnerabilities of this form of bid-encryption are explained in Annexure-I (Section 2.6) of DeitY-Guidelines on page-25. Note: Apart from the reasons detailed in Annexure-I (section 2.6) of DeitY-Guidelines, for decryption this method would entail the 'mandatory' physical presence (during the public tender opening) of the bidder's representative who is the owner of the corresponding private key. Hence it is not acceptable as per DeitY-Guidelines and the established principles of public-procurement.	*If this method has been adopted, it is a 'Red-Flag'.*
	Scenario-3: Where symmetric encryption methodology (bidder-generated passphrase) is used for bid encryption	
	Most security issues which are applicable for other forms of bid-encryption become irrelevant in this case (refer page-22 of DeitY-Guidelines). This view is corroborated by section 6.7 of the final report issued by the e-Tendering Expert Group (e-TEG) appointed by European Commission (e-TEG, 2013). A report titled 'Recommendations for Encryption Policy' issued by the Data Security Council of India (DSCI) reinforces this view. However, even in this method, DeitY-Guidelines rightly require a few checks to be done as described in Annexure-I (section 4.1) on pages 27-28. Check 4.1(c) has now been made mandatory by STQC.	*As per section 6.7 of the final report issued by the e-Tendering Expert Group (e-TEG) appointed by European Commission, this is the only legitimate method that ensures '**full confidentiality**'.* *The DeitY-Guidelines also confirm this view subject to a few minor concerns being suitably addressed.*
	Scenario-4: Where symmetric encryption methodology (system-generated password/ passphrase) is used for bid encryption	

	DeitY-Guidelines have not bothered even to discuss this method in detail, presumably because by inference the security concern mentioned on page-27 of DeitY-Guidelines becomes applicable in this case, viz – "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". If the symmetric key (used for encryption/ decryption) is generated within the system, a copy of the key will always remain in the system for decryption, and such a key will be accessible to the database administrator. Even if this method is modified to some extent, such as by taking a copy of the system-generated symmetric key and further encrypting it with the public key(s) of the tender opening officer(s) simultaneously (ie having hybrid-encryption at this stage), bid-confidentiality can still be compromised through connivance of such officer(s).	*If this method has been adopted, it is a 'Red-Flag', unless a fool-proof method has been implemented to prevent access of the system-generated key or password to the database administrator(s) of the system. Even in case of hybrid-encryption (especially the way it would have to be implemented in this case), connivance of the concerned officers cannot be ruled out.*
	Notwithstanding the above Scenarios of Bid-Encryption Methodology, additional functionality checks relating to Bid-Encryption would have to be done as follows:	
	Annexure-I (section 1.2) of the DeitY-Guidelines requires that – "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." The above requirements are reiterated in Annexure-I (sections 6.1 and 6.2) of the DeitY-Guidelines. Based on the above prescriptions, the following checks can be done:	
	Is there a facility in the system of having a 'summary format' (ie a flexible electronic template) for the **prequalification envelope**?	*If any of these facilities is not available in the prescribed form, it is a 'Red-Flag'.*
	If the above answer is 'Yes', is there a facility in the system of digitally signing, as well as, encrypting such a bid-part at the client-end using one of the permissible encryption methodologies (suitably augmented as discussed above)?	
	Is there a facility in the system of having a 'detailed bid' (ie a file of at least 10 MB) for the prequalification envelope?	
	If the above answer is 'Yes', is there a facility in the system of digitally signing, as well as, encrypting such a bid-part at the client-end using one of the permissible encryption methodologies (suitably augmented as discussed above)?	
	Is there a facility in the system for 'Modification' of the prequalification envelope?	
	If the above answer is 'Yes', is such a modification-bid suitably encrypted and digitally signed before submission?	
	Is there a facility in the system for 'Substitution' of the prequalification envelope?	

