

Vigilance Awareness Week - 2014

27.10.2014 to 01.11.2014

VIG-KIRAN Ver.4

Theme : Combating Corruption - Technology as an Enabler



beml

NEW FRONTIERS. NEW DREAMS

Vigilance Department

Includes a CD containing compendium of
National and International ICT and
e-governance
+
Live recording of
One day workshop on
e-Procurement

PLEDGE



WE, THE PUBLIC SERVANTS OF INDIA, DO HEREBY SOLEMNLY PLEDGE THAT WE SHALL CONTINUOUSLY STRIVE TO BRING ABOUT INTEGRITY AND TRANSPARENCY IN ALL SPHERES OF OUR ACTIVITIES. WE ALSO PLEDGE THAT WE SHALL WORK UNSTINTINGLY FOR ERADICATION OF CORRUPTION IN ALL SPHERES OF LIFE. WE SHALL REMAIN VIGILANT AND WORK TOWARDS THE GROWTH AND REPUTATION OF OUR ORGANIZATION. THROUGH OUR COLLECTIVE EFFORTS, WE SHALL BRING PRIDE TO OUR ORGANIZATIONS AND PROVIDE VALUE BASED SERVICE TO OUR COUNTRYMEN. WE SHALL DO OUR DUTY CONSCIENTIOUSLY AND ACT WITHOUT FEAR OF FAVOUR.



RAJIV



केन्द्रीय सतर्कता आयुक्त
केन्द्रीय सतर्कता आयोग

**CENTRAL VIGILANCE COMMISSIONER
CENTRAL VIGILANCE COMMISSION**

MESSAGE

I am happy to know that BEML is releasing the special journal "VIG-KIRAN Ver.4" with focus on the theme "Combating Corruption - Technology as an enabler" commemorating the observance of Vigilance Awareness Week-2014.

Corruption is one of the major impediments to progress and technology plays an important role in weeding out this evil from the system. Adoption of various e-initiatives can ensure transparency and efficiency along with productivity and profitability in an organisation. Vigilance Division has an important role in bringing to the notice of all employees & stakeholders of the organization the various initiatives undertaken. Journals such as "VIG-KIRAN" are one of such sources.

I convey my best wishes to BEML for publishing the "VIG-KIRAN" series.

Rajiv
3.11.14

(Rajiv)



सचिव (रक्षा उत्पादन)

SECRETARY (DEFENCE PRODUCTION)

G. MOHAN KUMAR

MESSAGE

ICTs (Information & Communication Technologies) offer powerful tools that if well managed, will help to achieve a more open, transparent and accountable organisation and therefore possess the ability to contribute effectively towards any anti-corruption efforts.

I am happy to note that the "Vigilance Department of BEML Limited is publishing a special journal "VIG-KIRAN Ver.4" focussing on the theme "Combating Corruption - Technology as an enabler" to commemorate the Vigilance Awareness Week-2014.

My best wishes to BEML for publishing the "VIG-KIRAN" series.

(G. Mohan Kumar)



स्पेशल सचिव (डीपी) & सीवीओ
SPECIAL SECRETARY (DP) & CVO

ASHOK KUMAR GUPTA

MESSAGE

It is well known to all of us that there are multiple ways in which Technology can contribute in identifying and reducing corruption and bribery. The theme of this year's Vigilance Awareness Week-2014 is "Combating Corruption - Technology as an enabler" is very apt and I am happy to note that the Vigilance Department of BEML Limited is releasing the special journal "VIG-KIRAN Ver.4, highlighting the use of technology in fighting corruption.

My best wishes to BEML for publishing the "VIG-KIRAN" series.

(Ashok Kumar Gupta)



ALOK KUMAR



सचिव

केन्द्रीय सतर्कता आयोग
SECRETARY
CENTRAL VIGILANCE COMMISSION

MESSAGE

I am glad to know that BEML is releasing the special journal "VIG-KIRAN Ver.4 with focus on the theme "Combating Corruption - Technology as an enabler" commemorating the observance of Vigilance Awareness Week-2014.

Corruption is a major obstacle to economic development and leveraging of technology can address the challenges of corruption to a large extent. The adoption of technology initiatives can mitigate various factors leading to corruption. Vigilance plays a critical role in induction and adoption of best practices as well as creating awareness among employees & stakeholders of the organization of the various initiatives undertaken. Publications such as :VIG-KIRAN" are a step in this direction.

(Alok Kumar)



P. DWARAKANATH



MESSAGE

I am happy vigilance awareness week 2014 is being observed throughout the Organisation and on this important occasion our vigilance department is bringing out this special journal “VIG-KIRAN Ver.4” on the theme, “Combating corruption - Technology as an enabler”.

