AUDIT TRAIL FOR
GOVERNMENT E MARKET (GEM) PLACE

Jeevan Tara Building
Ashoka Rd, Janpath, Connaught Place, New Delhi, Delhi 110001

Audit Trails for GeM

Introduction

Government e-Market Place (GeM) is a meeting place of suppliers and purchasers where purchase to pay (P2P) process is electronically supported and a Government department defines sets of rules for procurement process. E-marketplace is a Business to Business relationship model (B2B) wherein multiple buyers can select products and services from pre-sourced catalogues and perform commercial transactions with multiple sellers through a Web platform. The B2B model allowing direct purchases, procurement through bidding and reverse auctioning that helps organizations in saving cost and increasing productivity enormously. So realizing the benefits of Government e-Market Place, several government agencies and suppliers are joining it. But all of them are concerned about the confidentiality and privacy of their sensitive data, suppliers are worried about the confidentiality of their price quotation before bid opening time. Therefore, it is essential to put in place best audit practices to protect the interest of both buyers & suppliers to encourage the competitiveness in the business. Audit trails and controls are kept to combat the threat of data loss, leakage or manipulation.

An audit trail (also called audit log) is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.

Audit objectives

The purpose of keeping audit trail in the system is to allow Auditors to assess and evaluate that approved transparent processes, filters, data, evaluation criteria and confidentiality techniques are used in e-procurement system.

The aim is also to ensure that notifications are given to all the eligible suppliers; and fair practices are adopted in technical and financial evaluation of bids.

System and artifacts audit

Audit is performed on the basis of input/output data, artifacts and risk envisaged based on audit risk model. The audit model envisaged here is a system based audit which can be performed in efficient and expedient manner since relevant and adequate audit proofs and evidences are collected at every stage of an e Procurement transaction. The audit can be performed on the server as system audit combined with evidences to the extent possible. The evidences gathered in the system are bid and financial approval pdf, encryption/decryption keys, files, emails and e Sign put on bid, contractual documents, Consignee’s Receipt & Acceptance Certificate (CRAC).

Table 1: Audit Risk Model

S.No.	Risk	Severity	Actors Impacted
1	Ability to see price quote of suppliers before opening date and time of bid as it is not encrypted and disclose or modify it	High	Suppliers
2	Price quotes are in the same table where bid generated and accessible to DBA	High	Suppliers
3	Weak Authorization security control with no binding as to who created the following: • Order /Bid • Comparison/ Bid Evaluation • Placed Order • Received and Accepted Products • Made Payments	High High High High	Security Agencies and other Agencies
4	No intimation of bids/Reverse Auctions sent to Suppliers/Service Providers when bid/reverse auction initiated	High	Suppliers
5	Suppliers fill up fake turn over figure, experience or undertaking claiming they are OEM/Authorized Suppliers	High	Buyers
6	Sensitive personal information such as Social Security Numbers, Mobile Numbers and turn over are in plain text and visible to every one	High	Both Buyers and Suppliers

Internal Controls of GeM System

Several internal controls in the GeM system are defined to ensure a complete, exact and timely processing of approved transactions, and purpose of these internal controls is to prevent errors from occurring, or indeed ensure that errors are discovered and corrected.

Control 1: User Definition

The principle of segregation of duties is adopted while defining buyers in the system. Four types of users are defined:

Verifying/authenticating officer

Any officer from administration of the organization who is authorized to verify the details of primary user can be the Verifying/authenticating officer. He/She must be at the level of Under Secretary/Equivalent or above.

HoD/Primary User

Role of HoD/Primary User in GeM is to create Secondary users for his organization i.e. Buyer, consignee, DDO/ Paying Authority. He/She can add secondary users after clicking on Manage Users tab after logging in the GeM portal. HoD/Primary User cannot perform Buying functions on the portal.

Secondary Users

- **Buyer and Consignee**
    - Only Buyer and Consignee role can be given to same person.
- **PAO/DDO**
    - PAO/DDO role can be given to a person other than Buyer / Consignee only.