	If the above answer is 'Yes', is such a substitution-bid suitably encrypted and digitally signed before submission?	
	Is there a facility in the system of having a 'summary format' (ie a flexible electronic template) for the **technical envelope**?	
	If the above answer is 'Yes', is there a facility in the system of digitally signing, as well as, encrypting such a bid-part at the client-end using one of the permissible encryption methodologies (suitably augmented as discussed above)?	
	Is there a facility in the system of having a 'detailed bid' (ie a file of at least 10 MB) for the technical envelope?	
	If the above answer is 'Yes', is there a facility in the system of digitally signing, as well as, encrypting such a bid-part at the client-end using one of the permissible encryption methodologies (suitably augmented as discussed above)?	
	Is there a facility in the system for 'Modification' of the technical envelope?	
	If the above answer is 'Yes', is such a modification-bid suitably encrypted and digitally signed before submission?	
	Is there a facility in the system for 'Substitution' of the technical envelope?	
	If the above answer is 'Yes', is such a substitution-bid suitably encrypted and digitally signed before submission?	
	Is there a facility in the system of having a 'summary format' (ie a flexible electronic template) for the **financial envelope**?	
	If the above answer is 'Yes', is there a facility in the system of digitally signing, as well as, encrypting such a bid-part at the	

	client-end using one of the permissible encryption methodologies (suitably augmented as discussed above)?	
	Is there a facility in the system of having a 'detailed bid' (ie a file of at least 10 MB) for the financial envelope?	
	If the above answer is 'Yes', is there a facility in the system of digitally signing, as well as, encrypting such a bid-part at the client-end using one of the permissible encryption methodologies (suitably augmented as discussed above)?	
	Is there a facility in the system for 'Modification' of the financial envelope?	
	If the above answer is 'Yes', is such a modification-bid suitably encrypted and digitally signed before submission?	
	Is there a facility in the system for 'Substitution' of the financial envelope?	
	If the above answer is 'Yes', is such a substitution-bid suitably encrypted and digitally signed before submission?	
	Is there a facility in the system for 'Withdrawal' of the submitted bid by the bidder with his digital signature?	

2. **Online Public Tender Opening Event**: This is another critical functionality to be checked, as this event is the backbone of 'Transparency' in public-procurement. It is important to note that an 'Online Public Tender Opening Event' is different from a mere 'Online Tender Opening Event'. While the former type, if sincerely implemented and conducted in the 'simultaneous' and 'interactive' online presence of bidders in an elaborate manner ensures proper 'Transparency', the latter type has the potential of being a mere 'eyewash'. Annexure-I (section 6.3) on pages 35-38 of DeitY-Guidelines describes the issues and requirements in reasonable detail and should be thoroughly perused. Other sections of the DeitY-Guidelines, such as -- Annexure-II (checkpoint 8 on page-45),

Annexure-III (pages 54, 60, 63, 64, 68, 69) are also relevant. Some recommended checks are as follows:

	Functionality to be Checked	**Inference/ Conclusion**
	Is there an Online Public Tender Opening Event conducted in the 'simultaneous' and 'interactive' online presence of bidders? Where the answer to the above question is 'Yes', the following questions should be asked:	*If this facility is not available in the prescribed form, then this is a serious 'Red Flag'.*
	Are the bids opened in the simultaneous online presence of the bidders? Note: 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.	*If any of the required facilities is not available in the prescribed form, it is a 'Red-Flag'.*
	Is there are a proper online attendance record of the authorized representatives of the bidders, as well as, the Tender Opening Officers authorized for that tender?	
	Is the opening of the Online Virtual Tender Box distinct from opening of the bids?	
	Is there facility for one-by-one opening of the sealed bids in the simultaneous online presence of the bidders?	
	Is there facility for performing Online Security Checks to assure bidders of non-tampering of their bids, et al during the online TOE itself? Note: A prerequisite for such a facility is that bidders should be able to 'interact online' with the TOE officers in a	