Corruption is a complex problem and require multi-faceted action and use of modern technology can play an important role in eliminating human interface and promotes transparency and accountability to identify and reduce corruption.

I hope that this issue achieve its objective of generating greater awareness amongst all of us about the ill-effects of corruption and the need to combat corruption.

(P. Dwarakanath)

**Chairman & Managing Director
BEML LIMITED**

From CVO's Desk



Corruption has been defined as ‘the misuse of public office for private gain’ and is said to be a function of both the opportunity to request/receive bribes and the risk of detection. It follows from this that monopolies and discretion are corruption facilitators, while accountability and morality are inhibiting factors, best expressed in the formula $Corruption = Monopoly + Discretion - Accountability - Morality$. A key tool in the fight against corruption, therefore, is access to information and transparency.

Ver.4 of VIG-KIRAN, on the theme ‘Combating Corruption –Technology as an enabler’, raises a salute to Technologies in general and Information and Communication Technology (ICT) in particular, as a viable tool for diminishing corruption by enhancing transparency and accountability of public administration. The use of ICT in e-government is a major focus. E-government, short for electronic government, refers to leveraging ICT to enhance service delivery in the public sector, allow greater public access to information, and make government more accountable to citizens. It includes digital interactions between a government and citizens, government and business, government and employees, and government and governments.

Several of India's e-Government initiatives, digitisation of land records, online property tax portals, online tax payment, e-procurement, are all taking away much of the power that individuals have to indulge in corruption. In fact, 'Technology' is today viewed as 'India's quiet anti-corruption crusader'. A combination of strategies, involving use of the tools of ICT and e-Governance is said to significantly aid the fight against corruption at the Transactional level, Administrative level and Policy level. The illustrative corruption prone areas at the three levels and the Centre, State, Integrated e-Government initiatives have been presented graphically on the back cover of VIG-KIRAN Ver.4.

According to UNDP the potential of e-government applications to fight corruption lies in their integration with the following four key anti-corruption strategies, namely prevention, enforcement, access to information and empowerment and capacity building.

Prevention:

Introducing e-government applications provide an opportunity to simplify rules and procedures, and re-engineer processes and system and make them less corruption prone.

The use of computers and online transactions eliminate gate keepers, depersonalize and standardize the delivery of services and thus, reduce abuse of discretion and other opportunities for corruption.

Enforcement:

Computerized procedures make it possible to track decisions and actions and thus, serve as an additional deterrent to corruption.

Where data are centralized, unbiased sampling procedures can be applied for audit purposes.

Access to Information and Empowerment:

Publishing of government information online builds accountability by providing documentation to citizens to substantiate their complaints against corrupt practices.

Capacity Building:

Introducing e-government applications requires that telecommunication infrastructure is strengthened, human resources are developed in ICT literacy, and the culture of good governance promoted.

In short, by reducing asymmetries of information between public officials and citizens, automatizing processes, cutting out intermediaries, limiting the discretion of public officials, reducing red tape and bureaucracy ICTS can promote transparency, accountability and civic participation enabling good governance or what is termed as 'SMART government' meaning, Simple, Moral, Accountable, Responsive and Transparent government.

It must, however, be pointed out that ICTs do not – and cannot – manage themselves. In fact, experience has shown they require aggressive and regular oversight. It must be remembered that ICTs are only a means not an end in themselves, what they do offer are powerful tools that if well managed will help to achieve a more open, transparent, accountable organisation.

The Central Vigilance Commission of India is the leading protagonist advocating leveraging of technology particularly web based technology in the fight against corruption. The CVC has adopted the strategy of “Leveraging Technology to prevent Corruption” since 2004 wherein organisations under its jurisdictions are persuaded to adopt e-governance measures and computerise on priority all those activities which are vulnerable to corruption. Public

Procurement being an activity most vulnerable to corruption it has been a priority concern of CVC, and it has been actively promoting the adoption of e-Procurement as an effective means of not only ensuring efficiency in public procurement but also enhancing competitiveness, transparency, objectivity and integrity.

e-Tendering, e-Procurement, Reverse Auction, e-Payment, are some of the powerful and effective ICT tools that can help combat corruption in public procurement and in this context as a highlight of Vigilance Awareness Week 2014 on the theme 'Combating Corruption-Technology as an enabler' a one day workshop on 'e-Procurement' for BEML Senior Executives, Division Heads, Procurement Managers, CIO Team, Vigilance Officers, numbering 150 in all, was organised on 27th October 2014 at Bengaluru. Shri. Jitendra Kohli a global expert in the field of e-Procurement, and Shri. Joydeep Sinha, GM (IT Consulting), TCIL, were invited as Speakers for the day long workshop. A live recording of the workshop has been included in the CD appended to VIG-KIRAN Ver.4, besides featuring some moments of the workshop and Vigilance Awareness Week 2014 captured in print.

