SUPREME AUDIT INSTITUTION OF INDIA
लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

Report of the Comptroller and Auditor General of India on Information Technology Audit of e-Procurement System in Government of Odisha for the year ended March 2022

Government of Odisha

Report No. 1 of the year 2025

Report of the
Comptroller and Auditor General of India
on
Information Technology Audit of
e-Procurement System in Government of Odisha
for the year ended March 2022

Government of Odisha

Report No. 1 of the year 2025

Table of contents

Preface

This Report of the Comptroller and Auditor General of India on Information Technology Audit of e-Procurement System in Government of Odisha for the year ended March 2022 has been prepared for submission to the Governor of Odisha under Article 151 of the Constitution of India and under provisions of Section 19A of the Comptroller and Auditor General's (Duties, Powers and Conditions of Service) Act, 1971, as amended from time to time, for being laid before the Legislature of the State.

The audit was conducted to assess whether the e-procurement system has been effectively implemented and utilised to achieve the objectives of promoting competition, transparency and accountability; business rules have been adequately mapped onto the system; completeness, integrity, and reliability of data in the system was being maintained; and adequate controls have been built into the system.

The audit has been conducted in conformity with the Auditing Standards issued by the Comptroller and Auditor General of India.

Executive Summary

The State Government implemented online tendering during the year 2008 by using Government e-Procurement System developed by NIC (GePNIC). The audit of this application was conducted to assess whether the e-procurement system has been effectively implemented and utilised to achieve the objectives of promoting competition, transparency and accountability. Further, Audit also assessed whether business rules have been adequately mapped onto the system; completeness, integrity, and reliability of data in the system was being maintained and adequate controls have been built into the system.

The major Audit findings are as under:

1. Government has not signed any service level agreement with NIC for development and implementation of the GePNIC. NIC could not complete the implementation of modules such as Vendor Management, Indent Management, Contract Management and Catalogue Management. In the absence of any agreement, no action could be intiated to reap the intended benefits of the system.

2. Significant business processes such as tender evaluation (both technical and financial), negotiation with vendors, and award of contract are still being carried out manually, instead of through the e-Procurement system. As a result, the objective of eliminating human interface for these key processes has not been achieved. In the absence of application controls for these processes carried out manually, Audit noticed instances where Tender Inviting Authorities (TIAs) had manually increased the bid amounts submitted by bidders after downloading the financial bid (Bill of Quantities) from e-Procurement portal and excluded the L1 bidder from consideration at the time of award of contract.

3. Business rules have not been fully mapped into the e-Procurement application. Provisions for enforcing the prescribed minimum period for submission of bids from the time of publication of tender, defining threshold limits for two-cover tendering system, preventing and detecting splitting of works by TIAs have not been implemented in the system.
4. There are deficiencies in key application controls implemented in the e-Procurement system. These deficiencies have resulted in instances where bids are being submitted after closing time, bids being decrypted by users other than those designated for the purpose, violation of chronological and logical sequencing of timestamps for creation and updating data in the system, BoQ awarded not matching the BoQ specified in the tender, and contract value awarded being higher than the L1 bid amount.
5. There are significant lapses in user access management at the front end and in the maintenance of logs to record user actions at the back end of the application due to which, Audit was unable to rule out unauthorised

modification of data and derive assurance on the completeness and correctness of the data in the system.

The objective of the e-Procurement system was to eliminate human interface; bring transparency in the functioning of tendering activities; facilitate faster dissemination and easy access to information related to tenders; and provide a fair, competitive platform that would safeguard authenticity and enhance efficiency in procurement. Owing to the deficiencies as pointed out by Audit, in this Report, there was a material risk of commission of errors, deliberate irregularities like irregular increase in value of work by exclusion of eligible L-1 bidder and accepting higher bids by the Tender Inviting Authorities and Tender Evaluation Committees when carrying out these processes manually. Deficiencies in input controls in the system resulted in registration of bidders with invalid/incorrect PAN and Digital Signature Certificates (DSCs). During the course of audit, instances of mapping of multiple user IDs with same PAN/DSCs were also noticed making the system prone to manipulations by submission of multiple bids by same bidder. Lack of sufficient system security resulted in submission of bids after expiry of tender closing dates. Deficient system security exposed it to the risk of manual intervention in modification of bid data and change in bid openers, and defeated the very purpose of implementation of e-Procurement System.

Recommendations

Considering the audit observations, it is recommended that:

Government may

- Ensure execution of Agreement/ MoU with NIC, to ensure clarity on timelines, deliverables and service levels.
- Implement the remaining Modules of the e-Procurement system and fully map all the relevant business rules into the system, to ensure that technical and financial evaluation and award of contract is only carried out through the system.
- Integrate WAMIS and CDMS with e-Procurement system, to minimise the risk of manual errors/ deliberate irregularities.
- Adopt the revised threshold value of ₹1 lakh for mandatory e-Procurement as prescribed by Department of Commerce, Government of India.

Government may implement appropriate validation controls for user access management during the registration of bidders, to ensure that

- Valid DSCs, PAN, dates *etc.,* are entered into the system in compliance with executive instructions.
- The essential attribute of non-repudiation is upheld in the system.

Government may consider to

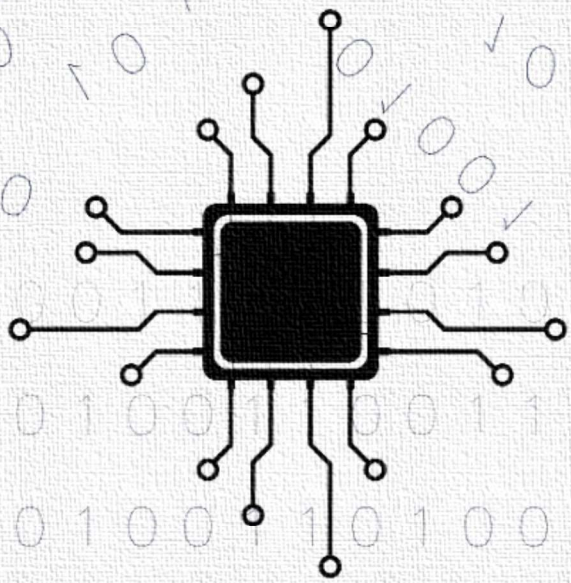
- Implement mapping of business rules for minimum period for submission of bids, mandatory two-cover process for tenders with value more than ₹50 lakh and computation of tender fees based on tender value;
- Implement validation controls to ensure correct recording of bids in the BoQ template and processing controls for correct computation of tender value based on BoQ in the system;

- Enforce application controls to prevent submission of bids after tender closing time;
- Implement validation controls to enforce chronological and logical sequencing of user actions in the system;
- Implement application controls to prevent mapping of the same mobile numbers to multiple users in the system, and enquire into cases where the same mobile numbers had been mapped to Departmental users and bidders;
- Minimise manual interventions at the back end of the system, by adopting formal change management process to implement required functionality for users at the front end of the application;
- Ensure mandatory maintenance of application and DBA logs to record all user actions at the front and back end of the system;
- Adopt standard operating procedures for patch management, version control and documentation of scripts used in the system;
- Enquire into the reasons for the gaps in the sequence of IDs in the major tables of the database;
- Implement appropriate application controls to enforce chronological and logical sequencing for user actions in the system;
- Ensure maintenance of web, application and DBA logs for the system;
- Adopt relevant standards specified by Ministry of Electornics and Information Technology, Government of India from time to time.

Government should

- Map the full business requirements for bid evaluation and award of contract into the system, through implementation of appropriate application controls to ensure compliance and minimise errors/ irregularities.

Chapter 1
Introduction



Chapter I

Introduction and Audit Framework

1.1 Introduction

The State Government introduced online tendering during the year 2008 by using the e-Procurement system/ portal developed by National Informatics Centre (NIC). The objective of the e-Procurement system was to eliminate human interface; bring transparency in the functioning of tendering activities; facilitate faster dissemination and easy access to information related to tenders; and provide a fair, competitive platform that would safeguard authenticity and enhance efficiency in procurement. Initially, tenders costing more than ₹50 lakh were floated through e-Procurement portal from July 2008 in four major engineering departments *i.e.,* Works, Rural Development, Water Resources and Housing & Urban Development Department. From January 2009, all tenders costing ₹20 lakh and above, and from April 2009, all tenders costing ₹10 lakh and above, were made compulsory to be floated through e-Procurement portal. The e-tendering for all tenders costing ₹5 lakh and above except for Urban Local Bodies (ULBs) were started from August 2015. For ULBs the ceiling was fixed at ₹1 lakh and above for mandatory adoption of e-tendering through e-Procurement portal, which was subsequently (03 January 2018) enhanced to ₹2 lakh. Online receipt of tender paper cost and Earnest Money Deposit (EMD) was implemented from December 2017.

During the period from 2011-12 to 2016-17, NIC extended support as part of Government e-Procurement (GePNIC) Mission Mode Project (MMP) under National e-Governance Plan (NeGP) funded by Government of India (GoI). The cost for 2017-18 was borne by NIC using its own resources. Later, Government of Odisha (GoO) paid[1] project cost of ₹402.15 lakh to NIC for implementation and maintenance of GePNIC for three years from April 2018 to March 2021. Further, Works Department in GoO paid ₹388.26 lakh (September 2021) to NIC for extension of GePNIC roll out services for further period of three more years from April 2021 to April 2024.

As of 31 March 2022, total 3,74,806 tenders with tender value of ₹3,31,908.51 crore were floated through e-Procurement portal. 2,637 officials were registered as Departmental Users and 27,359 were registered as Bidders. Out of 40 Departments of GoO, 29 Departments[2] along with PSUs under these Departments were using the e-Procurement system and remaining 11

[1] 27 December 2018 – ₹183.71 lakh and May 2019 – ₹218.44 lakh

[2] Housing and Urban Development Department, Rural Development Department, Department of Water Resources, Works Department, ST and SC Development Department, Agriculture Department, Department of Home, Department of School and Mass Education, Industries Department, Department of Steel and Mines, Food Supplies and Consumer Welfare Department, Department of Energy, Department of Tourism and Culture, Forest and Environment, Department of Health and Family Welfare, Department of Handlooms Textiles and Handicrafts, Department of Co-operation, Commerce and Transport Department, Odia Language literature and Culture Department, Department of Law and Justice, General Administration Department, Fisheries and Animal Resources Development Department, Skill Development and Technical Education, Revenue and Disaster Management Department, Department of Social Security and Empowerment of Persons with Disabilities, Department of Higher Education, IT Department, Sports and Youth Services Department, Department of Finance

departments[3] have not used e-Procurement system and have been using other channels like e-NIVIDA, Government e-Marketing (GeM) and manual tendering for procurements.

1.2 System information and workflow

The System has been developed by NIC using the following platforms:

- Operating System: Linux
- Web Server: Apache Tomcat
- Database: PostgreSql
- Front End: Java/J2EE

The software and the data are held in servers at National Data Centre, New Delhi with disaster recovery site at Hyderabad maintained by NIC.

The web-based application contains the following modules:

Registration Module: Registration/Enrolment of Government officials and bidders with/without Digital Signature Certificate (DSC).

Publishing of tender: Tender creation and publishing, publishing of corrigendum, publishing of pre-bid meeting documents, clarification on the tenders published.

Bid submission: Online bid submission/re-submission as many times as required, freezing of bids, facility for online payment collection through bank payment gateway, encryption of bids submitted by the bidder, facility for single/multiple cover bid system.

Tender opening: Tender opening online.

Technical evaluation: Provision of automatic technical evaluation available.

Financial bid opening: Opening of financial bid online.

Financial evaluation: Evaluation of the financial bid through automatic comparison of Bill of Quantity (BoQ) and selection of L1 bidder.

Award of contract (AOC): Module for awarding to contract to selected bidder(s).

A schematic diagram showing the various modules available on the e-tendering portal / GePNIC is shown in **Figure No.1**.

[3] Excise, Information & Public Relations, Labour & Employees' State Insurance, Micro, Small & Medium Enterprise, Panchayati Raj & Drinking Water, Parliamentary Affairs, Planning & Convergence, Public Enterprises, Science & Technology, Women & Child Development and Mission Shakti

Figure No 1: Schematic diagram showing various modules available on the e- tendering portal/GePNIC

Source : System Requirement Specification (SRS) Document

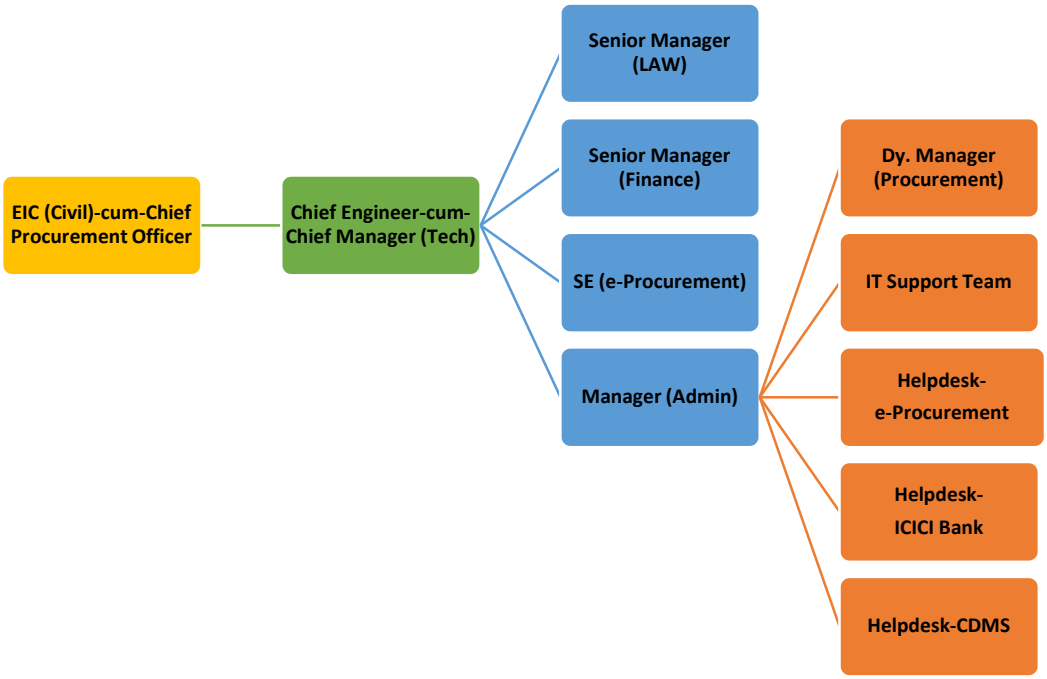
The GePNIC system is certified by STQC, MEITY in compliance with Guidelines for Compliance to Quality requirement of e-Procurement System (GCQE) dated 31 August 2011 issued by Department of Electronic & Information Technology, New Delhi (DEITY) and the certification is current and valid for three years from 21 December 2020.

1.3 Organisation Set Up

With the objective of supervision of the full roll out of the e-Procurement in four Engineering Departments and PSUs, State Government constituted (May 2008) the "State Procurement Cell" under the administrative control of Works Department with EIC[4] (Civil) Odisha as the Chief Procurement Officer and with officers from Law, Finance, IT and Engineering Departments as members to act as an umbrella organisation to sustain, manage, and carry forward the changes. A help desk has been made operational to give technical solutions to tender-related issues of departments and bidders.