	transparent manner during the event itself which is visible online to all participants.	
	Is there facility for online verification of the digital signatures of bidders affixed to their respective bids?	
	Is there facility for 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)? *Cautionary Note*: In some systems, while the bidders are allowed to login for witnessing the opening event, they are essentially passive spectators. Bidders cannot participate interactively. Furthermore, the data of the opened bids is posted subsequently, sometimes after many days, and for certain bid-parts it is not posted at all! In such situations there is obviously tremendous potential for indulging in mal-practices.	
	Is there a procedure for seeking clarifications by the tender opening event (TOE) officers during Online Public TOE from a bidder in the online presence of other bidders, and recording such clarifications? Note: A prerequisite for such a facility is that bidders should be able to 'interact online' with the TOE officers in a transparent manner during the event itself which is visible online to all participants.	
	If there feature of digital counter-signing (by all the tender opening officers) of each opened bid, in the simultaneous online presence of all participating bidders?	

	If there facility for generation of the 'Minutes of the Tender Opening Event' and its signing by the concerned officers in the simultaneous online presence of the bidders?	
	Can the Tender Opening Officers be changed at the last moment without jeopardizing the conduct of Online Public Tender Opening Event, and without using the 'decryption key / digital signature key' of the absent officers?	
	While bidders should be welcome to be present physically during the TOE, it should not be mandatory for them to do so.	

(iCISA, 2018a)

Sample Checklist for Audit of some 'Other Important Aspects of e-Procurement Systems'

The following checklists should be perused in continuation of the checklists for two most critical functionalities covered above, namely – (1) Bid-Encryption Methodology; and (2) Online Public Tender Opening Event.

3. **Authentication of Electronic Records**:

Background-Note with reference to GFR and IT Act 2000 (and its Amendment 2008)

With reference to IT Act 2000 (and its Amendment 2008), on p-72 of Annexure-IV of DeitY-Guidelines dated 31st August 2011, it is mentioned that –

QUOTE: 1 (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). UNQUOTE

The requirement of transparent Tender Notice, Corrigenda, Tender Documents, Addenda etc, as required under Rules-149, 150, 151, 180, 181 of GFR, is also elucidated in Annexure-III of DeitY-Guidelines dated 31st August 2011 on pages 57 to 70.

Note: The 'Rule Numbers' of GFR rules (2005) may have changed in the GFR-2017. However, to be consistent with the DeitY-Guidelines, GFR rule numbers (as given in GFR 2005) and as reproduced in the DeitY-Guidelines are being mentioned here.

In addition to the comments/ references of IT Act 2000 (and its Amendment 2008) and GFR given in the 'Background-Note' above, please note the following:

Section 6.1 of Annexure-I of DeitY-Guidelines (p-31, 32, 33) dated 31st August 2011 requires –

QUOTE: … For authenticity and for assurance that it has not been tampered, the electronic **Tender 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 …UNQUOTE;

QUOTE: … At the time of online sale/ downloading of the tender documents, official serial number should be given along with the receipt. UNQUOTE;

QUOTE: … 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… UNQUOTE;

QUOTE: … 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… UNQUOTE;

QUOTE: … 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… UNQUOTE.

An Office Order No. 43/7/04 dtd 2nd July 2004 was issued by the CVC, which also addressed the above mentioned issue under the sub-heading, 'Issues Connected with Data Security, Legality and Authenticity of Bid Documents', along with a Technical Note from NIC. Some excerpts are as follows:

QUOTE: … certain parties may alter the downloaded documents and submit their bids in such altered tender documents which may lead to legal complications…

…The provisions of digital signatures through Certifying Authority can be used to ensure that in case of any forgery or alteration in downloaded documents it is technically feasible to prove what the original document was. There are sufficient legal provisions under IT Act to ensure …UNQUOTE;

QUOTE:

1. Integrity of Document: The documents should be digitally signed by the person submitting them…;

4. Download Procedure:

a. The user verifies the digital signature of the document on the website… UNQUOTE

An e-procurement system should have functionality as prescribed in DeitY-Guidelines (excerpts reproduced above) and the CVC Office Order. If this has not been done, such systems cannot be certified by STQC for compliance with DeitY-Guidelines dtd 31st August 2011.