Shri. Jitendra Kohli's article demystifying some of the myths surrounding e-Procurement/e-Tendering and providing solutions titled 'Red Flags in Public e-Procurement/e-Tendering & Some Remedial Measures' has been featured in VIG-KIRAN Ver.4

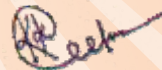
BEML Limited as a leading multi-technology and multi-location, 'Miniratna Category-1' company under the Ministry of Defence, has undertaken major initiatives in ICT. One such is the companywide ERP (Enterprise Resource Planning) System, which is a business process with inbuilt capability for corruption risk management. To address the challenge of vigilance being treated as a standalone activity and not as part of the overall risk management strategy wherein

it becomes an integral part of the duties of every executive to prevent leakages which adversely affect productivity and profitability, an article 'ERP-A Corruption Risk Management Tool' has been featured in VIG-KIRAN Ver.4. It is hoped this will serve the purpose of sensitizing the Executives.

As an innovation in Ver.4 of VIG-KIRAN, the Directors on the Board of BEML were requested to contribute a feature for publication which would contain their assessment of the corruption risks in their functional area of work and how technology would enable them to mitigate those risks. VIG-KIRAN Ver.4 features their contribution in the area of Defence, Rail and Metro, Finance and Human Resource.

The Chief Information Officer (CIO) is the mainstay of an e-Platform workspace and the way forward in the use of ICT to combat corruption penned by the CIO, BEML Limited, has been featured in VIG-KIRAN Ver.4

The CD also contains a compendium of National and International use of ICT and e-Government initiatives to fight corruption. A detailed User Guide to the CD attached is provided.



(Kavitha Kestur)
Chief Vigilance Officer

ERP - A Corruption Risk Management Tool

Risk Management involves the identification, prioritisation, treatment and monitoring of risks that threaten an organisation's ability to provide value to its stakeholders, like increasing profitability and shareholder value. More specifically, risk management balances risk appetite-how much risk management is willing to accept- with the ability to meet organisation's strategic, operational, reporting and compliance objectives. The risk of fraud is one among many risks that an organisation faces and should be considered within the full spectrum of risks. A typical organisation is said to lose an estimated 5 percent of its annual revenues to fraud. It, therefore, makes sense to integrate the fraud detection objectives into risk management. Techniques to help detect fraud within manufacturing organizations encompass a variety of manual and automated solutions, which are dependent upon technology systems, as well as the availability of accurate data. More manufacturing organizations have found it is necessary to employ checks and controls to analyze large amounts of data effectively and efficiently in order to eliminate the “human error” associated with manual controls. Data analysis in the form of continuous monitoring of transactions and controls is a key component of risk management.

Enterprise Resource Planning (ERP) applications, such as SAP and Oracle, widely used by manufacturing companies, constitute the first line of defence. in helping to monitor for fraud risk. ERP is a helpful preventative measure for reducing the chances of fraud and other irregularities. ERP can assist companies in ensuring compliance with legal requirements, accounting rules, strict authorization, segregation of duties and approval mechanisms, and prohibiting fraudsters from performing functions they are not authorized to do. With an ERP system in place, companies get tighter control of processes, alerts on certain fields and the

benefit of comprehensive audit tracking.

In an ERP System, Configurable Controls are the user-defined settings that determine tolerance limits and ranges, data integrity checks, data field requirements and workflow approvals, among other areas. Through a detailed review of configurable controls, companies can take full advantage of the controls built into the software and strengthen the checks and balances that will help prevent fraud. The tighter the fraud prevention controls and procedures, the harder it is for unscrupulous employees to take advantage.

BEML's Journey with ERP:

BEML started its ERP journey in October 2007 with the implementation of SAP ECC (Enterprise Central Component). Subsequently in October 2008 SAP SRM (Supplier Relationship Management) and ICH (Integrated Collaboration Hubs) were implemented. With these business suites from SAP all major activities of BEML business like procurement, inventory management, production planning, sales & distribution, finance & controls and quality management are done in e-mode.

SAP ERP systems – Business Suite / R/3 and Supplier Relationship Management – are fully integrated business real-time systems. They enable transactions to be processed end-to-end and eliminate data inconsistencies between sub-systems. Many companies have replaced their old business systems with the best-of-breed ERP package developed by SAP.