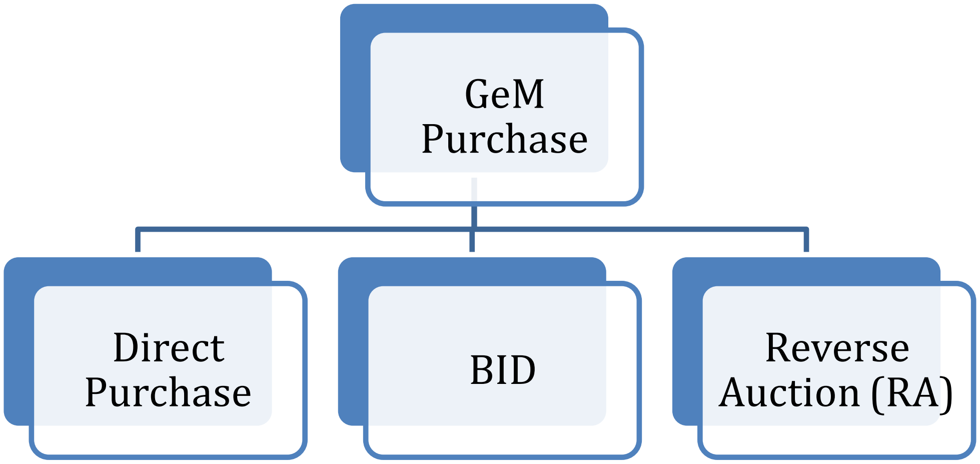
Primary user and Secondary user roles cannot be performed by same officers. Secondary user always needs to be different from Primary user

Control 2: Access Policy

- **User Registration Policy**: Registration of Suppliers and Government buyers is mandatory and it is ensured they are not registered without proper e-verification (e.g. Aadhaar, OTP on Aadhaar linked mobile used) and they cannot register multiple times.
- **System Access**: Access to system is through User accounts and passwords coupled with provisioning of captcha to avoid un authorized users to access system

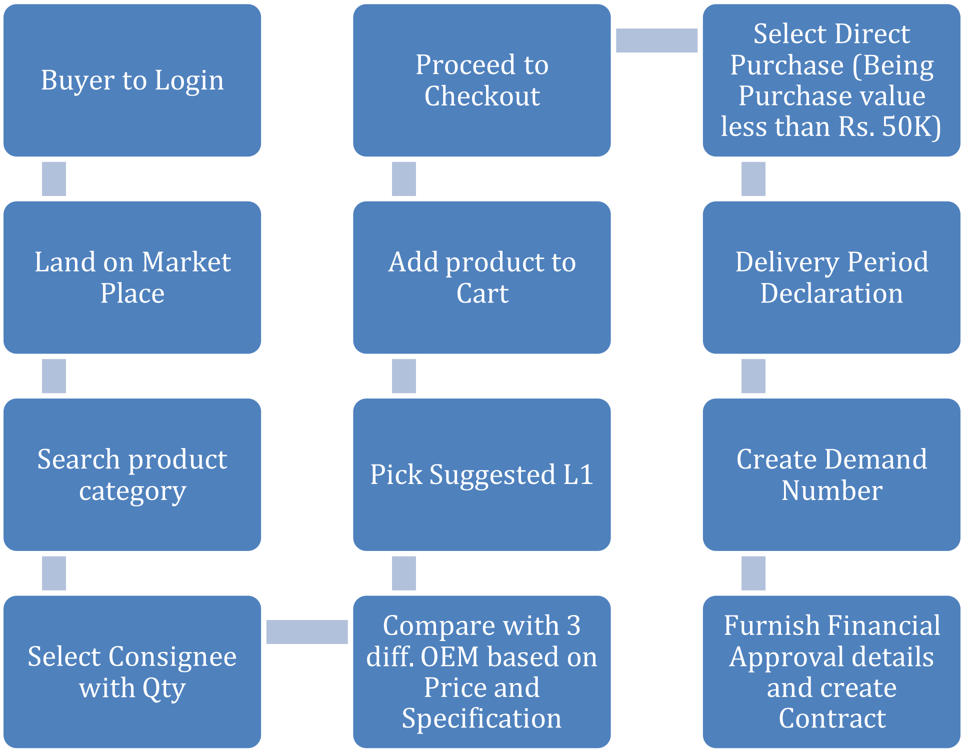
Procurement Methods

As described above based upon the purchase value the method of purchase has been broadly classified as below:



Direct Purchase

As per the rule 149 under GFR a buyer will be allowed to purchase through direct purchase up to Rs.50, 000/- through any of the available suppliers on the GeM.