	Functionality to be Checked	**Inference/ Conclusion**
	Is the Online Tender Notice digitally signed by one of the authorized users of the Buyer organization before it is posted online?	*If any of these facilities is not available in the*

	If the answer to the above is 'Yes', is there an online facility in the system itself for verifying the digital signature by a person viewing the Tender Notice?	*prescribed form, it is a 'Red-Flag'.*
	Is the Online Corrigendum to Tender Notice digitally signed by one of the authorized users of the Buyer organization before it is posted online?	
	If the answer to the above is 'Yes', is there an online facility in the system itself for verifying the digital signature by a person viewing the Corrigendum to Tender Notice?	
	Are the Tender Documents digitally signed by one of the authorized users of the Buyer organization before it is posted online?	
	If the answer to the above is 'Yes', is there an online facility in the system itself for verifying the digital signature by a person viewing/ downloading the Tender Documents?	
	Is the Addendum to Tender Documents digitally signed by one of the authorized users of the Buyer organization before it is posted online?	
	If the answer to the above is 'Yes', is there an online facility in the system itself for verifying the digital signature by a person viewing/ downloading the Addendum to Tender Documents?	
	Is the Response to Query pertaining Tender Documents (Clarification to Tender Documents) digitally signed by one of the authorized users of the Buyer organization before it is posted online?	
	If the answer to the above is 'Yes', is there an online facility in the system itself for	

	verifying the digital signature by a person viewing/ downloading the Response?	
	Are the bids digitally signed by an authorized user of a bidder organization, specifically authorized for that tender?	
	If the answer to the above is 'Yes' is there an online facility in the system itself for verifying the digital signature by an officer during the Online Public TOE?	

4. **Facilitation of various Types of Bidding-Methodologies**:

Background-Note with reference to DeitY-Guidelines dated 31st August 2011

Some relevant references of DeitY-Guidelines are sections – 1.2, 3.1, Annexure-I (sections 1.2, 5.1, 6.1), Annexure-II, Annexure-III' and Reference Document-1. An e-procurement system should have functionality as prescribed in DeitY-Guidelines. If this has not been done, such systems cannot be certified by STQC for compliance with DeitY-Guidelines dtd 31st August 2011.

	Functionality to be Checked	**Inference/ Conclusion**
	Is facility available online for one or more of the following Bidding Methodologies?	*If any of these facilities is not available in the prescribed form, it is a 'Red-Flag'.*
	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	
	Any of the above, combined with a Pre-qualification stage	

	In any of the above, facility for submission of one or more Alternative bids (if allowed by the Buyer)	
	In any of the above, after having submitted the 'original' bid for each bid-part, facility to a bidder to submit: 'Modification' bid 'Substitution' bid or 'Withdrawal'	

5. **User Organization's Virtual Administrative Hierarchy**:

Background-Note with reference to DeitY-Guidelines dated 31st August 2011

Some relevant references of DeitY-Guidelines are sections – 2.0, 3.0, *Annexure-I (section 5.1),* and Annexure-II (Table-5). An e-procurement system should have functionality as prescribed in DeitY-Guidelines. If this has not been done, such systems cannot be certified by STQC for compliance with DeitY-Guidelines dtd 31st August 2011.

	Functionality to be Checked	**Inference/ Conclusion**
	Is there a facility within a Buyer organization to create an online Administrative Hierarchy (such as different departments and authorized users at more than one level)?	*If any of these facilities is not available in the prescribed form, it is a 'Red-Flag'.*
	If 'Yes', can different tenders be handled by different departments of a Buyer organization created above?	
	Can different users of a Buyer organization be authorized for different activities of a tender, and can such users be changed from tender to tender, and during the course of a tender after the tender has been notified?	
	Is there a facility within a Supplier organization to create an online Administrative Hierarchy (such as different	

	sales-departments and authorized users at more than one level)?	
	If 'Yes', can different tenders be handled by different sales-departments of a Supplier organization created above?	
	Can different users of a Supplier organization be authorized for different activities of a tender, and can such users be changed from tender to tender, and during the course of a tender after the tender has been notified?	