SAP Enterprise Central Component for manufacturing in BEML has the following modules:

MM or Materials Management

PP or Production and Planning

SD or Sales and Distribution
CS or Customer Support
FICO or Finance and Controls
QM or Quality Management

Module wise strategies for risk management are as follows:

❖ MM or Materials Management:

PR mandatory for PO: Purchase request (PR) is mandatory for creation of Purchase order (PO). In simple terms, purchase orders are driven by demand created in the system in terms of purchase requisitions restricting Purchase Order (PO) quantity to the demand thereby preventing stock accumulation and attendant risks.

Inbound compulsory for GR: For any Goods Receipt (GR) with reference to Purchase Order (PO) Inbound delivery is mandatory. Incoming consignments are validated with reference to vendor and purchase order combination hence unauthorised supplies and payment there off cannot be made.

Quality check before posting the GR: Usage Decision from Quality is mandatory for GR (Goods receipt) Posting. Quality check is material master driven and one time settings. This validates conformity to quality parameters defined in the system. Thereby preventing receipt and stock accounting of inferior quality supplies from valid and authorised vendors.

GR based invoice processing: GR (Goods Receipt) based Invoice processing control is configured in the system. User can post the invoice verification Movement in Receipt out (MIRO) transaction by adopting the delivery document or PO with reference to

GR posted Movement in Goods out (MIGO) and quality cleared. System posts the accounting entry and validates with reference to PO conditions.

Cross plant authorisation controls: User Level control authorization is configured in the system. Users are allowed to do the transaction related to their plant only.

Validation for PO quantity for making GRs: With this control in the system GR quantity cannot exceed the PO quantity thereby controls the inventory accumulation.

Auto posting of stock accounting: Financial entries related to all material transactions are posted automatically to the respective General Ledger (GL) A/cs. The GL A/cs is triggered based on the valuation class maintained in the material Master.

Shelf life monitoring and control: The materials which are batch activated monitor and control the shelf life of material while doing the transactions. User cannot issue or receive any expired material.

Information management:

o Procurement Information:

- ME5A - Purchase requisition status (division wise)
- ME2L – Purchase order list by Vendor (across division)
- ME2M – Purchase order list by Material (across division)
- ME2N - Purchase orders list PO Number (division wise)
- ME2W – Purchase orders by Supplying Plant (division wise)
- ME2C – Purchase Orders by Material Group (division wise)
- ME81N - Analysis of Order Values

o **Inventory Information:**

- MB51 - Material Document List (division wise)
- MB5B- Stock on Given Date (division wise)
- MBLB- Material Stock at Sub Contractor (across division)
- MB52- Ware house Stock
- MMBE- Stock Overview at Company Level (across division/region)
- MB5T- Stock in Transit
- MB5M- Shelf life Expiration List
- BMBC- Batch information Cock pit(Shelf Life Monitoring Tool)

❖ **PP or Production and Planning:**

Engineering Change Notification: System will not allow to update material master with Revision level without ECN (Engineering change notice) number for any design changes. Latest revision number for materials can be viewed using report (T.Code - ZC91).

PI Plan: Production plan for equipment and aggregates is fed in demand management in SAP and MRP (Material Requisition Plan) is run to meet the requirements. The results of MRP run can be viewed using T.Code MD04 & Demand /requirements can be viewed using T.Code - MD63.

MRP run: Material Requisition Plan (MRP) is the planning tool in SAP which takes into account all aspects of a material management. MRP looks at current inventory, current requirements, open purchase requests/orders and so on. So if a material is required to satisfy a sales order and there is no inventory, MRP will create a planned

order if the item is to be produced in house. This planned order can then be converted to a production order by the master scheduler. If the item is to be procured, then MRP will create a purchase request which the purchaser will convert to a purchase order. Hence system will balance all requirements with receipts like PRs and Planned orders etc. (T. Code - MDBT,MD02,MD03).

Production Order Control: Production order for all project items cannot be created without standard cost in material master. i.e. all materials should have standard cost /planned price in material master in accounting views.

90% check for material draws: System will not allow to post goods receipt/delivery unless 90% materials are drawn in production orders (T.Code – CO03, ZC122,MB51).

Consumption based planning: Consumption-based planning (CBP) is based on past consumption values and uses the forecast or other statistical procedures to determine future requirements. The procedures in consumption-based planning do not refer to the master production schedule. That is, the net requirements calculation is not triggered either by planned independent requirements or dependent requirement. Instead, it is triggered when stock levels fall below a predefined reorder point calculated using past consumption values. In BEML CBP is introduced for medical items, canteen items and also for some non-project items like consumables which generate PRs, based on stock level falls below re-order point.