Buyer to Login
Land on Market Place
Search product category
Select Consignee with Qty
Compare with 3 diff. OEM based on Price and Specification
Pick Suggested L1
Add product to Cart
Proceed to Checkout
Select Direct Purchase (Being Purchase value less than Rs. 50K)
Delivery Period Declaration
Create Demand Number
Furnish Financial Approval details and create Contract

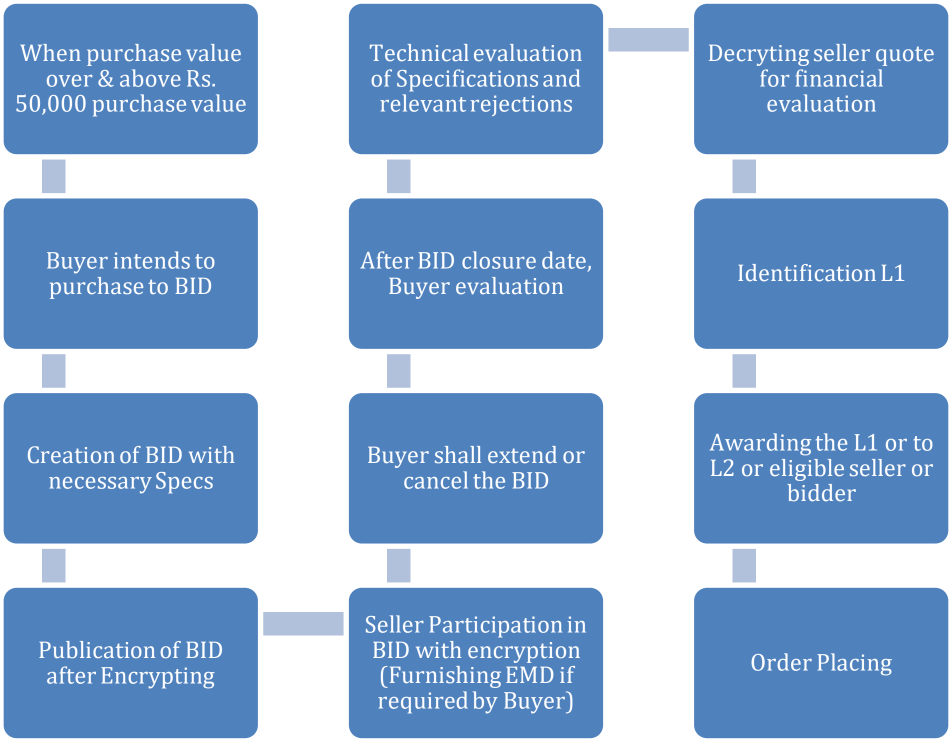
- The registered buyer to GeM portal to login and will be validated against their registered details from database.
- On successful validation, buyer will land on the Market Place page.
- Buyer to search for the relevant product category to purchase.
- Should select and log the consignee details along with the no of quantities required to purchase.
- The buyer have to select in minimum of 3 different OEMs to compare based upon the price and specification and arrive at the L1 product.
- The system will auto populate the L1 price product which is the least quoted price value of the OEMs compared, which will be added to the Cart.
- Product added to Cart will remain in the same price for 5 days to that buyer, though price changes in the market place.
- Buyer has to proceed checking out the product added to cart and select 'Direct Purchase' (when the purchase value is lesser than Rs. 50,000).
- Buyer has to key the delivery tenure within which expected to get it delivered.
- Post that the Demand number will be generated for the purchase of products.
- The buyer has to furnish the necessary scanned financial approval documents (taken in physical) with finance authorizing officer details for further proceedings.
- The other process of consignee exercising his right for inspection and Acceptance/Rejection and generates Consignee Receipt and Acceptance Certificate (CRAC) and other payment mechanisms remain the same through DDO and PAO officers.