6. **Password-Generation and Storage**:

Background-Note with reference to DeitY-Guidelines dated 31st August 2011

Section 3.1 of DeitY-Guidelines (p-6, 7) dated 31st August 2011 requires -- QUOTE: 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. Once the password is forgotten, a new password may be allotted following a set of processes needed for allotment of password. The forget password request shall be digitally signed. UNQUOTE;

Section 7.2 of Annexure-I of DeitY-Guidelines (p-39) dated 31st August 2011 requires -- QUOTE: 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. UNQUOTE; …

QUOTE: 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. UNQUOTE

An e-procurement system should have functionality as prescribed in DeitY-Guidelines (excerpts reproduced above). If this has not been done,

such systems cannot be certified by STQC for compliance with DeitY-Guidelines dtd 31st August 2011.

	Functionality to be Checked	**Inference/ Conclusion**
	Is the Password created by the user himself at the client-end? [Note: A password generated by the system (which is accessible to the administrator) and then communicated to the user is not in accordance with the DeitY-Guidelines]	*If any of these facilities is not available in the prescribed form, it is a 'Red-Flag'.*
	Is the Password created/ generated (by the user himself as mentioned above) encrypted? If so, is it encrypted at the client-end?	
	In case of 'Forgot Password', is the New Password created by the user himself at the client-end after due diligence by the system/ service-provider?	
	In case of 'Change-Password', is the New Password created by the user himself at the client-end?	
	Does the user account remain unlocked even in case of a number of un-successful attempts? [Note: Instead of locking the user account in the above scenario, the system should have a system of alerting the concerned user after a specified number of unsuccessful attempts, and a mechanism to break the continuity of multiple attempts.]	

(iCISA, 2018b)

7. **Audit Trails**:

There should be independent audit trails for 'three categories of users' – Buyers, Suppliers, Application Administrators of the portal. Important activities/ events conducted by each of these category of users should generate audit trails. At times, it is not enough to merely audit trail only when an activity or an event took place along with the identity of the user. A good audit trail should also store the 'corresponding data', as well as, what was added, modified or deleted. This is illustrated with examples given below.

Examples:

i. Let us say a Tender Notice is created and submitted by an authorized user of a Buyer organization. It is not enough to only record the identity of the concerned user of the Buyer organization, and the date and time of submission. In a good audit trail, data of that Tender Notice should also be saved as part of the 'audit trail data'. This should be in addition to actual data of the Tender Notice, which is used for display of that Tender Notice.

ii. While creating a Corrigendum to the Tender Notice, some data is changed. For example, the 'Last Date and Time of Receipt of Bids' is changed from '5th January 2020 14.00 GMT' to '15th January 2020 14.00 GMT'. A good audit trail should not only record when the change was made to the Tender Notice, but also the old 'Last Date and Time of Receipt of Bids', as well as, the new 'Last Date and Time of Receipt of Bids'.

Background-Note with reference to DeitY-Guidelines dated 31st August 2011

Some relevant references of DeitY-Guidelines are sections – 3.1, Annexure-I (sections 2.2, 3.1, 5.1, 5.2, 6.1, 7.4, Summary- Analysis of Risk of eProcurement Systems), Annexure-II, and Annexure-III.

	Functionality to be Checked	**Inference/ Conclusion**
	Audit Trails relating to Activities of a Buyer	

	Are detailed Audit Trails created for various activities conducted by a Buyer organization? Where the answer to the above question is 'Yes', the following questions should be asked:	*If any of these facilities is not available in the prescribed form, it is a 'Red-Flag'.*
	Is there a facility to authorize a 'special person' (ie independent of the concerned users) to generate/ access such Audit Trail Reports?	
	Audit Trails for some 'Important Activities' in this Category	
	Detailed list will depend upon the design and functionalities of the application software. Only a sample list of activities is given below: • Tender Rules and Configuration along with Digital Signature • Authorization of various activities Tender/ Non-Tender related activities • Tender Notice along with Digital Signature • Corrigendum along with Digital Signature • Tender Documents along with Digital Signature • Addendum along with Digital Signature • Response to Bidder's Query - Clarification to Tender Documents along with Digital Signature • Minutes of Pre-Bid Meeting along with Digital Signature	