Controls for Job Card Booking: Job card booking for employee will not happen unless job card is printed and production order is confirmed. Each control number in job card can be booked and printed only once. Also job card booking for employees can happen only if employee number is maintained in ZEMP T.Code with respect to work centre. Also job card booking for employees can happen only for + /- 25% of standard

man hours as per company standard norms (T.Code- ZC40N,ZJCREPORT, ZJCSMH,ZC40DIS).

Control keys exist in production order/operationmaster:

- o Separate Control key in production order is introduced as given below
 - For Operation processed with subcontractors (PP02)
 - In-house manufacturing(PP01)
 - Quality check (PPQM)
 - Operation in-house without Job card (PP07)
 - Operation in-house without Job card without confirmation (PP17)
 - T.Codes CO03,CA03 can be used to display production orders/ operation master

Information Management:

- o COOIS – Production order information system
- o MD04 – Stock/requirement list
- o ME5A- Purchase requisition list
- o MB51- Material document list
- o MB52- Ware house stock for materials
- o ZJCREPORT-Report for job card
- o ZJCSMH –Report for incentive booking.
- o ZC122 –Excess shortage drawl report.
- o ZCMD04 – MRP Report
- o ZC74 –Shortage list

❖ SD or Sales and Distribution:

Controls for sale order creation: Sale order cannot be created without the following details:

- o Customer details from customer master
- o Customer Purchase order number and date
- o Material details from material master
- o Price from pricing master
- o Taxes will flow from tax master

Controls for delivery:

- o Delivery can be created only if there is a sale order.
- o Quantity to be delivered cannot exceed sale order quantity

Controls for invoice: Invoice can be created against delivery/sale order only.

Document flow: Document flow is a feature in SAP which shows the flow from enquiry to invoice, namely, enquiry->quotation->sale order->delivery->invoice and vice versa.

Information management:

- o List of invoices: ZV0120
- o List of sale orders: ZV0191
- o List of deliveries: ZV0183

❖ CS or Customer Support:

Controls for creation of service order: Equipment master is mandatory for creating service order which prevents fake/ dummy service order creation.

Information Management:

- o List of equipments: IH08
- o List of service orders: IW59

❖ FICO or Finance and Controls:

Invoice Verification: In FI (Finance) module systems posts vendor/customer liability transactions as per terms of Purchase order/sale order, accounting entries are predefined in implementation.

Payments to vendors are linked to Vendor Movement in Receipt out (MIRO) document posted in FI module, hence, prevents any excess payment/duplicate payment.

Advance Payments to vendors are made only against Released Purchase orders with advance terms of payment.

Debit Balance: System suggests adjusting advance against vendor invoice posted.

The concept of Business Area/Profit Center enables respective divisions to take schedule of vendor/customer ledger and Recon-account wise schedules forming part of Finance Statement – Balance Sheet.

Inventory Accounting and Asset Accounting are integrated with Material Master –Accounts view and Asset master –Asset Class for selection of GL accounts for schedule 108 and 105.

Accounting Entries: are posted in FICO module from modules like MM, SD, PP, PM, Quality, Payroll, Asset Module, as per the predefined system settings with reference to which Masters are created in respective modules and validation procedures are

established accordingly, user access is restrained.

Material Drawal Accounting: Consumption entries are posted primarily to Inventory schedule and consumption/expenditure GLs. Consumption is further analysed with reference to cost objects like Production orders, sales orders, maintenance orders etc or to cost centres (in ERP it is called as cost objects), Schedule 219.

Cost of In-house Manufactured goods: This is done with reference to Bill of Material and Routing defined in Production planning module and over heads like Material over head, Tooling cost, Labour Hour Rate defined in costing module (FICO). This rate is called Standard cost used for the purpose of valuing store credit from production orders, and other transactions like drawal against sale order, stock transport order, production order etc.

Expenditure Management: Developed mail alerts to selected Expenses GLs as proposed by management to give alert to profit centre owners, to review the expenses and take corrective action if any (schedule 221).

Variance Analysis: System proposed corrective entry called variance accounting, to withdraw the effect of cost of Actual booking to production order –like materials, labour hours etc. and standard costing – This give costing department to analyse and take corrective action for future orders, for this purpose we have introduced 90% check which will be increased to 95% check with management approval for all PLANTS (Production divisions - Schedule 219, Schedule 218).

Depreciation Schedule 205: Depreciation accounting is being developed to fall in line with Companies Act 2013, waiting for management approval.