Table 2: Direct Purchase Log Information

Field	Value
Order Number	GEMC<Orgname>-<Order No>
User Name	Buyer
Login Time	DD:MM:YY HH:MM:SS
IP of Client Machine	IP Address
Comparison of Product Prices	Products, Prices Comparison Link
Product Name and Date time Stamp(DTS) of Carting	Product Name, Offer Price, Quantity, MRP, Location, Date and time of Carting.
Financial Approval Artifact Link	Link to Financial Approval (PDF)
Order Creation Date/Time	DD:MM:YY HH:MM:SS
Order Details	Link to Order Artifacts (PDF)
Order Status	Order Placed/Dispatch by seller/Accepted by Consignee/ Bill Generate/ Paid

E – Bidding

When purchase value is over and above Rs.50,000/- and up to Rs.30,00,000/- through the GeM Seller having lowest price amongst the available sellers, comparing of at least three different manufacturers, on GeM, meeting the requisite quality, specification and delivery period. The tools for e - bidding or reverse auction (RA) available on GeM can be used by the Buyer.


When purchase value over & above Rs. 50,000 purchase value
Buyer intends to purchase to BID
Creation of BID with necessary Specs
Publication of BID after Encrypting
Seller Participation in BID with encryption (Furnishing EMD if required by Buyer)
Buyer shall extend or cancel the BID
After BID closure date, Buyer evaluation
Technical evaluation of Specifications and relevant rejections
Decrypting seller quote for financial evaluation
Identification L1
Awarding the L1 or to L2 or eligible seller or bidder
Order Placing

- Whenever the purchase value buyer product is over and above Rs. 50,000, buyer has to go through the e Bidding or Reverse Auction process to award the order.
- Buyer shall proceed towards creating BID based on the specs available for the product by default, or shall even quote additional specs.
- Also buyer has option to add EMD asking from seller, for the participation of this BID.
- To proceed creating the bid through encryption of the same with the key pairs.
- If the buyer doesn’t have key pairs to encrypt, should first generate the key pairs which a copy will be sent via email to his/her registered email id. The generated key pairs will be used to encrypt the BID while creation.
- Sellers in relevance to the product category, to which BID is created for, will be notified through email asking for their participation on the BID.
- When a buyer has raised BID along with the requisite of furnishing EMD, seller has to download the EMD BG form and furnish the necessary details at the bank. The seller BG will be authenticated electronically with the bank for the effectiveness of the seller to participate on the BID.
- Seller quotes the BID price and encrypt with the buyer’s public key.
- At the discretion of the buyer, the closure date of the BID may be extended or even cancel the BID.
- Post the BID participation closure date, technical evaluation of the BID will be processed by the buyer to identify the products matching the technical requirement of the BID and shall reject those seller for not matching the technical specs.

- Post the technical evaluation, buyer will decrypt seller's quote for financial evaluation and identify the L1 seller quoted least price.
- Still the option of ordering the goods lies with the buyer, to offer the deal to L1 or L2 based on the evaluation. Relevant reason for non offering of the order to L1 has to be captured for future audit purpose.
- The other process of consignee exercising his right for inspection and Acceptance/Rejection and generates Consignee Receipt and Acceptance Certificate (CRAC) and other payment mechanisms remain the same through DDO and PAO officers.

Table 3: Log Information of Bid

Field	Value
Bid No	GEM/B/<BID No>
User Name	Logged in user
Login Time	DD:MM:YY HH:MM:SS
Bid Creation date	Date and time of bid creation
Product Comparison Sheet	Link to compare sheet
BID reference price	Amount
Bid Details	Link to bid document
Bid Publication Date • Buyer Name • User Id • User IP	Date and time of BID Published
No. of times bid extended	Count & Date and time
Bid Status	Open/Close/Cancel/Order Placed
Bid Opening Date • Buyer Name • User Id • User IP	Date and time of BID opened
Bid Cancellation Date • Buyer Name • User Id • User IP	Date and time of BID cancelled and reason
Bid Technical Evaluation Date • Buyer Name • User Id • User IP • Status (Rejected/Qualified)	Date and time of BID evaluated, specification sheet of product offered by sellers
Bid Financial Evaluation opening Date • Buyer Name • User Id • User IP	Date and time of BID evaluation opened, L1….Ln Selected Seller, Price.
Final order Awarded to Seller	Link of order file

Control 3: Maintaining Confidentiality of Price Quote

The Price Quotations received from bidders are invited in encrypted format using Public Key Infrastructure. Supplier encrypts the price quotation using Buyers' Public Key and two employees of Buyer Department decrypt it using their Private Key stored on either dongle or High Security Module (HSM) by giving One Time Password which they receive on their registered mobile number in the presence of Suppliers.