	• Conducting Tender Opening Event along with Digital Signature • Opening of Bids • Countersigning of Opened Bids along with Digital Signature • Countersigning of Unopened/ Archived-unopened Bids along with Digital Signature • Minutes of TOE along with Digital Signature • (Query) Technical Conformance (Post Bid Opening/ Evaluation) along with Digital Signature • Shortlisting of Qualified Bidders along with Digital Signature • Award of Contract along with Digital Signature	
	A specific critical requirement of audit trails during the Online tender Opening Event is as follows: "…Further, it is important to understand that the comparative statement (CS) is a derivative of the opened bids. It must be ensured that the comparative statement should be automatically derived from the opened bid data and displayed instantly to the bidders, and not complied and uploaded later by the officers of the purchasing entity (and certainly not by the support personnel of the service-provider). Importantly, each opened bid must be digitally countersigned by the authorised TOE-officers in the simultaneous online presence of bidders and this activity should be audit-trailed by the system."	

	Audit Trails relating to Activities of a Supplier	
	Are detailed Audit Trails created for various activities conducted by a Supplier organization? Where the answer to the above question is 'Yes', the following questions should be asked:	
	Is there a facility to authorize a 'special person' (ie independent of the concerned users) to generate/ access such Audit Trail Reports?	
	Audit Trails for some 'Important Activities' in this Category	
	Detailed list will depend upon the design and functionalities of the application software. Only a sample list of activities is given below: • Authorization of various activities Tender/ Non-Tender related activities • Clarification to Tender Documents – Query by Supplier along with Digital Signature • Various events/ activities related to Bids along with Digital Signature o EMD Details o ElectronicForms of Bid-Part o Main-Bid of Bid-Part o Bid-Annexures o Tender Documents/ Addendum o General Terms and Conditions (GTC)	

	○ Special Terms and Conditions (STC) • Tender Opening Event – Attendance Register along with Digital Signature • (Response to Query) Technical Conformance (Post Bid Opening/ Evaluation) along with Digital Signature	
	A specific critical requirement of audit trails during Bid-submission, and the Online tender Opening Event is as follows: "… Furthermore, in case of all e-procurement systems (which fall under 'Scenarios 1, 2, and 4' of bid-encryption methodology as described in the previous article), there should be a 'standard operating procedure (SOP)' for checking in detail the audit trails and the digital signatures, ie signed/ encrypted one-way-hash (OWH), of each bid as submitted and digitally signed by each bidder. Under the SOP, the signed OWH of each bid as submitted, and signed OWH of the that bid after opening (or before opening if the bid has been signed after encryption) should be matched 'each time every time'. Most importantly, this SOP should be performed interactively in the simultaneous online presence of bidders during the Online Public TOE by the authorised officers of the purchasing entity (and not by the support personnel of the service-provider)."	
	Audit Trails relating to Activities of Application Administrators	

	Are detailed Audit Trails created for various activities conducted by an Application Administrator (of the service provider)? Where the answer to the above question is 'Yes', the following questions should be asked:	
	Is there a facility to authorize a 'special person' to generate/ access such Audit Trail Reports?	
	Audit Trails for some 'Important Activities' in this Category	
	Detailed list will depend upon the design and functionalities of the application software. Only a sample list of activities is given below: • Acceptance of Registration of a user-organization (Buyers/ Suppliers) • Change in Registration Details of a user-organization (eg User-Organization Name, Main Contact Person of the organization, etc) • Request received online from any user-organization for expunging any incorrect posting made public • Expunging any incorrect postings made public (on request from concerned user-organization, or on orders from Law-Enforcement authorities) • Renewal of Registration (if applicable) • Updating status of verification of a user-organization • Generating audit log reports of events executed by various Buyer	

		organizations, as well as, Supplier organizations, subject to certain conditions and constraints. For example, audit logs of Supplier organizations related to bid-submission should be accessible to application administrators only after commencement of Online Public TOE.	