Establishment Cost: Schedule 220 consisting payroll run data, travel etc., are validated with reference to employee master data maintained in HR Module,

accounting entries are pre-defined in the course of implementation.

Information Management: T.Codes for certain reports are:

- o GL Balances Report: S_PLO_86000030.
- o Financial Statement: S_PLO_86000028.
- o Periodical values of GLs Per Fiscal Year /Profit Centre: FAGLB03.
- o GL Transaction listing: FAGLL03.
- o Vendor Transaction list: FBL1N.
- o Customer Transaction List: FBL5N.
- o Asset Details Asset wise: AS03.
- o Vendor /Customer Balances forming part of schedule to accounts: FG13.
- o Bank Reconciliation: ZF032.
- o Cost Centre wise report: this is used for computing labour hour Rate.

❖ **QM or Quality Management:**

Usage decision is mandatory for all Goods Receipt and Goods Issues in the system. SAP does not allow the user to post Good Receipt (GR) without quality check system.

Quality Notification is Mandatory for making Vendor Recoveries/Returns. Whenever the purchaser wants to send the rejected material based on Quality Notification to vendor, system checks for the vendor recovery document.

Information Management:

- o QA03 - Display Quality Lot
- o QM03 - Display Quality Notification
- o QA13 - Display Usage Decision
- o QM11 - List of Notifications

- o MCXV - Key Figures for Material Notification analysis
- o MCVZ - Key Figures for Vendor Notification analysis

❖ **SRM or Supplier Relationship Management:**

Authentication: Publishing of the bid invitation in SRM happens only after the scrutiny and approval of the department head.

Digital Signature Certificate (DSC): Use of Class III DSC which provides highest level of security and authentication for both purchaser and vendor. This prevents impersonation by vendors and purchasers.

Display of Bid Details: Details of submitted bids can be seen by authorised officers, only after the opening date and time is reached.

Extension of Bid: Extension of the bid is possible only before the bid opening date and time only.

Bid submission by vendor: Vendor will not be able to modify the bid after the submission deadline is passed.

➤ **ICH (Integrated Collaboration Hub):**

Online Purchase Order: Purchase Order can be viewed by purchaser pertaining to order published to him only which is also non-editable.

Online Purchase Order confirmation: Acceptance of purchase order by the supplier is done by supplier in e-mode and same is captured in ECC (Enterprise Central Component).

Online Delivery Challan Creation: Delivery is done through e-mode, where system does not allow despatching more than the purchase order quantity.

Dynamic Goods Receipt updates: Supplier will know for his despatch when the GR has been updated and its accepted quantity.

Information Management:

- o Vendor/ BEML can see the Purchase Order from-to date released to vendor.
- o Despatch details report can be extracted from BEML/ Vendor.
- o For a given period Vendor can extract the due list pending for despatch.

Conclusion:

Enterprise Resource Planning (ERP) applications constitute the first line of defence in helping to monitor for fraud risk. Stopping fraud before it occurs directly increases the organisation's bottom line and effective fraud risk management, among others, enhances the organisation's public image and reputation. It is, therefore, an integral part of the duties of every executive to deal with fraud risk by a continuous process of reviewing and addressing the significant risks of fraud. As stated in the Special Chapter on Vigilance Management in Public Sector Enterprises, 'Vigilance is basically and admittedly a managerial function and therefore, it is an integral part of the duties of an executive'.

Combating Corruption – Technology as an enabler

Technology is increasingly seen by governments as well as activists and civil society as important tools to promote transparency and accountability as well as to identify and reduce corruption. ERP and e Procurement solutions have been around for more than two decades now and they bring in lot of accountability in Governance. New technologies, in the form of websites, mobile phones, applications etc. can be used to facilitate the reporting of corruption and the access to official information. They are also used to monitor the efficiency and integrity of social services and of a country's political life, and to make financial information more transparent. Technology can also support campaigning efforts and help mobilise people against corruption. Over the last decade governments have launched an increasing number of e-government initiatives to enhance the efficiency and transparency of public administration and improve interaction with citizens.

Following are some areas where technology can help in combating corruption:

Automation, which can reduce the opportunities for corruption in repetitive operations.

Transparency, which can help reduce the room for discretion;

Detection in operations, to identify anomalies, outliers and under performance

Preventive detection through monitoring of networks and individuals;

Awareness raising to empower the public and inform it about its right to resist arbitrary treatment;

Reporting, to create complaint channels that can lead to concrete action and help

punish violations and close loopholes;

Deterrence, by disseminating information about reported cases of corruption;

Promoting ethical attitudes through public engagement and online discussions.