[4] Engineer-in-Chief (Civil)

Figure No 2: Organisation Chart of E-Procurement Cell



1.4 Audit Objectives

The objectives of the audit were to assess whether:

- the e-procurement system has been effectively implemented and utilised to achieve the objectives of promoting competition, transparency and accountability
- business rules have been adequately mapped onto the system
- completeness, integrity, and reliability of data in the system was being maintained
- adequate controls have been built into the system.

1.5 Scope of Audit

The audit focussed on analysing the implementation and utilisation of the e-Procurement portal for procuring goods, works and services from the date of roll-out up to 2021-22. Audit examined the portal with reference to general controls, system and network security, application controls, change management controls, disaster management and business continuity plan. Besides, analysis of the database and the data / information uploaded onto the portal by departmental offices and bidders was also done. Data samples, wherever required, were verified through field audit in the respective departmental offices to substantiate the audit findings.

1.6 Audit Sampling

For sample selection of tenders, the tenders published during the last five years *i.e.,* from 2017-18 to 2021-22 were taken as universe. 10[5] out of 29[6] user departments were selected through stratified random sampling using risk-based assessment scores (***Appendix-I***). From amongst the 10 selected departments, a total of 48 out of 678 (seven *per cent*) departmental offices or tender-inviting authorities (TIAs) were selected through stratified random sampling based on population proportionate to size. 10 tenders from each selected TIA were selected through stratified random sampling based on risk scores. Total 486[7] tenders amounting to ₹943.89 crore were selected out of 1,68,178 tenders valuing ₹1,68,517.00 crore for field verifications.

1.7 Audit Criteria

The criteria for audit were derived from the following sources –

- Technical documentation including Software Requirement Specification of each application/ module;
- Relevant acts, rules and policies *i.e.,* IT Act 2000 and subsequent amendments, National e-Governance policies and standards, *etc.,*
- Service level agreements (SLAs), Request for Proposals (RFPs), *etc.;*
- Odisha Public Works Department Code;
- e-Procurement implementation guidelines of GePNIC;
- Guidelines for Compliance to Quality Requirements of e-Procurement System;
- Guidelines issued by Central Vigilance Commission (CVC), Government of India on e-Procurement system;
- Odisha General Financial Rules (OGFR)

---

5 Housing and Urban Development Department, Rural Development Department, Department of Water Resources, Works Department, Industries Department, Department of Steel and Mines, Forest and Environment Department, Odia Language literature and Culture Department, Fisheries and Animal Resources Development Department

6 Housing and Urban Development, Rural Development Department, Department of Water Resources, Works Department, ST and SC Development Department, Agriculture Department, Department of Home, Department of School and Mass Education, Industries Department, Department of Steel and Mines, Food Supplies and Consumer Welfare Department, Department of Energy, Department of Tourism and Culture, Forest and Environment Department, Department of Health and Family Welfare, Department of Handlooms Textiles and Handicrafts, Department of Co-operation, Commerce and Transport Department, Odia Language literature and Culture Department, Department of Law and Justice, General Administration Department, Fisheries and Animal Resources Development Department, Skill Development and Technical Education Department, Revenue and Disaster Management Department, Department of Social Security and Empowerment of Persons with Disabilities, Department of Higher Education, IT Department, Sports and Youth Services Department, Department of Finance

7 Six additional tenders selected based on finding of data analysis

1.8 Audit methodology

Audit objectives, criteria, scope, sample and methodology of audit were shared with GoO through an Entry Conference on 18 July 2022.

Field audit in the selected departments and offices (TIAs) was conducted involving scrutiny of sample selected files, and collection of documentary and electronic evidence from the e-Procurement portal. Analysis of data, log files, and other electronic documents in the e-Procurement portal database as received from NIC was done using computer-assisted audit techniques (CAATs) like VB Script, JAVA, Python, PostgreSQL, Burp suite, IDEA *etc.*

The audit report contains detailed findings arranged in various chapters: Introduction, Project Management and Execution, User Management, Tender Creation and Publication, Bid Creation and Submission, Bid Opening and Evaluation, Award of Contract, Timestamp Management & Application Security, and other issues. The exact names of tables and columns as in the system database have not been used in view of system security.

Exit meeting was conducted on 25 May 2023 with the Departments to discuss the findings. The replies of Department were considered while finalising the report.

Chapter II
Project Management and Execution

Chapter II

Project Management and Execution

2.1 Absence of Agreement/ MoU with NIC for implementation of e-Procurement system

General Control

A service level agreement (SLA) is a contract between a service provider and the end user that defines the level of service expected from the service provider. The roles and responsibilities, timelines, and deliverables along with penalties for under or non-performance are clarified by executing the SLA between both the parties for smooth implementation of Project.

Government of Odisha (GoO) decided (May 2006) to sign a Memorandum of Understanding (MoU) with NIC for implementation of the e-Procurement project which was funded under National e-Governance Plan upto 2017. After which, the GoO had paid ₹790.41 lakh to NIC for implementation and maintenance of GePNIC from April 2018 to March 2024.

Audit, however, observed that agreement or Memorandum of Understanding (MOU) for customization/ implementation of the e-Procurement System had not been entered into with NIC.

Due to the absence of Agreement/ MoU, the roles and responsibilities, timelines, deliverables and service level metrics for performance of the system had not been clearly defined between both the parties, for smooth implementation of the project.

In reply the Department stated (December 2023) that initially the portal was handled by the IT Department, GoO and the same was handed over to Works Department GoO in 2010. Agreement had not been entered into and NIC has been requested to process the MoU, which is awaited.

The fact remained that GoO had implemented the e-Procurement system without an Agreement or MoU defining the roles and responsibilities of NIC, and as a result, it had no legal basis to approach NIC in case of any lapses noticed in implementing the application.

2.2 Non-implementation of key Modules of GePNIC

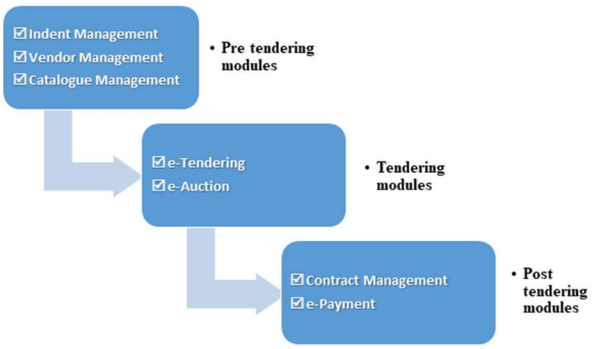
General Control

The e-Procurement application software envisaged modules such as Vendor Management, Indent Management, e-Tendering, e-Payment, Contract Management, e-Auction and Catalogue Management.

However, in the first phase it was decided to implement only the e-Tendering module, while the modules relating to pre-tendering and post-tendering stages were to be implemented in the second phase.

During August 2012, NIC informed the State Government regarding engagement of consultant to carry out required study for preparation of As-Is and To-Be documents for implementation of pre and post tendering modules and contractor database modules *etc.* The final study report of As-Is and To-Be documents were submitted during April 2013.

Figure No 3: Modules of e-Procurement



However, Audit observed that no action was taken after preparation of As-Is and To-Be documents for development of pre and post modules and modules like Vendor Management, Indent Management, e-payment, Contract Management, and Catalogue Management.

Though the e-Auction module was developed by NIC in 2012, it was not used by the Government of Odisha as of March 2022. Due to non-implementation of pre and post modules of the e-Procurement system, the objective of full-automation / elimination of human interface in the tendering process could not be achieved.

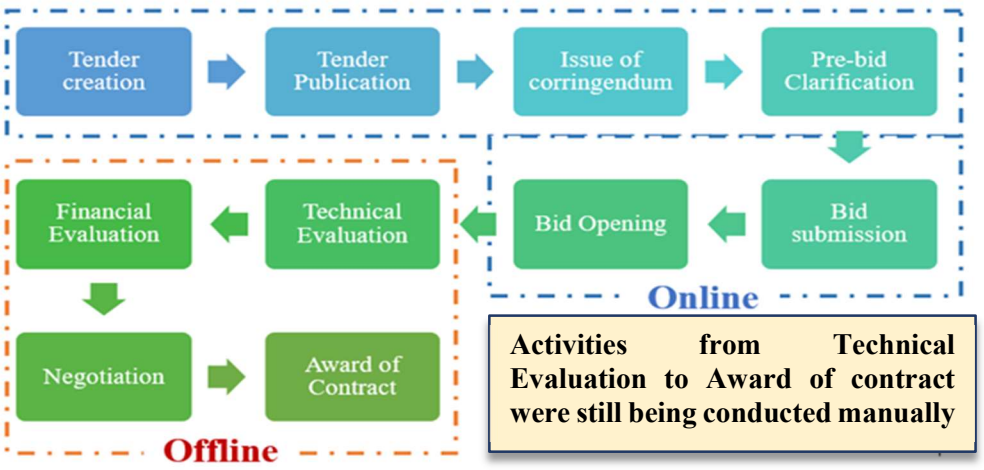
Department agreed (December 2023) about non-development of the modules by NIC. As a result, the pre and post tendering modules of the e-Procurement system are yet to be developed.

2.3 Partial implementation of the e-tendering module

General Control

The e-tendering module was designed to have the following processes:

Figure No 4: E-tendering module



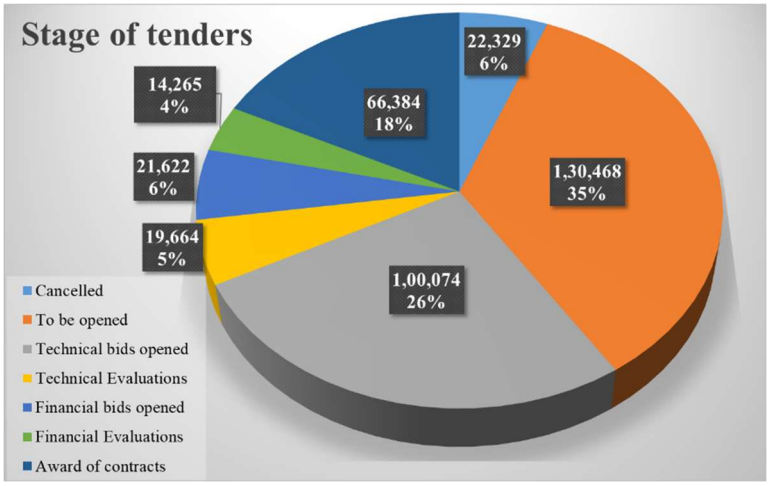
Departmental users, having creator roles, could log on to the portal and create online tenders. Authorised departmental users having publisher roles could verify the created tenders and publish them online. Registered bidders/ contractors could submit online bids and upload required documents till the time defined in the notice inviting tenders. On the bid opening date, departmental users responsible for bid opening could open/ decrypt the bids. The bid opening consisted of four stages *i.e.,* Technical Bid Opening, Technical Evaluation, Financial Bid Opening, and Financial Evaluation, followed by Award of Contract (AoC). Once the comparative statement of bids was generated through the system and L1, L2, L3…identified, L1 could be called upon for negotiation or sample checking. The last stage of e-tendering was the Award of Contract, where the departmental user could upload the award of contract mentioning the final rate finalised with the selected bidder.

As shown in the schematic diagram above, critical functions such as technical evaluation, financial evaluation, negotiation, award of contract were still being carried out manually, outside the e-Procurement system. However, the details of such manual processing viz. technical evaluation minutes, financial evaluation minutes, negotiation minutes with L1 bidder, and award of contract, were required to be uploaded onto the e-Procurement portal, as part of the workflow for the application.

Audit noticed that the details of manual processes for technical and financial evaluation and award of contract were being uploaded onto the e-Procurement portal with significant delays (even up to four years). Thus, the e-Procurement portal did not reflect the real-time, actual status of various tenders in its MIS reports.

Analysis of the stages of tenders revealed that out of 3.75 lakh tenders that were published during 2008-09 to 2021-22, and excluding 22,329 tenders that were cancelled, details of only 0.66 lakh tenders (18.75 *per cent*) had been entered in the Award of Contract process. Out of the remaining 2.86 tenders, 1.30 lakh tenders were depicted at "To be opened" stage, 1.00 lakh tenders at "Technical bid opened" stage, 0.20 lakh tenders at "Technical bid evaluated" stage, 0.22 lakh tenders at "Financial bid opened" stage and 0.14 lakh tenders at "Financial bid evaluated" stage. In 2.74 lakh out of these 2.86 lakh tenders, the delay after expiry of bid validity from the date of bid

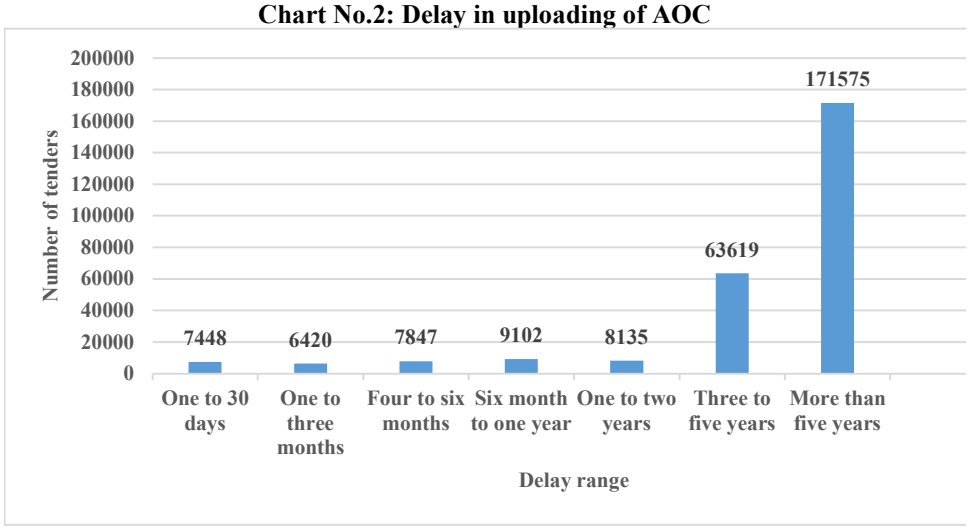
Chart No 1: Stages of Tender



(Source: e-Procurement database)

opening to 31 March 2022 ranged between one to 5005 days, as depicted in the ***Chart-2***.

Chart No.2: Delay in uploading of AOC



Source: Database analysis

Audit test checked 486 sample tenders at 48 selected TIAs to verify whether the status of the tender depicted on the e-Procurement system was correct, and noticed that Award of Contract (AoC) had been completed in 434 tenders as per manually maintained physical records. However, the e-Procurement system reflected the status of these tenders incorrectly, with 326 tenders depicted as at AoC stage while in the remaining 108 (25 per cent) tenders, the AoC details had not been uploaded into the system even after delays ranging up to 1773 days from the actual date of AoCs. Similarly, the details of tenders which had completed the Technical Evaluation and Financial Evaluation stages had not been uploaded into the system.

Further, in 248 out of the 486 test-checked tenders, portable document format (pdf) versions of unrelated/ irrelevant documents (documents containing designations of committee members who evaluated the technical and financial bids, Detailed Notice Inviting Tenders, *etc.*) had been uploaded into the system, instead of the actual minutes of proceedings of technical and financial evaluation committees. This indicated lack of due diligence by the users responsible for correct uploading of documents.