Process for Bid Encryption/Decryption without Dongle

Class 3 certificate is required for encryption/ decryption of Bids. The requirement for obtaining class 3 ceritificate is as under:

- An Electronic Application Form (e-form) decided by the Certifying Authority (CA) has to be filled online. Verification of the credentials will be as per Identity Verification Guidelines.

- For verification of the credentials, currently physical presence is required for obtaining class 3 certificate. In place of this, Unique Digital Identity assigned to buyer with biometric verification can serve the purpose after dynamic authentication with OTP.

Key generation:
A key pair needs to be generated on a High Security Module (HSM) applying Asymmetric algorithm based on one of the cryptography algorithms as notified under the Rules and Regulations of the IT Act.

Key Storage:
The public-private key pair will be generated applying PKI standards, i.e. using one of the cryptography algorithms RSA, Diffie-Hellman or Elliptic Curve Discrete Logarithm as notified under the Rules and Regulations of the IT Act. The bidder will use public key of the buyer to encrypt the bid.

- The buyer will use his/her Private Key to decrypt the bid.
- The private key of the bid owner (buyer) will be stored on an HSM complying FIPS 140-2 Level 2. HSM is temper proof storage device that keeps the keys in scrambled form and does not allow making copies. Key can also be generated and stored on key owner's mobile, provided the mobile complies to FIPS 140-2 Level 2 standard.
- The public key with the key owner's attributes such as name, organisation, key identifier, and validity period etc. would be made available through the Buyer's Class 3 Encryption Certificate.
- Valid Public Key needs to be embedded into e-Procurement System Bid submission form, allowing Bidders (Suppliers/Service Providers) to encrypt their bids for submission.
- The buyers (Bid Owners) will open the bid at designated time by giving their PIN after being dynamically authenticated through OTP.
- Current practice as per guidelines for compliance to Quality Requirement of e-Procurement Systems is that Private Key used for decryption remains available with the buyer (i.e. officer of buying department)

- The provision of storing private key on HSM and PIN before applying Private Key by buyer(s) to open Financial Bid in GeM has been used to build security control of the same strength as that of dongle.

Control 4: Logs

The details of each event, its time of occurrence and executor would all be recorded on HSM, so that these logs cannot be truncated, modified, deleted or added. Buyer held Dongle ensures that authentication is handled locally, whereas in the proposed process, the authentication is carried out remotely since keys will be stored on HSM in compliance to FIPS 140-2 level 2 standard.

Control 5: Separate Server for Key Generation and storing bids

The key pair is generated for each Buyer. A separate server is used to generate and store key pair other than the Database server where encrypted financial quotations are kept for increasing security and confidentiality of bids.

Control 6: Reverse Auction (RA)

Any Vendor, who has registered his product in that particular category of product and services, can participate in Reverse Auction and E bid so long he has registered his product 48 hours prior to closing of RA / E Bid**.** EMD is now being made compulsory so that if vendor withdraws after making a bid proposal, it can be forfeited. Right now option to Withdraw offer is not available, if any vendor does not supply products, he can be put in watch list or black list.

Sellers

The "Seller(s)" on GeM will be the OEMs (Original Equipment Manufacturers) and/or their authorized channel partner(s)/ resellers (having any general authorization / dealership of the OEM to sell their product in open market) and e- Marketplaces.

Control 7: Personal information hiding

Personal information Identifier (ID): Attributes that can directly and uniquely identify an individual, such as name, ID number and mobile number are planned to be hidden, Aadhaar is already encrypted, it cannot be seen by anyone. The other attributes will be shortly masked.

GeM Audit System

GeM team is working to extract logged in information generated during different stages of procurement transactions from various tables. Based on Contract Number/ Bid Number or organization name, bid summary sheet along with different artifacts, input/output data and events would be shown to the Auditing Team. It would be an automated process different from traditional audit system**.**