(iCISA, 2018b; STQC, 2011)

In addition to the above audit trails outlined above, there would also be audit trails at the server level, especially database level, which may be required in case of suspicion of any backend (ie not through the application) illegal access to the database. Such audit trails have not been discussed in this paper.

REFERENCES

Note: If a link does not open, to proceed further, copy and paste the URL/ link in the 'address bar' of a browser, such as Internet Explorer or Chrome.

CAG of India (2016). Comptroller and Auditor General of India. (2016, February 15). Our Vision, Mission and Values. *Comptroller and Auditor General of India, Supreme Audit Institution of India*. [Online]. Available at https://cag.gov.in/content/our-vision-mission-and-values [Retrieved March 31, 2020]

e-TEG (2013). Final report issued in 2013 by the e-Tendering Expert Group (e-TEG) appointed by the European Commission. *Recommendations for Effective Public e-Procurement, Part II: Operational Recommendations*. [Online]. Available at

http://ec.europa.eu/DocsRoom/documents/18025/attachments/1/translations/en/renditions/pdf [Retrieved March 30, 2020]

EUROSAI (2004). *E-government in an audit perspective.* Report by the IT Working Group in November 2004. [Online]. Available at http://www.eurosai-it.org/documents/activities/english_e_gov.pdf [Retrieved March 31, 2020]

iCISA (2018a). PursuIT May 2018 Issue, Audit Aids: Integrity Issues to be kept in Perspective during Audit of E-Procurement Systems. [Online]. Available at

https://cag.gov.in/uploads/icisa_resources/e-Journal-PursuIT-2018-First-Issue-062da28982f01a1-11197673-0646f53b9de1400-23008901.pdf [Retrieved June 30, 2024]

iCISA (2018b). PursuIT Second Half-yearly Issue, Audit Aids: Integrity Issues to be kept in Perspective during Audit of E-Procurement Systems. [Online]. Available at

https://cag.gov.in/uploads/icisa_resources/e-Journal-PursuIT-2018-Second-Issue-062da28bf79bc15-40713183-0646f53a8b5f4b8-90665977.pdf [Retrieved June 30, 2024]

Kohli, J. (2012). *Red Flags in e-Procurement/ e-Tendering for Public Procurement and Some Remedial Measures*. Paper presented at the IPPC5 at Seattle, USA. [Online]. Available at http://www.ippa.org/IPPC5/Proceedings/Part2/PAPER2-6.pdf [Retrieved March 30, 2020]

Kohli, J. (2015). "Combating Organized Corruption in Public-procurement Through Appropriately Designed e-Procurement Systems''. Paper presented at the Third Conference on Evidence-Based Anti-Corruption Policies (CEBAP III) on Organized Corruption', organized by Thailand's National Anti-Corruption Commission (NACC) in collaboration with the World Bank et al., Bangkok, Thailand, June17-18, 2015.

Kohli, J. (2016). Avoiding the Volkswagen Emissions Scandal in E-procurement Systems: Imperative of Transparent Disclosure Norms and Certification of Critical Functionalities. Paper presented at the IPPC7 at Bali, Indonesia, August 4-6, 2016. [Online]. Available at http://www.ippa.org/images/PROCEEDINGS/IPPC7/Paper41_Kohli.pdf [Retrieved March 30, 2020]

STQC (2011). *Guidelines for Compliance to Quality Requirements of eProcurement Systems,* issued on 31st August 2011 by STQC, Ministry of Electronics and Information Technology (MeitY), Government of India. [Online]. Available at

https://egovstandards.gov.in/sites/default/files/2021-07/Compliance%20to%20Quality%20Requirements%20of%20e-Procurement%20Systems.pdf [Retrieved June 30, 2024]