In the absence of online processing of technical and financial evaluation and award of contract through the system with the required application controls, there was avoidable risk of commission of errors/ deliberate irregularity on the part of the Tender Inviting Authorities (TIA) when carrying out these processes manually. One such example, where Audit noticed that the TIA had irregularly extended undue benefits to bidders during tender processing, is discussed in the case study below.

Case study

During test check of tenders Audit noticed that two TIAs- Bhubaneswar Municipal Corporation and Jeypore Municipality- had extended undue benefits to bidders in 30 tenders. This undue benefit was extended either through irregular increase of the value of bids submitted by the bidders or through irregular exclusion of the eligible L1 bidder and award of contract to other bidders with higher bids. Details are tabulated below:

Sl. No.	Nature of irregularity	Number of tenders	Total Tender amount (₹ in lakh)	Total Amount quoted by lowest bidder (₹ in lakh)	Total Amount Awarded (₹ in lakh)	Total Amount irregularly increased (₹ in lakh)
1	Manually increased the quoted value of bids	29	299.59	282.76	301.78	19.02
2	Excluded the eligible L1 bidder from the comparative statement	1	7.05	6.52	6.90	0.38
	Total	30	306.64	289.28	308.68	19.40

The total amount quoted by the Lowest (L1) bidders in these 30 tenders was ₹2.89 crore. However, the actual total amount awarded in these 30 tenders was ₹3.07 crore. This irregular increase would not have been possible, had the processes for technical and financial evaluation of bids and award of contract been carried out through the e-Procurement system, with the required application controls to ensure compliance with the executive instructions. In the absence of the use of the system for these processes, the TIAs had extended undue benefits as above.

Response of the concerned department is awaited (December 2024)

2.4 Absence of master data management functionality for contractors, in e-Procurement system

Project Management

NIC was to develop the Contractor Database Management System (CDMS) as part of the e-Procurement System, as per the As-Is and To-Be document prepared in 2012. However, NIC did not develop this module.

The CDMS was intended to provide functionality for master data management of contractors and was therefore essential to automate the processes of technical evaluation, financial evaluation and award of contract through the e-Procurement system.

As a result of non-implementation of the same by NIC and in the absence of a formal Agreement/ MoU to enforce the same, GoO decided (November 2017) that Works Department would develop the Contractor Database Management System (CDMS) through a different software vendor and to implement the same by April 2018.

Works Department, GoO approved (February 2018) the proposal amounting to ₹3.84 crore and requested the authorised GoO agency, M/s IDCOL Software Ltd (ISL) to initiate the tender process. ISL finalised (31 March 2018) the vendor M/s CSM Technologies Pvt Ltd for Development, Implementation, Maintenance and Support Services of web-based Contractor Database Management System at a cost of ₹3.58 crore and for Operating System and RDMBS (Operational) at ₹63.60 lakh. The project was to be completed within six months from date of award, in three phases.

In Phase II, there was provision for integration with e-Procurement portal for master data management for contractors. The Department issued (July 2019) User Acceptance Test (UAT) certificate for the developed CDMS software Phase-I, Phase II and Phase III.

However, Audit noticed that even as of December 2023, the integration of CDMS with e-Procurement had not been implemented, and the User Acceptance Test certificate had been issued by the Department without verifying the actual status of implementation. Such issue of the UAT certificate without exercising due diligence resulted in extension of a significant undue favour to the vendor.

Due to non-integration of e-Procurement system with CDMS, the processes of technical and financial evaluation and award of contract continued to be carried out manually outside the system, with the material risk of commission of errors/ deliberate irregularities.

Accepting the facts, the Department stated (December 2023) that the UAT certificate had been issued by the Department, but later it was found that the assigned works had not been completed. As a result, an amount of ₹2.86 lakh had been withheld as payment to the vendor.

The response was not tenable, since the fact remained that due to the absence of master data management functionality for contractors in the e-Procurement system, key business processes continued to be carried out manually and the Department had not fixed any responsibility for the delay in implementation of CDMS or for the incorrect issue of the UAT certificate.

2.5 Absence of integration with Works and Accounts Management Information System

General Control

Works and Accounts Management Information System (WAMIS) was developed by Center for Development of Advanced Computing (C-DAC) for different Engineering Departments like Rural Development, Roads & Building, Water Resources and Housing & Urban Development in Government of Odisha and implemented (May 2009) the application through Rural Development Department. Along with other functionalities, WAMIS has a facility for pre-tender activities such as Administrative Approvals, Technical Sanctions, preparation of BoQ, Tendering, Quotations, Awarding, Negotiation and Execution of Works.

To minimise human intervention, introduce automated tendering process and bring transparency in procurement, Government decided (May 2016) for end-to-end integration of e-Procurement system with WAMIS, so that the inputs such as BoQ, e-Estimates could be transmitted from WAMIS to the e-Procurement system, and inputs on award of contract (contractor identity, contract value *etc*.,) from the e-Procurement system could be transmitted to WAMIS. The integration was to be completed in three phases.

- In Phase I, the scope of work included sharing of pre-tendering information such as BoQ from WAMIS to the e-Procurement portal, for creation and publication of tender.
- In Phase II, General Technical Evaluation (GTE) was to be enabled using information available from WAMIS and comparative statement of bidders for technical evaluation was to be auto-generated in the e-Procurement system.
- In Phase III, the scope of work included sharing of post-tender information such as letter of acceptance (e-LoA), Award of Contract/ Agreement (e-AOC/e-Agreement) from the e-Procurement system to WAMIS.

The target date for completion of the above integration process was 01 June 2021. However, Audit observed that end-to-end integration of e-Procurement system with WAMIS had not been completed as of December 2023, despite the lapse of more than 2 years after the scheduled completion date.

In reply the Department stated (December 2023) that the integration with WAMIS would be completed after implementation of the new version of GePNIC.

The absence of the intended integration with WAMIS also contributed to the continued use of manual, offline processing of technical and financial evaluation of bids and award of contracts, which carried the significant risk of commission of errors/ deliberate irregularities.

2.6 Absence of executive instructions to revise the threshold value for mandatory e-procurement

General Control

Department of Commerce, Government of India (GoI) vide their letter 17 March 2015 suggested that all States/UTs irrespective of service provider may bring down the threshold value for e-Procurement to ₹1 lakh in a time bound and phased manner by 31 March 2016. All the Departments/Divisions/Rural Bodies/PSUs /Autonomous bodies would be brought under the purview of e-procurement by 30 September 2015. The above objectives regarding e-Procurement would be mandated through Legislation/Executive Orders.

Audit observed that despite implementation of e-Procurement since 2008 and GoI instructions in 2015, out of 40 Departments of Government of Odisha, only 29 Departments had registered in the e-Procurement system and the remaining 11 Departments had not registered themselves. Thus, these 11 Departments had

continued to use other channels for procurement for their Departmental requirements, even after 14 years of implementation of the e-Procurement system.

Further, the threshold value in respect of procurements by Departments of Government of Odisha had remained at ₹2 lakh for ULBs under the H&UD Department, and at ₹5 lakh for all other Departments, even after 6 years from the target date for revising the threshold value down to ₹1 lakh. This meant that there was avoidable risk of non-compliance with the applicable Rules for procurement in offline mode for values between ₹1 lakh and ₹5 lakh for Departments.

As per OPWD Code, contract for works having estimated cost up to ₹5 lakh may be awarded with or without invitation of open tenders, at the discretion of the Divisional Officer. Audit noticed that in the absence of executive instructions mandating the use of e-Procurement system for contract value of more than ₹1 lakh and in view of the provision to not opt for open tender in cases where contract value was less than ₹5 lakh, there were instances of TIAs splitting works to this range of contract value. One such example is described as a case study below.

Case Study
Splitting up of works to bypass e-tendering.

For preparation of detailed architectural design and structural grid of various floors and areas of the 300-bed new building of District Headquarter Hospital at Bhadrak, the Executive Engineer Bhardak R&B Division had submitted estimates splitting the original work into 22 works. The concerned Superintending Engineer had approved (June 2021) all the 22 split works limiting the amount in each case to below ₹5 lakh. Each of these 22 split works was awarded (21-24 May 2021) to the same contractor, for a total contract amount of ₹70.52 lakh across the 22 works.

If e-procurement had been mandated with threshold value revised to ₹1 lakh, the risk of such splitting of works could have been mitigated, as the system could have had application controls implemented to detect such instances of splitting of works (using the combination of data fields such as head of account, Division, contractor identity *etc.*,) and report the same to senior Officers of the Department.

Thus, in the absence of executive instructions to mandate e-procurement for contract value above ₹1 lakh, there remained avoidable scope for TIAs to opt for offline procurement with attendant risks, as well as the material risk of splitting of works to avoid escalation to the competent authority.

In reply, the Department stated (December 2023) that the e-Procurement portal has been designed as per the provisions laid down in the OPWD Code. Necessary changes to the system will be made on revision of the Code. The response was not tenable, as the revision of the threshold value for mandatory e-procurement was required to have been implemented in a phased manner by

March 2016 itself, as per communication issued by Government of India and the same was to be incorporated in the OPWD code through revision.

2.7 Absence of functionality in the system to manage privileged bidders

System Design

OPWD Code provides for special privileges[8] to 'B' class SC/ST contractors, Engineer Contractors who are Graduates and Diploma holders, physically handicapped 'D' and 'C' class contractors, Micro and Small Enterprises (MSEs) and Start-ups. Accordingly, the SRS had also provided for functionality in the system to define and manage such privileged bidders.

Audit, however, noticed that no functionality had been implemented in GePNIC to define, create and manage such categories of privileged bidders, except MSE category.

In the absence of such functionality, the TIAs had to adopt manual evaluation of technical bids when such privileged bidders participated in tenders.

Audit noticed that during such manual evaluation in three out of 48 test checked TIAs, there were errors in evaluation and award of contract as discussed below:

2.7.1 Wrongful selection of bidder

In two test checked cases Audit noticed that contractors were selected due to incorrect calculation of 10 *per cent* price preference manually.

- The work "Construction of Drain near proposed Poura Bhawan, ward No 15" was put to tender (June 2021) by Executive Officer (EO), Barbil Municipality with estimated rate of ₹4.46 lakh. Seven bidders participated and all were technically qualified by the committee. In the financial evaluation summary, it was seen that the L1 bidder had quoted ₹4.01 lakh being 9.99 *per cent* less than the amount put to tender. The ST Contractor had quoted ₹4.46 lakh (0 *per cent*) and other five bidders had quoted 9.9 *per cent* excess than the amount put to tender. The EO awarded the work to the ST contractor at ₹ 4.01 lakh by incorrectly calculating the price preference of 10 *per cent* on the quoted amount instead of calculating 10 *per cent* on the lowest quoted bid. The EO admitted (November 2022) the error.
- The tender for work "Construction of Chemical Laboratory Building at Kurmitar Iron Ore Mines in the District of Sundargarh" was floated by Odisha Mining Corporation with tender value ₹40.01 lakh. Two bidders

[8] **(a) SC/ST contractors**: Tender of the individual registered contractors belonging to SC/ST within 10 *per cent* of the rate quoted by the lowest tenderer for any work, would be considered for award to him/her at the lowest tendered rate.
(b) Engineer Contractor: Graduate and Diploma Holder Engineer contractors would pay deposit the security deposits (EMD, Security Deposit, Performance Security) at half the usual rate against the prescribed percentage.
(c) Physically Handicapped (deaf or orthopedically handicapped upto 40 *per cent* disability**)** class D and C contractors are exempted for paying EMD and ISD and would be given 3 *per cent* price preference in the rate quoted in their tenders. The preference will be allowed upto a prescribed limit.

had submitted their bids in response to this tender. One bidder quoted at ₹34.01 lakh being 14.99 *per cent* less than the estimated cost and the other bidder as an SC contractor quoted ₹38.01 lakh being five *per cent* less than the estimated cost. The price preference to SC bidder was ₹37.41 lakh (₹34.01+10 *per cent*). Hence, the quoted amount of SC bidder was not within the price preference and the other bidder should have been declared the L1 bidder. Contrary to this, the TIA incorrectly conducted a lottery between those two bidders and awarded the work to the SC bidder.

2.7.2 Awarding contract at a higher price

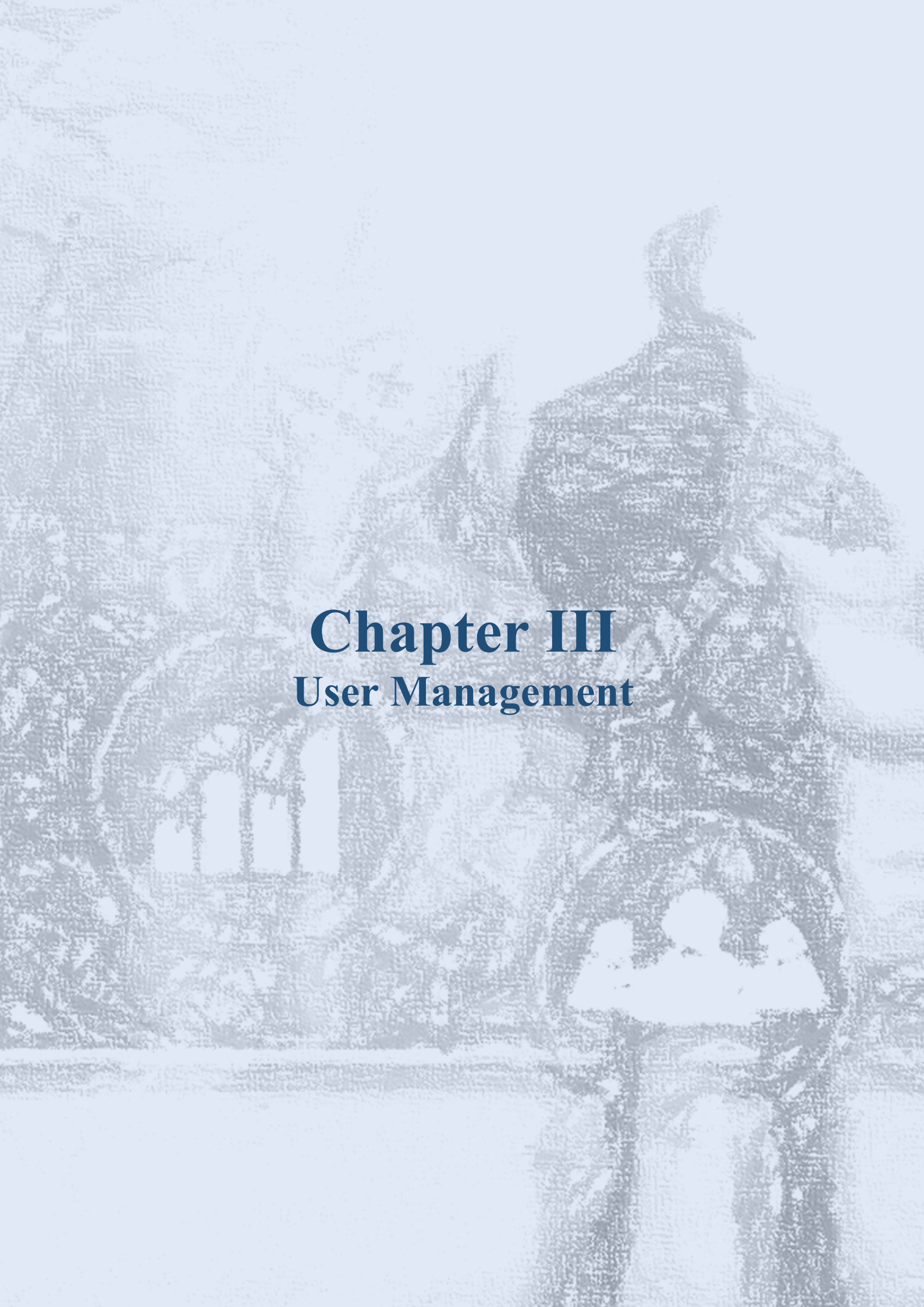
In one out of the test checked tenders involving privileged bidders, Audit found that DFO, Bargarh floated tender for "Construction of Boundary Wall at Kamgaon Forest Section of Bargarh Range" with estimated cost of ₹4.00 lakh. Five bidders had submitted bids out of which three bidders had quoted ₹3.04 lakh being 14.99 *per cent* less than estimated cost, one SC Contractor bid ₹3.32 lakh being seven *per cent* less than estimated cost and other one had quoted at estimated cost. As the price preference of SC contractors was within 10 *per cent* of price quoted by the lowest bidder, the evaluation committee conducted lottery among four of the five bidders and the work was awarded to the SC contractor at an incorrect amount of ₹3.32 lakh instead of ₹3.04 lakh quoted by L1 bidder. This resulted in an extra obligation of ₹0.28 lakh on the Government exchequer. These errors in tender evaluation could have been prevented if the technical and financial evaluation and award of contract had been conducted in the e-Procurement system, with necessary functionality implemented in the system to fully map the business rules related to definition and management of privileged bidders.