Frauds in Manufacturing Sector and Prevention:

As per the recent report published by Deloitte the manufacturing sector is often one of the most vulnerable sectors, which is exposed to the risk of fraud and corruption. Some of the most recent frauds in the manufacturing sector that have caused significant losses to companies have been due to inferior product quality triggering product recalls, warranty claims fraud and IP infringement. In some cases these have also resulted in criminal/ civil actions due to regulatory and statutory violations. As per Gartner one of the other most common frauds in manufacturing sector is inventory frauds, related to the theft or misuse of stocks, which continues to be a cause of concern.

A good ERP system can help to a large extent in addressing these issues. Over time, many companies have started to discover deficiencies in their information systems architecture. Most legacy business systems were made up of islands of automation – separate systems that handled some core business needs. There may have been systems to handle the General Ledger, another to handle the sales processes, a separate system to manage the manufacturing or production processes, etc.

Data had to be exchanged between these sub-systems in order to generate the reports that various levels of management needed to run their operations. When there were errors or inconsistencies between these sub-systems, these flowed on into the consolidation process

and skewed the management reports. Most of the purchases were done manually which was prone to errors and provided scope for corruption.

The main business benefit of using ERP is that the business gets comprehensive set of integrated, cross-functional business processes. Here are some other benefits of using ERP:

Audit trail feature captures details of all transactions like original value, changed value, date, time and who changed it. This brings in accountability and helps in investigations. The other major advantage of ERP system is electronic bill processing and payment which reduces the risks involved in manual processing and payments.

New IT trends for fighting corruption:

Some of the recent IT developments take the fight against corruption to a new level. Depending on the nature they can be **controlling, reporting or social tools**.

❖ Some of the controlling tools are:

GRC: GRC stands for Governance, Risk and Compliance. ERP has been great IT tool for conduct of business end to end. Most of the ERP vendors provide CRM and Procurement solutions also. GRC is a new offering which works with ERP and Procurement solutions.

Typical controls available under GRC are as follows:

- o **Access Control:** Confidently manage and reduce access risk across the enterprise. minimize fraud and lower the cost of access management and ongoing compliance activities.
- o **Audit Management:** Amplify the influence and value of internal audits – and provide

greater insight into key business risks – with audit management software.

- o **Access Control Violation Management:** Identify access control violations and review and report on their financial impact.
- o **Regulation Management:** Confidently assess and respond to regulatory intake and change – and ensure compliance – using a proactive, holistic approach to regulation management.
- o **Process Control:** Continuously monitor key risk indicators and compliance effectiveness across the critical business processes – and drive process efficiency and control.
- o **Risk Management Software:** Maximise risk visibility with comprehensive analytics, balance risk and opportunity – and protect business value by pro-actively preventing and mitigating risks.
- o **Fraud Management:** Detect fraud earlier – and improve prevention.

Web Proctoring: Web proctoring is mostly used for online tests wherein a proctor can monitor the candidates taking the exams using web camera. The candidates can access only the browser window where the test is active. They will not be able to access any other windows like calculator, search or local files.

Camera Surveillance: Camera surveillance can be an excellent tool for combating corruption if it does not infringe into right to privacy especially in places where there is scope for corruption. Kerala State Chief Minister has installed video cameras in his office and live stream is available for the general public to view it. One State in India announced that video of anyone giving or receiving bribe will be uploaded on social websites like Youtube and Facebook. Measures like this can definitely act as deterrent for corrupt practices.

❖ **Some of the reporting tools are:**

Data Mining and Business Intelligence: Data mining and Business intelligence tools help in detecting fraud patterns based on business rules.

Mobile Apps and SMS alerts: India's right to information movement had tremendous success in making strategic use of transparency for securing government accountability. Thanks to this success, demanding and disseminating information are among the most used tools in the work of activist organizations in the country today. Public records are typically demanded on paper and disseminated manually, making the process costly and slow. Over the last few years, governments have started making relevant information available online.

At the same time, the availability of mobile phones has exploded with more than half the households in India owning a mobile phone - even in India's poorest states. As the census commission soberly put, more families have mobile phones than toilets in India today. The project seeks to make use of these parallel developments to assist credible activist organizations to collect and disseminate information through the exploding network of mobile phones.

The recipients will be able to provide feedback and submit official complaints through a simple interface on their mobile phones, and the feedback can be used by activist networks for advocacy and collective action. Relevant and timely information is already an important part of the activist toolkit, and the project is based on the premise that this power can be significantly expanded through the use of technology.

❖ **Some of the social tools are:**

Youtube, Face book and blogs like Twitter can be made use as deterrent to report

bribery cases. Online reporting of Bribery on websites is effective tool which can be used as deterrent in reporting bribery cases. Such reporting can create social stigma for recipients of bribe.