In reply the Department stated (December 2023) that the functionality to define and manage privileged bidders had now been made available as a configuration option for TIAs. The response was not tenable, as the requirement of full mapping of business rules to ensure that the e-Procurement system generated comparative sheet of financial bids by taking into account the details of the privileged bidders in order to determine L1 through the system itself, had not yet been implemented.

Recommendations

Government may

- Ensure execution of Agreement/ MoU with NIC, to ensure clarity on timelines, deliverables and service levels.
- Implement the remaining Modules of the e-Procurement system and fully map all the relevant business rules into the system, to ensure that technical and financial evaluation and award of contract is only carried out through the system.
- Integrate WAMIS and CDMS with e-Procurement system, to minimise the risk of manual errors/ deliberate irregularities.
- Adopt the revised threshold value of ₹1 lakh for mandatory e-procurement as prescribed by Department of Commerce, Government of India.



Chapter III
User Management

Chapter III

User Management

3.1 Inadequate validation controls during registration of users

Input Control

The online bidder enrollment form had provision for enrolling suppliers of goods and services, and assigning them login ID/ password for logging into the application software. The system generates unique user ID for each user. For two factor authentication, the user has to register his Digital Signature Certificate (DSC) with the system. On expiry of the DSC, the user must again register the new DSC in the system. In this process, the DSC details like username, user id, serial number of DSC, thumbprint, public key hash, validity date *etc.,* are recorded by the system.

3.1.1 Registration of incorrect DSC/ mapping of same DSC with multiple bidders

Input Control

Audit analysed the names of the bidders and the names of the holders of the DSC which the bidders had registered, and noticed that out of 1,751 bidders, in 1,120 cases the names did not match and the same DSC had been mapped to multiple bidders. This indicated that the name of the bidder had not been validated at the time of registration of DSCs used by the bidder.

Due to the absence of this validation control (verification by a Departmental user in the system), the DSC used by the bidders did not have the essential attribute of non-repudiation. A bidder could potentially disown any bids or inputs submitted into the system on the grounds that the action had not been performed by him, since the DSC used to digitally sign off on such actions was not registered in the name of the bidder or was mapped to multiple bidders in the system. This was a major deficiency in the e-Procurement system, given the nature of its functions.

Department replied (December 2023) that since Certifying Authorities issue DSC to individuals with different alias names and since individuals authorised to bid on behalf of a company may change over a period, mapping the names of the bidders and the names of the DSC holders was not feasible.

However, the fact remains that matching the DSC details with the bidder's identity is crucial to prevent impersonation or unauthorised actions.The system should not permit registration of DSC without first validating that the name of the bidder matches the name of the DSC holder, to uphold the essential attribute of non-repudiation.

3.1.2 Absence of application control to verify the validity period of DSC used by bidders

Input Control

DSCs were mapped to bidders and each DSC has a defined validity period, as specified by the DSC Certifying Authorities. In order to uphold the essential attribute of non-repudiation, the e-Procurement system should have had application control to verify the validity of the DSC, when a bidder sought to digitally sign inputs into the system.

Audit noticed that such an application control had not been implemented in e-Procurement system. This was evidenced by the fact that the database had 23 instances in which bidders had uploaded bids/ submitted inputs into the system after the date of expiry of validity of their DSCs. This was a major deficiency in the application controls implemented in the system.

In response, Department admitting the fact, stated (December 2023) that validity checking of DSCs was being carried out at the time of user logging into the system. The response was not tenable as the instances noticed by Audit clearly showed that the validity of the DSC had not been verified by the system.

3.2 Deficiencies in application control to correctly record PAN for registered bidders

General Control

As per functional requirement specification of the system, the online user registration forms shall clearly indicate which fields are mandatory and validation controls shall be implemented to ensure that all the mandatory fields are filled with valid and relevant data by the user. Bidders should be registered with correct Permanent Account Number (PAN) issued by the Income Tax Department, Government of India and system should ensure that each unique PAN recorded in the system is mapped to the concerned bidder only, and not to multiple bidders registered in the system.

3.2.1 Recording invalid PAN during registration of bidders

Input Control

As per design of the PAN, the fourth character of PAN represents the status of the PAN holder. C stands for Company, P for Person, H for Hindu Undivided Family (HUF), F for Firm, A for Association of Persons (AOP), T for AOP (Trust), B for Body of Individuals (BOI), L for Local Authority, J for Artificial Juridical Person and G for Government. If any other letter presents in fourth character of PAN, it is invalid. Further, as PAN was a mandatory field, the data field should not be permitted to be left blank at the time of registration of the bidder.

Audit analysed the tenderer/ corporate tenderer profile table of the system and noticed that there were 80,304[9] users registered. Out of these 80,304 users, the PAN of 154 users as recorded in the table was either blank or invalid, as fourth character of the PAN did not belong to the set of permissible letters.

Out of these 154 users having blank/ invalid PAN, 39 users had been irregularly permitted to submit bids in 600 tenders and in 11 tenders, had even been irregularly awarded the contract.

Thus, GePNIC had deficiencies in validation controls to mandate entry of PAN and to verify the correctness of the PAN data entered in the concerned data field, during registration of the bidders.

This deficiency resulted in the material risk of participation of the same bidder with multiple bids in the same tender, and consequent risks of award of contract on the basis of competitive bids which had all been submitted by a single bidder using different user IDs.

3.2.2 Mapping the same PAN to multiple user IDs during bidder registration

Input Control

Permanent Account Number (PAN) is a unique number issued by the Income Tax Department to various persons like individuals, HUF, company, BoI, Government *etc.* Therefore, each bidder in the user master table should have only one PAN and multiple bidders should not be registered with the same PAN.

Out of 80,304 bidders registered in the system, Audit analysed the bidder data and their PAN and noticed that in case of 25,109 bidders, the PAN number was not unique, *i.e.,* the same PAN number was also found mapped to other bidders (ranging from 2 to 212) in the database.

Out of these 25,109 bidders having non-unique PAN,

- 10,124 bidders had submitted 2,82,229 bids for 1,55,235 tenders.
- 1,156 bidders had been awarded contract for 4,347 tenders valued at ₹ 11,694.36 crore.
- The above included 29 bidders with the same PAN (but different user IDs) who had submitted 88 bids (ranging between 2 to 4 bids) in the same tender, on 39 occasions. Due to lack of validation controls to prevent duplicate PAN mapped to multiple bidders, these 29 bidders had submitted 2 to 4 bids in the same tender, as illustrated in an example below:

[9] There are 80,304 bidders in the bidder profile tables against 80,310 bidder users in the user master table because 6 bidder users did not have records of their profile data.

Case Study

Multiple bidders mapped to the same PAN and participating in the same tender

1. A total of 13 bids were submitted for the tender "Expression of Interest for selection of authority engineer for construction of four lane dedicated coal corridor from Bankibahal (coal mines) to Bhedabahal (Sh-10) from 0/000 to 30/811 km". In these 13 bids, two bids were submitted by bidders having different user IDs but the same PAN. However, without rejecting the bids received from the common bidder, the TIA considered the bids as valid and awarded the contract to one of the two bids, which was determined to be L1. The reason for considering the two bids from different user IDs but having the same PAN as valid during evaluation of bids, was not found on record.
2. A total of three bids were received for "Engagement of transport contractor for transportation of different seeds for the period from 01 January 2022 to 31 December 2023 for Bhubaneswar zone". In these three bids, two bids were submitted by bidders having different user IDs but the same PAN. However, without rejecting the bids received from the common bidder, the TIA considered one of the two bids as valid and went ahead with the bid evaluation process. The reason for considering one of the two bids from different user IDs but having the same PAN as valid during evaluation of bids, was not found on record.

The Department had not conducted any review to identify and eliminate such user IDs which had been mapped incorrectly to PAN not belonging to the user. There was no application control to flag and prevent mapping of an already registered PAN to a new user at the time of bidder registration.

This deficiency in the application control to prevent mapping of same PAN to multiple users resulted in the material risk of participation of the same bidder with multiple bids in the same tender, and consequent risks of award of contract on the basis of competitive bids which had all been submitted by a single bidder using different user IDs.

3.2.3 Manual entry of incorrect PAN by bidders during submission of bids

Input Control

As per system design, a copy of profile of bidder details like company name, business nature, mobile number, PAN, registration number, created date and address of bidder is captured in a separate bidder profile table against each bid during bid submission by the bidder.

Audit noticed that instead of auto-populating the PAN from the master data for the user as recorded during bidder registration, the system permitted manual entry of PAN once again during the time of submission of bids.

This deficiency in the system design had resulted in 244 bidders having manually entered different PAN numbers during bid submission in the different tenders that they had participated in.

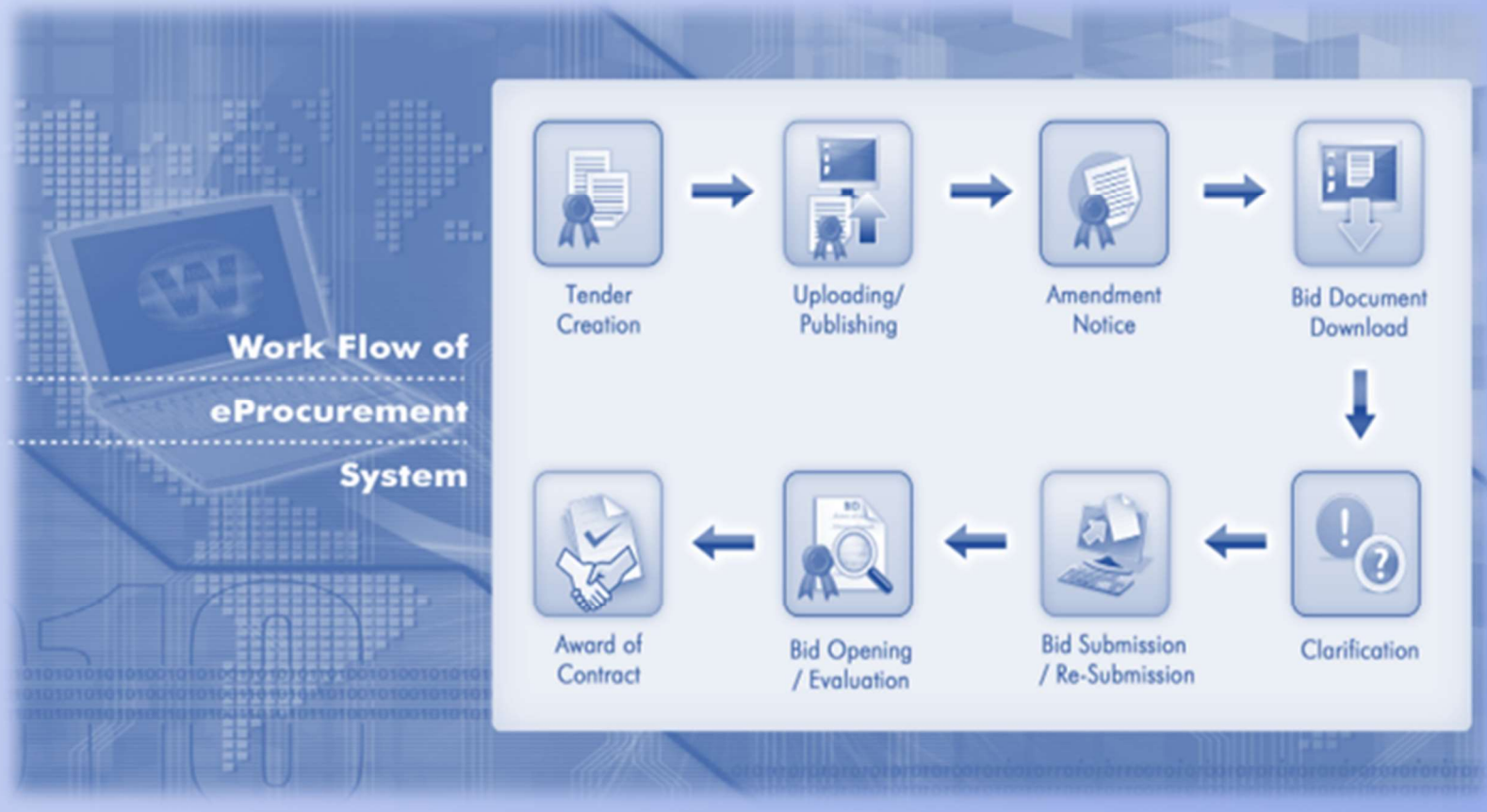
Department accepted these above observations and stated (December 2023) that integration of Goods and Services Tax Number (GSTN) with e-Procurement system is being planned, and that validation controls for PAN will be implemented once that integration is in place.

Recommendation

Government may implement appropriate validation controls for user access management during the registration of bidders, to ensure that

- Valid DSCs, PAN, dates *etc.,* are entered into the system in compliance with executive instructions.
- The essential attribute of non-repudiation is upheld in the system.

Chapter IV
Tender Creation and Publication



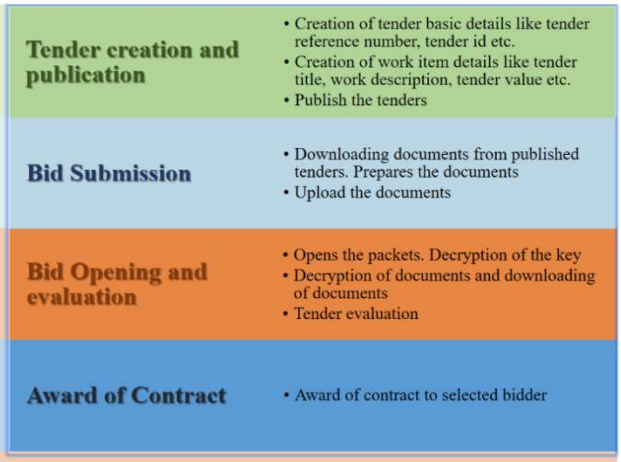
Chapter IV

Tender Creation and Publication

4.1 Deficiencies in the workflow for tender creation

As per system design, the tender creator was required to complete the tender publishing process by providing information like basic details such as notice inviting tender, work details, fee details, critical dates, and Bill of Quantity (in MS Excel format) *etc.* The tender documents were required to be uploaded into the e-Procurement system. According to the BoQ template, the bidders were required to submit their bids in the system by digitally signing, encrypting and uploading the technical and financial bid documents. After opening of the bids, details of the opened bids such as bid documents, decryption date, file names, uploaded dates, file sizes against each bid were required to be stored in the system.

Figure No 5: Tender process flow



Audit analysed the dataflow in the system for the above processes and observed the following inconsistencies:

4.2 Absence of application control to enforce minimum period for submission of bids

System Design

As per OPWD Code Vol-II, Annexure XI as amended on 19.01.2004, time limit between issue/publication/sale and receipt of bids is stipulated as follows:

Table No. 1: List showing threshold limit of time limit between issue/ publication/sale and receipt of bids

Estimated cost put to tender	Minimum number of days	Maximum number of days
Not exceeding ₹50 lakh	10	15
More than ₹50 lakh but not exceeding ₹3 crores	15	21
More than ₹3 crores	15	30
Very large and complex project	21	45

(Source: OPWD Code)

Further, in case of corrigendum issued to the tenders, minimum seven days' time is to be provided for bid submission from the date of publication of corrigendum.

Data analysis revealed that out of 3,74,806 tenders published up to 31 March 2022, fewer days than stipulated were provided for submission of bids in 82,994 tenders. The fewer days provided for submission of bids ranged between 1 and 14 days as follows:

Table No. 2 : List showing deviations in threshold limit of time limit between issue/publication/sale and receipt of bids

Tender value	Minimum permissible days	Number of tenders where fewer days provided
<=5000000	10	64,199
>5000000 and <=30000000	15	16,604
>30000000	15	2,191
Total		**82,994**

(Source: Database analysis)

Further, in 421 out of 69,163 corrigenda, the time given from date of publication of corrigendum to date of bid submission closing date was less than seven days. The fewer days given ranged between one to six days.

During the test check of tenders, Audit found that in 168 out of 486 tenders, fewer days were allowed than prescribed for bid submission ranging between one to nine days. There was no reason for giving fewer days to bidders for submission of bids.

Audit concluded that the business rule specifying the minimum period for submission of bids had not been mapped into the system in the form of application control to enforce the minimum period for submission of bid based on tender value.

Department stated (December 2023) that while OPWD Code has provisions for different time periods for submission of bids based on tender value, TIAs can reduce the time prescribed.

The response was not tenable, since lack of this application control meant that the possibility of prospective bidders being deprived from participation in the tendering process due to lack of adequate time and the possibility that TIAs could favour certain selected bidders by giving them the tender details in advance of the tender publication date on the system, could not be ruled out. The lack of compliance with the minimum prescribed time period for submission of bids adversely impacts the objectives of transparency and fairness in the procurement process and hence, this is a major control failure in the system.

4.3 Absence of application control to enforce two-cover process for tenders with value more than ₹50 lakh

General Control

OPWD Code provided for two cover process for tenders costing above ₹50 lakhs - one cover containing technical bid and other containing financial bid.

Data analysis revealed that out of 3,74,806 tenders, single cover process had been followed in 4,045 tenders despite the tender value ranging between ₹50.10 lakh and ₹752.00 crore, instead of following the two cover system. The year wise details of number of tenders with single cover with minimum and maximum value of tender is given as below:

Table No.3: Statement showing year-wise number of tenders invited with single cover instead of double cover with minimum and maximum value of tenders

Year	Number of tenders	Minimum tender value (₹ in crore)	Maximum tender value (₹ in crore)
2008-09	4	0.90	3.77
2009-10	25	0.50	141.20
2010-11	68	0.51	138.87
2011-12	189	0.50	181.35
2012-13	101	0.51	11.23
2013-14	736	0.50	187.06
2014-15	670	0.50	224.13
2015-16	377	0.50	752.00
2016-17	334	0.50	221.88
2017-18	431	0.50	116.17
2018-19	432	0.50	9.57
2019-20	221	0.50	13.00
2020-21	210	0.50	22.23
2021-22	247	0.50	22.23
Total	**4045**	**0.50**	**752.00**

(Source: e-Procurement database)

Audit noticed that the number of tenders irregularly following single cover process instead of the applicable two cover process had been increasing over the above period.

Audit test checked 486 tenders for detailed scrutiny and found that out of 129 tenders with tender value more than ₹50 lakh, in case of seven tenders, single cover process had been irregularly followed, without recording any reasons for the non-compliance with the Code.

Audit concluded that the business rule for following two cover process for tenders having value more than ₹50 lakh had not been mapped as an application control in the e-Procurement system. The workflow permitted the Departmental user to opt for single cover process even when the tender value was more than ₹50 lakh.

The Department accepted (December 2023) that NIC had not implemented the application control to make two cover process mandatory for tenders with value more than ₹50 lakh.

4.4 Loss of tender fees due to absence of mapping of fees based on the tender value

System Design

As per Rule 15 to Appendix IX of OPWD Code Vol-II, the tender fees is based on the value of tender, as follows:

Table No.4: Statement showing cost of tender papers according to tender value

Tender Value	Tender Fees
Tenders costing up to ₹ 10,000	₹200
Tenders costing over ₹10,000 but below ₹1.00 lakh	₹400
Tenders costing over ₹1.00 lakh but below ₹2.00 lakh	₹600
Tenders costing over ₹2.00 lakh but below ₹5.00 lakh	₹2,000
Tenders costing over ₹5.00 lakh but below ₹10.00 lakh	₹4,000
Tenders costing over ₹10.00 lakh but below ₹50.00 lakh	₹6,000
Tenders costing over ₹50.00 lakh and above	₹10,000

(Source : OPWD Code)

In the "As-is and To-be" document the same was also considered for development of software.

Data analysis revealed that out of the 3.75 lakh tenders published up to 31 March 2022, in 10,152 tenders the Tender Inviting Authority (TIA) had invited tender with less than the prescribed and applicable tender fees. The shortfall in tender fees ranged between ₹75 and ₹9,999. In eight tenders, the tender fees had been fixed as ₹1 instead of ₹10,000. On verification with the DTCN, Audit noticed that these had arisen due to manual computation by users and subsequent data entry errors.

Hence, due to non-mapping of the business rule for computation of tender fees based on tender value in the system as a processing control, incorrect data had been manually entered into the system by users, resulting in non-compliance and loss of revenue for the Government.

The tender value wise number of tenders and number of bids for which less tender fees was collected was as follows:

Table No.5: Statement showing tender value wise number of tenders and number of bids for which less tender fee was collected

Sl No	Tender value range	Number of tenders	Number of bids	Tender fees applicable based on tender value (₹ in lakh)	Tender fees actually paid by bidders (₹ in lakh)	Shortfall in tender fees paid by bidders (₹ in lakh)
1	Tenders costing over ₹50.00 lakh and above	13	23	0.09	0.06	0.03
2	Tenders costing over ₹10.00 lakh but below ₹50.00 lakh	742	1550	9.30	7.19	2.11
3	Tenders costing over ₹5.00 lakh but below ₹10.00 lakh	1061	3434	206.04	151.65	54.39
4	Tenders costing over ₹2.00 lakh but below ₹5.00 lakh	2008	4866	97.32	34.19	63.13
5	Tenders costing over ₹1.00 lakh but below ₹2.00 lakh	1798	5168	206.72	111.73	94.99
6	Tenders costing over ₹10,000 but below ₹1.00 lakh	366	1862	186.20	110.01	76.19
	Total	**5,988**	**16,903**	**705.67**	**414.83**	**290.84**

(Source: e-Procurement database)

The above finding was verified during test-check of tenders in selected TIAs, wherein it was found that in 16 tenders, tender fees of ₹2.13 lakh was collected against the applicable fees of ₹3.46 lakh resulting in shortfall of ₹1.33 lakh.

The Department accepted (December 2023) the Audit observation and stated that the business rule would be mapped into the system.

4.5 Deficiencies in computation of tender value

As per para 3.5.6 of OPWD code and Appendix IX of OPWD Code volume - II, tender for works should be invited only after a detailed estimate showing quantities, rates and amounts of various items of works and specifications to be adopted are prepared and sanctioned by competent authority. The tender documents comprise (i) the notice inviting tenders (NIT) in the prescribed form, (2) the schedule of quantities of works, (3) complete specifications of the work to be done, (4) a set of complete drawings and (5) the form of tenders be used along with a set of special conditions.

In the notice inviting tender, the BoQ is also required to be uploaded by the Tender Inviting Authority (TIA). The amount put to tender (tender value) in the Notice Inviting Tender should match the total estimated amount in the BoQ.

4.5.1 Deficiency in validation controls in BoQ template published in tenders

Input Control

As per system design, the BoQ template (in MS Excel format) containing details of various items, quantities, rate and amount for the work and NIT was to be uploaded by the TIA while creating the tender.

After submission of bids as per BoQ template and during financial evaluation, comparative statement is generated by the system, with the total amount of the BoQ computed as tender value.

Analysis of the e-Procurement system data revealed that in four out of 3.75 lakh tenders, the total amount of the BoQ were stored as 'NaN', instead of the correct numerical tender value.

Further, in 257 tenders, the items in the BoQ had been irregularly recorded more than once in the database, resulting in mismatches between the tender value stored in the system and the total amount of the BoQ. The year wise details of such tenders were as follows:

Table No.6 : Statement showing discrepancy between figures of BoQ and database

Year	Number of tenders	Total amount put to tender (₹ in crore)	Total BoQ amount of tenders (₹ in crore)	Difference between tender value and BoQ amount (₹ in crore)
2010-11	12	3.94	7.87	3.94
2011-12	5	2.07	4.13	2.07
2012-13	8	14.54	29.09	14.54
2013-14	70	81.97	163.93	81.97
2014-15	81	30.2	60.41	30.2
2015-16	24	6.88	13.76	6.88
2016-17	3	2.66	5.32	2.66
2017-18	1	0.04	0.07	0.04
2018-19	14	27.83	55.67	27.83
2019-20	2	0.09	0.19	0.09
2020-21	1	11.1	22.2	11.1
2021-22	36	265.64	531.28	265.64
Total	**257**	**446.96**	**893.92**	**446.96**

(Source : e-Procurement database)

Due to irregular recording of BoQ items more than once by bidders and the storage of such data in the database, the total BoQ amount did not match the tender value declared in the published documents. This mismatch had occurred due to deficiencies in the validation controls implemented for recording inputs from bidders in the published BoQ templates.

In the absence of automated processes within the system for technical and financial evaluation and award of contract, this deficiency created material risk of errors/ deliberate irregularities during manual processes for bid evaluation in these tenders.

4.5.2 Deficiency in processing controls to compute tender value based on BoQ

Input Control

The tender value, *i.e.,* the amount put to tender in the Notice Inviting Tender should match with that of the total estimated amount in the BoQ for which tender was invited, as tender fee and Earnest Money Deposit (EMD) amount to be deposited is dependent on the tender value.

Analysis of database revealed that in 1.34 lakh out of 3.75 lakh tenders, the BoQ amount did not match the tender value.

The year wise details of the number of tenders in which tender value and BoQ amount differed were as follows:

Table No.7 : Statement showing year-wise discrepancy between figures of BoQ and tender amount in database (₹ in crore)

Year	Number of tenders	Total amount put to tender	Total BoQ amount of tenders	Difference between tender value and BoQ amount
2010-11	2,899	976.77	970.94	5.83
2011-12	7,598	5,336.83	5,306.57	30.26
2012-13	10,125	6,420.57	6,335.26	85.31
2013-14	14,487	7,365.23	7,147.65	217.58
2014-15	11,393	5,009.27	4,877.33	131.94
2015-16	11,697	5,049.20	4,872.79	176.42
2016-17	13,095	4,651.51	4,402.66	248.85
2017-18	15,677	12,897.30	7,430.40	5,466.92
2018-19	15,264	9,514.87	9,500.49	14.38
2019-20	8,979	3,203.64	3,180.55	23.09
2020-21	9,074	5,016.01	4,153.16	862.85
2021-22	14,018	8,198.88	7,892.92	305.96
Total	**1,34,306**	**73,640.08**	**66,070.72**	**7,569.39**

(Source: e-Procurement database)

Audit noticed that these differences had arisen because the Departmental users were expected to manually enter the tender value into the concerned data field, instead of the system computing the same based on the details entered in the BoQ. The absence of this processing control resulted in material risk of incorrect manual entry of tender value, and consequent shortfalls in collection of tender fees and Earnest Money Deposit.

The Department stated (December 2023) that the responsibility of entering the correct tender value was that of the concerned TIAs.

The response was not tenable, as it only reflected the fact that the responsibility for ensuring compliance remained on the individual users instead of shifting to the system through the implementation of necessary controls.

Recommendation

Government may consider to

- Implement mapping of business rules for minimum period for submission of bids, mandatory two-cover process for tenders with value more than ₹50 lakh and computation of tender fees based on tender value;
- Implement validation controls to ensure correct recording of bids in the BoQ template and processing controls for correct computation of tender value based on BoQ in the system.

Chapter V
Bid Creation and Submission

Chapter V

Bid Creation and Submission

5.1 Deficiencies in the workflow for creation/ submission of bids

As per system design, while creating tender, the tender creator enters the critical dates like published date, document sale start date, document sale end date, seek clarification start date, seek clarification end date, bid submission opening date, bid submission closing date and bid opening dates for the tender published. During bid submission by the bidder, the bid submission date timestamp is stored in bids table. As per system requirement, the system shall not accept any bids after bid submission end date and time. System shall also terminate all bid submission process related to those tenders where bid submission has started before bid submission end date and time and reached the deadline.

5.1.1 Absence of application controls to prevent submission of bids after expiry of tender closing time

System Security

As per system workflow, no bids should be permitted to be submitted after tender closing time.

Data analysis revealed that there were 228 bids relating to 224 tenders where bids had been submitted after bid closing time, ranging between 0.026 fraction of seconds to 3 days 3 hours 37 minutes. The year wise details of the number of bids submitted after bid submission closing time was as follows:

Table No.8: Year-wise submission of bids after tender closing time

Year	Number of bids	Number of tenders	Minimum time after bid submission closing time (in days HH:MM:SS)	Maximum time after bid submission closing time (in days HH:MM:SS)
2007-08	1	1	2 days 01:47:44.252	2 days 01:47:44.252
2008-09	15	12	00:00:41.868	3 days 03:37:30.351
2009-10	16	16	00:00:01.052	00:03:18.619
2010-11	45	44	00:00:00.168	00:05:02.318
2011-12	25	25	00:00:00.946	00:02:00.4
2012-13	65	65	00:00:00.363	00:18:47.57
2013-14	37	37	00:00:00.026	00:02:56.201
2014-15	7	7	00:00:00.062	00:00:44.045
2015-16	3	3	00:00:00.415	00:39:32.234
2019-20	1	1	00:00:00.137	00:00:00.137
2021-22	13	13	00:00:00.368	00:01:27.23
Total	228	224		

(***Source : extracted from e-Procurement database)***

This significant and material irregularity had arisen due to either absence of application controls to prevent submission of bids after tender closing time or due to manual intervention at the back end of the system.

Audit noticed that the Department had not conducted a detailed review of this data from the system and determined the root causes for such discrepancy, which created doubts on the integrity of the procurement process.

The Department stated (December 2023) that minor differences in bid submission time and tender closing time could take place due to latency issues in the application server, and such latency and performance issues had been addressed and fixed in September 2021.

The response was not tenable, as the data above shows that the differences between bid submission time and tender closing time ranged up to three days, which cannot be the result of any server latency issue but is strongly indicative of application controls not functioning at the front end or manual intervention at the back end of the system.

5.1.2 Absence of validation controls to enforce chronological sequencing of actions

Processing Control

As per system workflow, bids could be created only after document sale start date of a work item put to tender, and bids could only be updated after they were created.

However, Audit analysed the e-Procurement database and observed that

- A total of 14 bids pertaining to 12 tenders had been recorded as created before the tender document sale start date, with the difference in time ranging from 16 hours to 15 days.
- A total of 2,192 bids had bid update time recorded as before the bid creation time.
- A total of 6,26,115 bids had bid uploaded time recorded as before the bid creation time, with differences ranging up to 60 days.

The above findings indicated that there were inadequate validation controls to enforce correct recording of time and enforcement of chronological sequencing of user actions in the system, and hence there was absence of timestamping integrity in the system.

The Department stated (December 2023) that this issue had been fixed in April 2016.

The response was not tenable, since no patch management reports were furnished to Audit and the issue of inconsistent/ illogical timestamps persisted in 2022.

5.2 Absence of application controls to prevent mapping of same mobile number to multiple bidders

Input Control

As per system design, bidder details such as company name, mobile number, PAN, registration number, created date and address of bidder is recorded in the system during bidder registration.

There was provision in the system to intimate registered bidders through SMS on their mobile numbers about tender publication, corrigenda published after tender publication, status of technical evaluation and financial evaluation, and status of award of contract. Hence, the mobile number plays a significant role in the e-Procurement system for sending SMS intimation on various events. Audit analysed the data on registered bidders in the system and noticed that

- Out of the 80,310 registered bidders, 1,385 bidders had invalid mobile numbers and hence, could not receive any SMS intimations at all.
- Of the remaining 78,925 registered bidders with valid mobile numbers, 27,069 registered bidders had been mapped to 10,571 mobile numbers, with the same mobile number being mapped to multiple registered bidders. The number of registered bidders mapped to the same mobile number ranged between two and 296.
- A total of 106 mobile numbers which were registered by Departmental officials were found to be mapped to 1,264 registered bidders.
- During bid submission, instead of auto populating the mobile number data field from the master data for registered bidders, the bidders were expected to once again enter their mobile numbers manually. As a result, there were instances of the same mobile number being entered by multiple bidders during the bid submission, which were different to the one that they had used during bidder registration.

The above circumstances indicated that the absence of application controls to prevent the mapping of the same mobile number to multiple bidders, and lapses in the process of authentication of the mobile numbers through OTP, at the time of registration. The mapping of the same mobile numbers to Departmental officials and registered bidders indicated material risk of either lack of due diligence during data entry or probable collusion. This material risk should have been mitigated through implementation of necessary application controls to prevent duplication in mapping of the mobile numbers.

During field verification by Audit of 486 test checked tenders, it was seen that in 11 tenders, 18 bidders had submitted bids with the same mobile number. Scrutiny of tender documents revealed that they were close relatives of one another (siblings, father-son, mother-son, husband-wife). The Tender Inviting Authority had technically qualified these bidders without any investigation, indicating either lack of due diligence or collusion between the bidders and the department officers. In such six cases, such bidders had also been awarded the contract.

The Department stated (December 2023) that as certain organizations require two login IDs and may have the same mobile number mapped, it is not possible to impose unique constraint for mobile numbers. However, verification of the mobile number through OTP at the time of registration would be considered.

The response was not tenable, in view of the nature of risks as outlined above.

Recommendation

Government may consider to

- Enforce application controls to prevent submission of bids after tender closing time;
- Implement validation controls to enforce chronological and logical sequencing of user actions in the system;
- Implement application controls to prevent mapping of the same mobile numbers to multiple users in the system, and enquire into cases where the same mobile numbers had been mapped to Departmental users and bidders.

Chapter VI
Bid Opening and Evaluation

Chapter VI

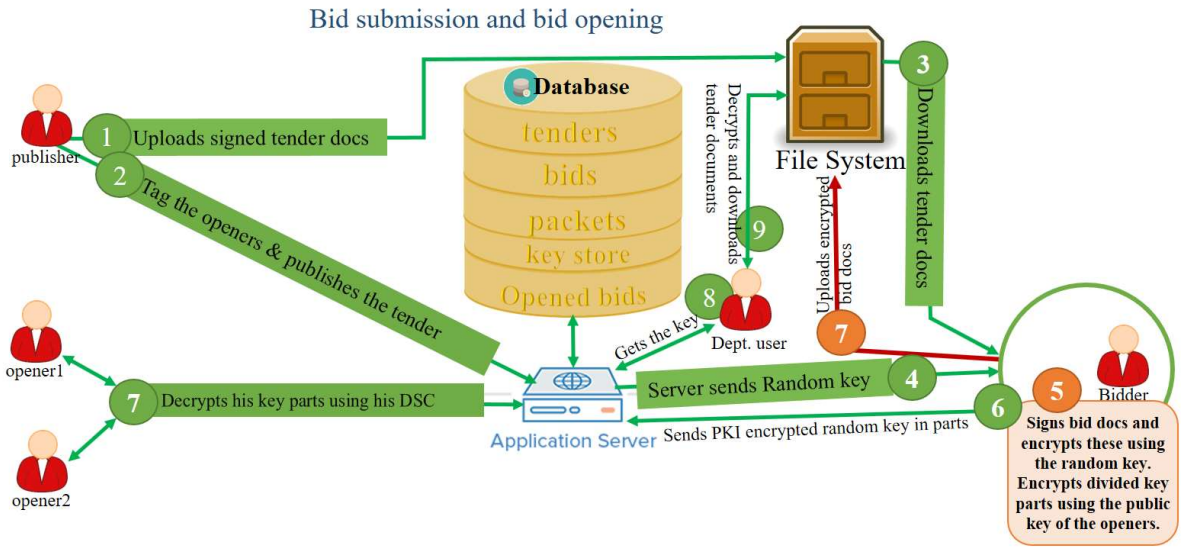
Bid Opening and Evaluation

6.1 Packet opening and bid decryption

As per SRS, the system shall support encryption of bids submitted by the bidder, using the Public Key of the Bid Opening Authority. Encryption shall be done at the client side, and the encrypted bid shall be time locked by the system, till the time of bid opening. Only the Bid Opening Authority shall be able to decrypt the submitted bids only at the bid opening time, using the Private Key of the Bid Opening Authority. There were two types of processes for bid opening- single cover and two-cover.

In case of two-cover process, stage wise bid opening and decryption is to be followed, with the financial bid cover remaining encrypted till the completion of technical evaluation. Financial bid cover would be decrypted only for those bidders who have qualified in the technical evaluation.

Figure 6: Flowchart showing processes of bid submission and bid opening



In the bid opening process, the designated bid openers first opens the cover packet (**Step 7** in above picture). The date of opening is recorded in the database. After that, each bid of the tender is decrypted by the authorised departmental user one by one (**Steps 8 and 9)** and the date of bid decryption is recorded in the database.

The e-Procurement system was implemented in Odisha in July 2008. A total of 3,22,897 tenders were published up to 31 March 2022 against which 17,42,000 bids were received. Audit analysed the database tables with data related to opening and decryption of bid packets, and found the following inconsistencies.

6.1.1 Risk of change in bid openers through manual intervention at the back end of the system

System Security

As per system design, at the time of creation of tender, the tender creator selects the bid openers. The system allows configuring any four bid openers out of which any two or three can open the bid at the actual bid opening time. The details of bid openers is recorded in the database. At the time of submission of bid documents by bidders, the documents are digitally signed by the bidder and encrypted using the bid openers' public key. The details of bids, bid openers, and the random encryption key data are stored in the key store table of the system in parts, thereby ensuring that nobody can open or decrypt the bid.

At the time of tender opening, the tender is opened online by the authorized bid openers who have been configured at the time tender creation. Any two, three or four officials as configured can open the bids once the bid opening date and time is reached. The decryption key is updated in the key store at the time opening of tender. Then the encrypted bid documents are decrypted and opened one by one by the bid opener. As the decryption key is updated at the time of opening of tender, the bid opener should be same as defined at the time of creation of tender.

Audit analysed the data in the bid openers master table and the key store table in the system and noticed that in three tenders, the bid openers as per the key store table were not the ones recorded in the bid openers master table, as follows:

Table No.9 : List showing undesignated tender openers

Sl. No	Tender ID	Bid opener id in key store table not matching bid openers master table
1	7687	2793
2	7691	884
3	87361	18037

(Source: e-Procurement database)

At the time of bid submission by the bidder, the symmetric key was encrypted using the public key of the bid opener as defined in the bid opener master table. However, the system recorded that decryption of the symmetric key had been carried out by another user's private key. This indicated that in these cases, the bids had been opened by users other than the designated bid openers and raised doubts on the integrity of the procurement process.

The Department stated (December 2023) that at the early stage of the application, there was a deficiency in the process of changing bid openers, which had resulted in this anomaly and had been subsequently fixed.

The response was not tenable, as Audit noticed that in one of the three tenders, there was evidence of another bid opener having been added to the bid opener master table through manual intervention at the back end of the system. As a result, Audit was unable to derive assurance that integrity of the process of

designating bid openers in the absence of a clear and verifiable trail of user actions in the system.

6.1.2 Risk of modification of decrypted bid data through manual intervention at the back end of the system

System Security

As per system flow, after opening of submitted bids against a particular tender, the bids are decrypted and stored in the 'bid decrypted' table. The 'bid decrypted' table had columns like bid identity number, packet identity number, date of decryption, the user id of the user who decrypted the bid and the tender ID. Hence, for every bid decrypted, the corresponding tender ID should have been populated in the decrypted table and there should not be any null value in the tender ID data field against any decrypted bid, otherwise the link between the tender and the decrypted bid will be lost.

Audit analysed the 'bid decrypted' table and noticed that

- A total of 15.39 lakh bids pertaining to 2.61 lakh tenders published up to 31 March 2022 had been decrypted. Out of these, 1.79 lakh decrypted bids pertaining to 50,627 tenders had tender ID recorded as 'NULL', which was highly irregular.

  As bid decryption was an automated process in the system and since every bid has to have referential integrity with respect to a particular tender, the recording of the tender ID as 'NULL' indicated the material risk that these values had arisen as a result of manual intervention at the back end of the system by the Data Base Administrator, bypassing the application controls for the decryption process.

  The Department stated (December 2023) that there had been an error in the object relational mapping in the system which had led to 'NULL' value in the tender ID field in the bid decrypted table, and this issue had been resolved.

  The response was not tenable, since it did not explain how the tender ID field could be populated as 'NULL' in case the process had been carried out through the application front end. The Government also did not furnish the details of the resolution process or patch management in this regard.

- In a total of 77,554 tenders involving 2,45,521 decrypted bids, the time of decryption of bids was recorded as before the time recorded for opening of the bids. The difference between the bid decryption time being earlier than bid opening time ranged from 55 minutes to 2,252 days, which was highly irregular. This broken chronology and logical sequencing of actions in the system indicated the risk of manual intervention at the back end of the system.

- There were 1,89,141 decrypted bids having exactly the same bid decryption start time and end time, which again indicated the risk of manual intervention at the back end of the system.

- There were 342 bids pertaining to 120 tenders in the system, which were recorded as not having been decrypted. Out of these 120 tenders, 48 tenders had either been revoked, retendered or cancelled. However, there was no explanation as to why the bids in the remaining 72 tenders were recorded as not having been decrypted. Out of these bids which were recorded as not decrypted, contracts had been awarded in the case of five bids. This discrepancy indicated the material risk that these bids pertaining to the 72 tenders had been entered into the system through manual intervention at the back end.

  The Department stated (December 2023) that the 'bid decrypted' table was implemented at a later stage and that during initial deployment, the data had been populated from other tables using deployment scripts which had resulted in the above discrepancies.

  The response was not tenable, as these discrepancies had taken place even after the implementation of the 'bid decrypted' table in 2017-18 and details of the deployment scripts previously used were not provided to Audit for verification.

Recommendation

Government may consider to

- Minimise manual interventions at the back end of the system, by adopting formal change management process to implement required functionality for users at the front end of the application;

- Ensure mandatory maintenance of application and DBA logs to record all user actions at the front and back end of the system;

- Adopt standard operating procedures for patch management, version control and documentation of scripts used in the system.

Chapter VII
Award of Contract

Chapter VII

Award of Contract

7.1 Award of Contract

As described earlier in this Report, the processes of technical and financial evaluation of bids and award of contract are being carried out manually, outside the e-Procurement system. This section of the Report describes deficiencies in application controls in the functionality to record the details of award of contract in the system.

After Award of Contract (AOC) through manual process outside the system, details of the same are entered by the TIA into the system, so that EMD may be refunded to the unsuccessful bidders.

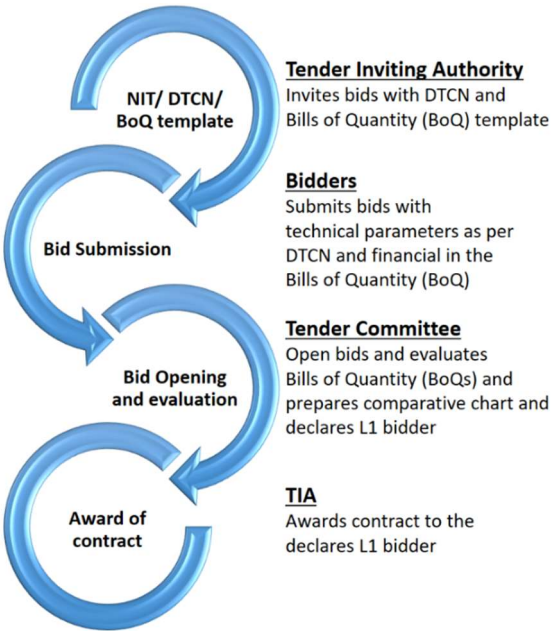
The completion of this workflow is essential for correct update of the status of the tender in the system, and hence for correct generation of the MIS Reports for that purpose.

7.1.1 Awarded value more than quoted amount

Input control

OPWD Code stipulates that the price quoted by the lowest bidder (L1) should be accepted followed by negotiation if required. Therefore, the quoted amount in the Financial Bid *i.e.,* Bill of Quantity (BoQ) should always be equal to or more than the awarded amount.

Figure No. 7: Process flow diagram from invitation of bids to award of contract



Database analysis revealed that out of 66,407 tenders which were awarded with contract, in 6,128 tenders the awarded value was shown more than the value quoted by the bidders. The excess amount awarded in these tenders ranged between ₹10 and ₹1,24,298.50 crore.

As an example, in one work where the work was shown awarded at an abnormal cost of ₹1,24,298.50 crore, there was data entry error. The BoQ amount and actual awarded value as per documents was ₹12.42 lakh only. This had happened due to lack of input validation in the system to compare the AOC value with the bid values.

Further, analysis revealed that in 11 bids of 11 tenders, the amount furnished in the BoQ by the bidder had been recorded as zero, due to deficiency in the input validation controls implemented for the BoQ template used to submit bids. The system generated comparative sheets in these cases and showed that all the bidders were qualified and deemed to be L1.

As a result, the tender evaluation committee had to manually calculate the correct bid amount for each bidder, based on inputs submitted on *per cent* rates from the bidders and create revised comparative sheets to identify the actual L1 bidder. This example demonstrated that the deficiencies in the e-Procurement system related to the technical and financial evaluation and AOC processes had contributed to the continued use of manual evaluation and AOC outside the system for these processes.

Audit test checked 486 tenders for detailed scrutiny and noticed that there were errors/ irregularities in 125 tenders. These included data entry errors in 46 tenders, irregular inclusion of GST amount in AOC value in 30 tenders, and irregular increase of the AOC value due to either increase in BoQ beyond the tender published or increase in bid amount of L1 in 49 tenders. These errors/ irregularities could have been avoided/ minimised if the bid evaluation and AOC processes had been followed within the system with implementation of the application controls required to correctly map the business requirements.

Accepting the observation, the Government stated (December 2023) that all TIAs have been intimated to use the e-Procurement portal cautiously while inviting tenders.

The response was not tenable, as it only indicated that the responsibility for ensuring compliance with executive instructions remained on the individual users instead of shifting to the system through the implementation of the required application controls.

Recommendation

Government should map the full business requirements for bid evaluation and award of contract into the system, through implementation of appropriate application controls to ensure compliance and minimise errors/ irregularities.

Chapter VIII
Timestamp Management and Application Security

Chapter VIII

Timestamp Management and Application Security

8.1 Gap in sequential numbers in database tables

System security

During analysis of database design of e-Procurement system, Audit observed that each table of the database contained a data field named "ID", which is a system generated sequential number[10] to each record in the tables to maintain uniqueness. As it is a system generated sequential number, there should not be any gaps between any two consecutive ID numbers except in the event of deletion of records, sequence failures due to server shutdowns/ restarts or transaction rollbacks.

Audit analysed the sequence of ID columns in ten important tables out of the total 742 tables in the database and found that there were 6.06 lakh records (IDs) missing in these tables. The numbers of missing records from these tables were as follows:

Table No. 10: List showing gaps in IDs in various tables

Sl No	Table description	Last ID in table	Total number of records	Number of times the gaps occurred	Number of missing serial numbers
1	User Master	87,621	87,105	186	516
2	User Certificate Master	1,75,307	1,73,718	805	1,589
3	User Login Logs	44,54,352	44,29,771	21,037	24,581
4	Tender Basic	84,384	79,588	3,287	4,796
5	Tender Master (Work items)	3,96,156	3,81,968	9,954	14,188
6	Bids details	18,24,643	18,22,882	1,508	1,761
7	Bank Transaction Details	6,66,989	6,66,766	70	223
8	History of Bank Transactions	27,01,771	21,91,022	21,238	5,10,749
9	Tender Fee Details	18,43,314	18,24,425	15,298	18,889
10	Decryption of bids	19,95,857	19,67,589	19,056	28,268
	Total	**1,42,30,394**	**1,36,24,834**	**92,439**	**6,05,560**

(Source: extracted from e-Procurement database)

The gaps between the sequential IDs of these ten tables ranged between 1 to 827. Gap of one in sequential ids can be explained due to server shutdowns / restarts; however, larger gaps indicated manual intervention at the back end of the system to delete records. The Department had not conducted a review of such deletion, and identified the root causes for the missing IDs. The existence of these sequential gaps raised doubts on the integrity of the database.

[10] Starting from one and incremented by one *i.e.,* if ID of first record is one, then ID of second record is two and so on.

In reply, Department stated (December 2023) that gaps had occurred during transaction failures in the events of network issues, users cancelling transactions, logical errors *etc.*

The response was not tenable, as the gaps were larger in size than would be expected with transaction failures. Audit examined these larger gaps and found that application logs were also missing for those periods (**details in *Appendix-II***), which indicated the material risk of manual intervention to modify data at the back end of the system.

8.2 Unreliable and incomplete user logs

As per SRS, every user is required to login to the e-Procurement portal using their username, password and Digital Signature for carrying out different activities. Therefore, the activities of users like tender creation, tender publishing, bid creation and submission by bidder, tender opening, and decryption and downloading of bids by department users *etc.,* should have corresponding user log record in the session login table. As both the login and logout time of the user were captured for all the user login session from 01 May 2017, Audit analysed the login records in the user login session tables for the period from May 2017 to March 2022 and observed that the above activities were carried out by the users where the log record about their logins were not available in the user login session table.

The major user actions which did not have associated user logs included the following:

1. Creation of tenders without log
2. Creation of bids without log
3. Submission of bids without log
4. Opening of bids without log
5. Decryption of bids without log
6. Absence of/ incorrect recording of IP addresses of users

These missing logs indicated the material risk of modification/ deletion of records through manual intervention at the back end of the system, and hence raised doubts on the integrity of the database and the procurement process as a whole.

8.3 Use of SHA1 instead of minimum SHA2

System Security

As per 'IT (Intermediary guidelines and digital media ethics code)– Rule 2021, Digital signature End Entity Rules 2015 – Rule 7, SHA2 was prescribed as the hashing algorithm for use in Digital Signature. Further, in view of the detected collisions in SHA1 algorithm, SHA2 should be used in the e-Procurement application.

During scrutiny of the application, Audit noticed that different hashes like password hashes, file name hash, file date hash, document hashes *etc.,* are calculated using SHA1 or MD5 algorithm. Even the digital signature process

in e-Procurement (GePNIC) is still using the SHA1 with RSA instead of SHA2.

Department stated (December 2023) that they are planning to use SHA512 hashing mechanism. The fact remained that there was lack of security in hashes.

8.4 Absence of provision for verification of digital signatures of bidders

System Security

IT Act 2000 Chapter-II Para 3 provides that in case of a person who authenticates an electronic record by affixing digital signature, any person by user of a public key of the person can verify the electronic record. 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.

Audit noticed that in compliance to a query raised (November 2019) by STQC during their audit of the e-Procurement system, it was commented that electronic record can be verified using public key.
However, Audit noticed that NIC had not provided for verification of digital signatures by stakeholders anywhere in the application. Further, Audit observed during testing of e-Procurement system that during uploading of bid documents by the bidders, the system mandated digital signature by bidders. Audit downloaded bid documents submitted against 48 tenders from the e-Procurement system and observed that there was no digital signature affixed on any of the bid documents.

It was explained by NIC that the digital signatures were detached and stored separately in the system and there was no provision for Departmental users to verify these digital signatures of the bidders.

The absence of this provision resulted in non-compliance with the IT Act 2000.

The Department stated (December 2023) that the provision to verify the digital signatures would be implemented in future versions of the system.

8.5 Maintenance of logs

System Security

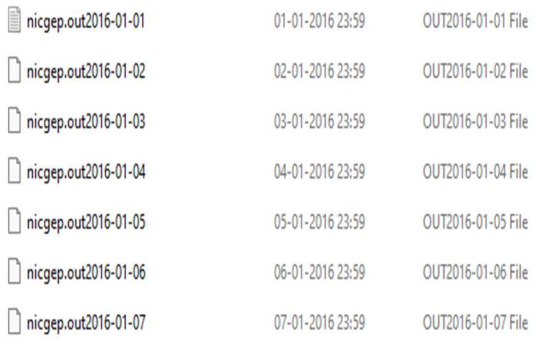
As per System Requirement Specification, a secure central logging server should be deployed for recording all the events in system and access to such central logging server shall be completely restricted for the system administrators. The server was to be synced with the International Time zone server and a log of these time synchronization details was to be maintained in the server. Logs shall be enabled for access methods of the servers (especially for production servers) and audit and log of activities referring to the operating system, access to the

system shall be maintained. Therefore, among other security logs, web logs[11], application logs[12], and DBA logs[13] are important.

Department had furnished two types log data *i.e.,* web log (January 2016 to December 2022) and application log from (Jan 2016 to April 2022). Application logs collected during the whole day were taken to a file named after the same date with prefix 'xxxxx.out'. As an example, the log of 01 January 2016 is collected in the file "xxxxx.out2016-01-01 which is collected normally at the day end at 23.59 hours each day. Similarly, the web logs (apache web logs) collected were stored in log store in a folder named after the server address like 'xxx.xxx.xxx.xxx' which was in a date wise folder and the date wise folders were kept within a month wise folder named with year and month like '201601' for January 2016.

Figure 8: Extracted data from log files furnished by NIC

Application Log storage in file system



Web log storage in log store

Analysis of these logs revealed the following:

8.5.1 Missing logs

Application logging ensures that each application's logging verbosity is set to an appropriate level in order to provide appropriate information when needed for security review. Web logs captures visitors browser agent, date time of access, method, IP address *etc.,* for analysis in case of forensic investigation.

Analysis of web logs revealed that out of 2,556 days period *i.e.,* (from 01 Jan 2016 to 31 Dec 2022), log for 1,087 days were not provided to Audit as follows:

[11] Web logs contain traces regarding the activity of users while accessing the web pages like date and time, IP address, method, name of page (URL endpoint), browser agent, *etc.*

[12] Application logs contain traces of activity of user in the system like IP address, User ID, Module Name executed, timestamp of activity, other details like bid id, tender id *etc.*

[13] DBA logs record details of all back-end activities of the DBA user like modification, deletion, insertion of transaction or master records in the backend or changing the definition of table structures, functions, procedures, other configurations *etc.,* by using SQL statements or scripts.

Table No.11: Table showing Period of missing web logs

From Date	To date	Missing days
10-Nov-2018	16-Jun-2019	219
18-Jun-2019	25-Jun-2019	8
05-Aug-2019	26-Aug-2021	753
27-Mar-2022	10-Jul-2022	106
12-Jul-2022	12-Jul-2022	1
Total Missing days		**1,087**

(Source: Apache Logs provided by NIC)

Similarly, in the application log, it was found that out of 2,311 days period, there were missing logs for 27 days as follows:

Table No.12: Table showing Period of missing application logs

From date	To Date	Missing records
24-Feb-2016	24-Feb-2016	1 day
28-Sep-2016	28-Sep-2016	1 day
29-Jan-2017	29-Jan-2017	1 day
31-May-2017	31-May-2017	1 day
07-Jun-2017	07-Jun-2017	1 day
12-Jun-2017	12-Jun-2017	1 day
16-Jun-2017	16-Jun-2017	1 day
19-Jun-2017	19-Jun-2017	1 day
24-Jun-2017	24-Jun-2017	1 day
27-Jun-2017	27-Jun-2017	1 day
01-Jul-2017	01-Jul-2017	1 day
04-Jul-2017	04-Jul-2017	1 day
09-Jul-2017	09-Jul-2017	1 day
14-Jul-2017	14-Jul-2017	1 day
04-Feb-2018	04-Feb-2018	1 day
23-Apr-2020	24-Apr-2020	2 days
26-Apr-2020	26-Apr-2020	1 day
03-May-2020	03-May-2020	1 day
31-May-2020	31-May-2020	1 day
03-Aug-2020	03-Aug-2020	1 day
02-Mar-2021	02-Mar-2021	1 day
21-Mar-2021	21-Mar-2021	1 day
08-Jun-2021	08-Jun-2021	1 day
05-Sep-2021	07-Sep-2021	3 days
Total		**27 Days**

(Source: e-Procurement database)

This indicates that these logs were deleted. Due to missing logs, the objective to provide appropriate information when needed for security review could not be achieved and reliability of system was compromised.

In reply, Department stated (December 2023) that Apache web logs only contains the URL ends points with the client IP and browser agent. Application logs are critical. Due to technical glitch, few times application logs may not be generated and subsequently by the end of day (EOD) the problems were resolved and logs were generated. However, the fact remained that there are losses of critical logs to both application and web logs. It is pertinent to mention here that further audit process is hindered due to absence of logs as pointed out in ***Appendix-II***.

Further, Department stated (December 2023) that CERT-ln recommendation is 180 days for ICT logs retention period. In addition to that, few times back Odisha e-Procurement was running under the Odisha NIC Data centre. The reply is not acceptable as CERT-In recommended the minimum period 180 days for log retention and the logs generated during the period when application was hosted in Odisha server could have been maintained separately.

8.5.2 Non Maintenance of DBA Logs

As per infrastructure administration policy, all internal servers deployed at National Informatics Centre must be owned by an operational group (e.g. data centre) and/or administrators who shall be responsible for System Administration of these servers. Operational group or administrators should monitor implementation and compliance of policy tailored to their environment. All servers not under the direct ownership of the respective data centre, must be identifiable to a particular group and/or administrator. A secure central logging server should be deployed for recording all the events in system and access to such central logging server shall be completely restricted for the system administrators.

Audit requisitioned (August 2022) the DBA logs to the Department. As the system did not preserve DBA logs, the same could not be provided to Audit for analysis. In the absence of DBA logs, unauthorised access and modification of the data at the back end of the system could not be ruled out.

In reply, Government stated (December 2023) that the server log has been maintained for last 3 years but the transaction log is not maintained beyond a week due to shortage of space.

Recommendation

Government may consider to

- Enquire into the reasons for the gaps in the sequence of IDs in the major tables of the database;
- Implement appropriate application controls to enforce chronological and logical sequencing for user actions in the system;
- Ensure maintenance of web, application and DBA logs for the system.
- Adopt relevant standards specified by Ministry of Electronics and Information Technology, Government of India from time to time.

Chapter IX
Conclusion

Chapter-IX

Conclusion

9.1 Conclusion

The State Government implemented the Government e-Procurement System developed by NIC (GePNIC) in 2008. In the absence of a formal Agreement/ MoU with NIC, there was lack of clarity on the timelines, deliverables, roles and responsibilities and service levels for this IT application. Further, there was no recourse for the State Government when key Modules (Indent Management, Vendor Management, Contract Management) of the application remained unimplemented even after 14 years. Even in the e-Tendering Module, key functionalities such as master data management for contractors, integration with the Works and Accounts Management Information System and Contractor Database Management System had not been implemented. These missing functionalities and the key dependencies had resulted in continued manual processes outside the system for bid evaluation and award of contract, which were the most crucial business processes intended to be covered by the e-Procurement application.

In the e-Tendering Module, the full mapping of business rules into appropriate application controls had not been completed. This had resulted in the absence of enforcement of the minimum period for submission of bids, absence of enforcement of two-cover process based on tender value, absence of functionality in the system to manage privileged bidders. These missing business rules had contributed to instances of incorrect selection of bidders, incorrect computation of tender fees and award of contract at amounts higher than bid amounts during the continued manual processes for bid evaluation and award of contract.

There were deficiencies in the validation controls to verify inputs submitted during the bidder registration process, with discrepancies such as mapping of incorrect/ duplicate Digital Signature Certificates (DSC), Permanent Account Numbers (PAN) and mobile numbers to the registered bidders. There were deficiencies in the processing controls for computation of total tender value based on BoQ entered by TIAs and computation of total bid value based on BoQ entered by bidders. There were also deficiencies in the application controls to prevent the submission of bids after expiry of tender closing time and to enforce chronological and logical sequencing of user actions in the system.

There was a material risk of access to and modification of data, including decrypted bid data, at the back end of the system without maintaining database

Administrator logs to record user actions, which was highly irregular. There were also other significant lapses in system controls for information security, such as gaps in sequential numbers in database tables, unreliable and incomplete user logs, use of hashing algorithms with lower than prescribed strength, absence of provision to verify Digital Signatures and non-maintenance of web and application user logs.

In conclusion, the responsibility of ensuring compliance with executive instructions related to procurement continued to remain on the individual users, instead of shifting and being borne by the e-Procurement system through the implementation of application controls. Hence, the objectives of implementing the e-Procurement system have not yet been fully achieved.

Bhubaneswar
The

(ATUL PRAKASH)
Accountant General (Audit-II), Odisha

Countersigned

New Delhi
The

(K. SANJAY MURTHY)
Comptroller and Auditor General of India

Appendices

Appendix-1

(Refer paragraph 1.6 at page 5)

Sampling Methodology

There were 3,74,823 tenders published since inception of the system upto 31 March 2022 with tender value ₹3,32,021.41 crore (except records for test type of tenders). Out of these published tenders, 1,77,593 tenders with tender value ₹1,74,019.46 crore was published during last five years *i.e.,* between 01 April 2017 to 31 March 2022 by 29 Departments out of 40 departments under Government of Odisha. Audit will verify the sampled tenders published during last five years *i.e.*, from 2017-18 to 2021-22 at field level.

The following risk assessment is considered for selection of sample tenders for physical verification during audit of e-Procurement taken up by field audits.

Stratification

Tenders are stratified on the basis of types of tenders

- Limited Tenders
- Open Tenders/ National competitive bid/ Global Tenders

Parameters for risk assessment:

Parameter-1. Number of Bids Received per tender.

Count of bids received against each tender prepared. The higher number of bids received means lower the risk. The lowest number of bid received for tender was '1' and the highest number of tenders received was '350'. The average number of bid received was 6. Further, the stata for number of bids received with tender count is as follows :

Range of number of Bids	Tender Count
1-5	1,04,515
6-10	27,084
11-20	18,246
21-30	5,568
31-40	2,177
41-50	1,083
51-60	527
61-70	393
71-80	159
81-90	92
91-100	66
101-200	119
201-400	8
Nil bids	17,440

As maximum number of tenders received one to 5 number of bids for tenders, tenders more than 5 bids are not allocated any score and tenders received 5 and less than 5 bids were inverse normalised using the following formula.

$$z_i = 1 - (x_i - min(x))/(max(x) - min(x))$$

Where-

$x_i = number\ of\ bids\ received\ for\ that\ tender$

$\min(x) = minimum\ number\ of\ bids\ received, taken\ as\ 1$

$\max(x) = maximum\ number\ of\ bids\ received, taken\ as\ 5$

Parameter-2. Tenders cancelled/ retendered

The tenders cancelled /retendered is marked as 1 , otherwise 0.

Parameter-3. Last bid being accepted.

If the condition is true the score is 1, otherwise 0.

Parameter-4. Difference of Time remaining (for close of tender) w.r.t. time of submission of accepted bid. If such difference is greater than 24 hours, no risk score was allocated. Where difference is less than 24 hours, the lowest difference allotted more score and the highest difference allotted less score. The normalised formula is

$$z_i = 1 - (\min(1, B - C))$$

Where-

B = Last date of submission of bid

C = Time of submission of bid

and if B-C >1 then minimum 1 is taken, E.g.,

Tender-Id	Last date of submission of bid	Time of submission of bid that was accepted	Difference	Normalised Score
A	B	C	D = Min(1,B-C)	E
T-1	31-01-2022 15:00	31-01-2022 14:45	0.010417	1
T-2	31-03-2022 15:00	30-03-2022 15:00	1	0
T-3	20-01-2022 15:00	20-01-2022 05:00	0.416667	0.589474
T-4	15-02-2022 15:00	11-02-2022 17:00	1	0
T-5	20-02-2022 15:00	18-02-2022 15:00	1	0

Parameter-5. Same set of bidders bidding for similar work types.

Top-5 set of bidders who bid together identified. Tenders having those sets of bidders given risk score 1 and other tenders are allocated 0.

Parameter-6. Tenders having at least one bid submitted from the IP address of department.

If the tender has at least one bid submitted from the same IP as that of department, but the L-1 bid was submitted from a different IP – the score is 0.5, if the bid approved (L-1) has been submitted from the same IP as that of department, the score is 1, otherwise 0.

Parameter-7. Tenders having two or more bids submitted from suspected collusion.

i. Same IP address
ii. Same PAN
iii. Same mobile number
iv. Same GSTN Number

If the condition is true the score is 1, otherwise 0.

Parameter-8. Estimated Financial Value of tender

The tender value range wise tender count is as follows:

Range of tender value	Number of tender
0-5 lakh	43,665
5-25 lakh	78,555
25-50 lakh	22,623
0.5 -1 crore	13,674
1-5 crore	14,534
5-10 crore	2,649
10-50 crore	1,615
50-100 crore	102
100-200 crore	73
200-500 crore	85
500 crore and above	18

Quaratile range and upper and lower limit calculated in excel sheet taking tender value for calculation

1st quartile	3rd quaratile	Inter Quaratile Range (IQR)	Upper Bound	Lower Bound
=QUARTILE (D2:D177594,1)	=QUARTILE (D2:D177594,3)	=Quaratile3-Quaratile1	=Quaratile 3 + 1.5*IQR	=Quaratile1-1.5*IQR
5,00,000	34,86,920	29,86,920	79,67,300	-39,80,380

Hence the upper bound is rounded as 79,67,300 = 80,00,000. As higher value of tender means higher risk, the tenders with tender value more than 80,00,000 allotted score 1 and for tender value less than 80,00,000, the score was calculated using the following formula.

$$z_i = 1 - ((8000000 - x_i)/8000000)$$

Where-

$$x_i = value\ of\ tender$$

Parameter-9. Time allowed for bidding

The difference of time of publishing tender and last date/time of submission of bid is calculated and (inverse) normalised. Bid submission period minimum 10 days with tender value less than Rs. 50 lakh, minimum 15 days with tender value between 50 lakh and 6 crore and minimum 21 days with tender value equal to or more than ₹6 crore is taken for calculation of time allowed for bidding. If such difference is greater than the minimum days specified, no risk score was allocated as per following formula.

$$z_i = (x - xi)/x$$

Where-

$x_i = Difference\ in\ time\ of\ publishing\ of\ tender\ and\ lastdate\ of\ submission\ of\ bid$

$x = minimum\ Time\ permissible\ for\ tender\ where\ x > 0\ and\ x > xi$

and when x>xi then zi= 0

Parameter-10. Time taken from opening of bids to signing of contract

As per OPWD code the time taken from opening of bid to award of contract should not exceed more than 90 days. The difference of date of signing the contract/ 31 March 2022 and date of opening of bids is taken and normalised as follows :

$$z_i = (x_i - min(x))/(max(x) - min(x))$$

Where-

$x_i = days\ Difference\ between\ bid\ opening\ and\ signing\ of\ contract/'31march\ 2022'$

$\min(x) = minimum\ number\ of\ such\ count, taken\ as\ 90\ days$

$\max(x) = maximum\ number\ of\ such\ count, taken\ as\ 180\ days$

All tenders having time gap less than 90 days between opening of bids and award of contract/contract not awarded as of 31 March 2022 was given score 0 and time gap more than 180 days have been allotted score 1.

Parameter-11. *Per cent* difference between L1 and L2.

The difference of price quoted by L-1 and L-2 calculated and *per cent* difference calculated. If such difference is more than 2 *per cent*, no risk score is allocated. If the *per cent* difference less than 2 *per cent* it was normalised as

$$z_i = (2 - x_i)/2$$

Where-

$x_i = Percentage\ difference\ between\ L1\ and\ L2\ bidder$

Parameter-12. Tenders where financial limits specified, have been breached.

As per GFR the tender value below ₹25 lakhs was to be limited tender and ₹25 lakh to ₹200 crore to be open tender and above ₹200 crore to be Global tender. The tenders falling in any of such exception category is allocated risk score 1 and otherwise 0.

Weight Matrix

The following weightage for these parameters for open tender and limited tender is considered for arriving the risk score .

No.	Parameter	Open Tender	Limited Tender
1.	Number of Bids Received per tender	10	0
2.	Number of times a tender has been cancelled earlier and now re-awarded	10	10
3.	Last Bid being accepted	10	10
4.	Difference of Time remaining (for close of tender) w.r.t. time of submission of accepted bid.	10	10
5.	Same set of bidders	10	0
6.	Tenders having IP of department	10	10
7.	Tenders having two or more bids submitted from same IP addresses/ suspected collusion	10	10
8.	Financial Value of bids	5	10
9.	Time allowed for bidding	5	10
10	Time taken in award of Contract	5	10
11	*Per cent* difference between L1 and L2	5	10
12	Exception cases/ breach of financial limits	10	10
	Total	100	100

Population Frame

There were 3,74,823 tenders published since inception of the system upto 31 March 2022 with tender value 3,31,911.77 crore (except records for test type of tenders). Out of these published tenders, 1,77,593 tenders with tender value ₹ 1,74,019.46 crore was published during last five years i.e between 01 April 2017 to 31 March 2022 by 29 Departments out of 40 departments under Government of Odisha.

Sample selection

For the purpose of sample selection, the tenders published during last five years *i.e.,* from 2017-18 to 2021-22 will be considered involving 1,77,593 tenders as sample universe with tender value ₹ 1,74,019.46 crore.

Selection of Departments

Department wise sum of risk scores of 29 Departments were ranged between 13 to 11,78,243. Based on risk scores, the Departments were stratified as high, medium, and low category and 10 departments out of 29 (35 *per cent*) are selected by stratified random sampling as given below:

Sl No	Range of risk parameter	Category of risk	Number of Departments	Number of Departments selected	Percentage of selection	Departments Selected
01	0 to 5,000	Low Risk	14	2	14.29	(i) Odia Language Literature and Culture (ii) FA&RD
02	5001 to 1,00,000	Medium Risk	15	04	26.66	i. Forest and Environment ii. Steel and Mine iii. Industry vi. Home
03	1,00,001 and above	High Risk	04	04	100.00	i. H&UD ii.RD iii. WR iv. Works.

Selection of Tender Inviting Authority

The TIA has been arranged in descending order of total risk score of each selected department. 48 TIAs were selected by stratified random sampling based on population proportionate to size of the selected Departments**.** Where there is population less than one then minimum one TIA has been selected. Where there is less than 5 as population in Department, one stratum is considered for selection of TIA.

Selection of Tenders

10 tenders from each selected TIA will be selected by stratified random sampling based on risk scores after forming 2-3 strata on risk score of tenders.

Appendix – II

(Refer paragraph 8.1 at page 42 and 8.5.1 at page 46)

Statement showing discrepancy or missing logs of various dates in the events of record creation where there were missing sequences (gap) between two consecutive ID numbers of a table

Sl No	Name of the table where there were gaps in sequential ID data	Gap in consecutive ID data		Gaps	Time stamp of IDs		Remarks
		First ID	Consecutive Second ID		First ID	Consecutive second ID	
1	Tender basic master	63258	63289	32	2019-08-27 17:13:00.571	2019-08-27 18:31:35.591	Log not available from 2019-08-27 17:46:31.813
2	Tender basic master	86448	68519	32	2020-05-19 22:57:47.899	2020-05-20 09:39:35.63	Log not available from 2020-05-20 06:32:08.596
3	Tender basic master	72389	72420	32	2020-12-29 15:44.48.788	2020-12-29 15:48:39.384	Log not available from 2020-12-29 13:30:38.236
4	Tender basic master	73375	73406	32	2021-02-03 08:05:58.415	2021-02-03 07:12:49.432	Log not available from 2021-02-03 05:24:14.568
5	Tender basic master	76428	76459	32	2021-06-08 21:12:13.482	2021-06-09 07:59:16.046	Log not available for 2021-06-08
6	Bid master	638084	638115	32	2017-01-29 10:03:54.548	2017-01-29 12:47:04.004	Log not available for 2017-01-29
7	Bid master	1463256	1463287	32	2021-02-03 05:18:38.231	2021-02-03 05:57:01.97	Log not available from 2021-02-03 05:24:14.568
8	Bid master	1562730	1562761	32	2021-06-08 22:16:04.345	2021-06-08 22.30.05.616	Log not available for 2021-06-08
9	Bid decryption	1583676	1583857	182	2021-02-10 19:45:49.01	2021-02-11 10:26:11.983	Tender was revoked after bid decryption deleting records from bid decrypted table
10	Bank transaction history details	526551	527377	827	2018-10-31 17:08:33.951	2018-11-01 07:58:12.936	The transaction details were not available in the log of that day.

Glossary of Abbreviations

Glossary of Abbreviations

AOC	Award of Contract
AOP	Association of Persons
BoQ	Bills of Quantity
CAAT	Computer Assisted Audit Technique
CDAC	Centre for Development of Advanced Computing
CDMS	Contractor Database Management System
CE	Chief Engineer
CPPP	Central Public Procurement Portal
CVC	Central Vigilance Commission
DBA	Database Administrator
DPI & Roads	Design Planning and Investigation and Roads
DSC	Digital Signature Certificate
DTCN	Detailed Tender Call Notice
e-AOC	Electronic Award of Contract
EIC	Engineer-in-Chief
e-LoA	Electronic Letter of Acceptance
EMD	Earnest Money Deposit
EO	Executive Officer
G2B	Government to Business
GCQE	Guidelines for Compliance to Quality requirement of e-Procurement System
GEMS	Government e-Marketplace
GePNIC	Government e-Procurement System developed by National Informatics Centre
GoI	Government of India
GoO	Government of Odisha
GSTN	Goods and Services Tax Network
GTE	General Technical Evaluation
H&UD	Housing and Urban Development
HUF	Hindu undivided family
ID	Identity Number
IDEA	Interactive Data Extraction and Analysis
IP	Internet Protocol
ISL	IDCOL Software Limited
IT	Information Technology
JAR	Java Archive
L1	Lowest one
MCL	Mahanadi Coal Fields Limited
MD5	Message Digest Algorithm 5

MEITY	Ministry of Electronics and Information Technology
MIS	Management Information System
MoU	Memorandum of Understanding
MSE	Micro and Small Enterprises
NaN	Not a Number
NeGP	National e-Governance Plan
NIC	National Informatics Centre
NIT	Notice Inviting Tender
OGFR	Odisha General Financial Rules
OPWD	Odisha Public Works Department
OTP	One Time Password
PAN	Permanent Account Number
PDF	Portable Document Format
PKI	Public Key Infrastructure
R&B	Roads and Building
RFP	Request for proposal
SHA	Simple Hashing Algorithm
SLA	Service Level Agreement
SPC	State Procurement Cell
SQL	Structured Query Language
SRS	System Requirement Specification
STQC	Standardisation Testing and Quality Certification
TIA	Tender Inviting Authority
ULB	Urban Local Body
WAMIS	Work Accounts Management Information System
XLS	Microsoft Excel file extension

https://cag.gov.in/ag2/odisha/en