Conclusion:

BEML has taken the right steps in adoption of IT with ERP-SAP based business suites. Adoption of new tools like Business Intelligence, GRC, Electronic File management system which are in the pipeline is expected to take this technology adoption to a higher level.

बी ई एम एल



VIGILANCE AWARENESS WEEK 2014

27th October to 1st November 2014

Combating Corruption - Technology as an ally
One Day Workshop on e-Procurement

27th October 2014





VIGILANCE AWARENESS WEEK - 2014

November 2



RED FLAGS IN PUBLIC e-PROCUREMENT/ e-TENDERING & SOME REMEDIAL MEASURES

ABSTRACT

Essentially, e-Procurement/ e-Tendering is conducting on the internet the equivalent of the manual tendering process, with the ostensible objective of enhancing Transparency and Efficiency of Public Procurement. While this naturally involves some re-engineering, it is important to ensure that under the pretext of re-engineering and technology, there should be no compromise on the security/ confidentiality, transparency and legal aspects of the well-established public-procurement process. The focus of the paper/ presentation will be on some such critical issues, or red flags, with suggestions for remedial measures.

INTRODUCTION

Some Distinctive Aspects of Government Tendering/ Public- Procurement Process: Public procurement constitutes 10% to 20% of the GDP in various countries. In addition to buying at the most economical price, the distinctive and 'stated-principles' of public procurement have been to ensure -- Transparency, Fairness and Accountability in the procurement process. Procedures for public- procurement have been developed to implement these stated-principles. Starting with advertising a bidding opportunity in a national-level newspaper for

The writer is Shri. Jitendra Kohli, B.Tech. (Electrical Engg) IIT Delhi (India), founder and Managing Director of Electronic Tender, who has been researching in the area of e-procurement/ e-tendering with focus on public procurement for over 12-years now. His work, 'e-Procurement Integrity Matrix' has been adopted and published by Transparency International India (Reference-1). The Government of India's guidelines for e-procurement (Reference-2) have taken inspiration from his writings on the security and transparency related aspects of e-procurement.

wider publicity, elaborate procedures exist in most countries for activities relating to the tendering process, which inter alia includes processes such as – 'Signing of each page of the bid by the bidder' to ensure authenticity, 'Bid-Sealing' to ensure confidentiality and independence of each bid, a fair and transparent 'Public Tender Opening Event' with its detailed procedures to ensure fair-play, et al.

E-Procurement, an emerging Methodology for Public Procurement: 'e-Procurement' or 'e-Tendering' is the emerging method for conducting 'Public Procurement' using the internet. As the name suggests, an e-procurement system/ portal will be accessed through the internet by authorized users of a Buyer organization, as well as, authorized users of different Supplier/ Bidder organizations for conducting various activities relating to the tendering process, ie bid invitation and response process, from the comfort of their respective offices. From Buyer and Supplier perspectives, an end-to-end e-procurement system is expected to offer broad functionality as outlined in Annexure-I of this paper. The depth and quality of implementation of each module may vary in each system, till standards emerge and are followed.

Overall, in terms of adoption and implementation, e-procurement is still in a nascent phase globally. While some countries like India are making e-procurement mandatory for Government procurement above a certain threshold value, many countries, including advanced countries in North America and EU, currently have limited e-procurement implementations for public procurement with rudimentary security features. However, the stated intent in many countries is to encourage e-procurement, as the potential benefits of e-procurement are compelling.

'Need for Re-engineering', and 'Need for Avoiding the Possibility of Cutting Corners on the Pretext of Re-engineering': With evolving technology, procedures inevitably undergo change.

As stated earlier, public procurement involves mammoth public expenditure in every country, and as an unfortunate consequence of this, scams and controversies have been associated with this sensitive area. Therefore, any re-engineering of the public procurement methodology while shifting from the manual tendering methodology to internet-based methodology (ie e-procurement), should be done with adequate due-diligence of the new methodology, and by taking adequate cognizance of loopholes of the new methodology. Specifically, in the process of re-engineering, the stated-principles of public-procurement should not be relegated or cast aside. However, the actual implementations of e-procurement in many countries are found wanting in this respect.

Benefits of e-Procurement: and some Associated Conditionalities: Undoubtedly, if e-procurement is done with proper security and functionality, it holds enormous potential for enhancing efficiency and transparency in public-procurement internationally, apart from the obvious benefits such as savings in time and cost, wider reach, et al. However, dearth of awareness about the intricacies of e-procurement/ e-tendering, especially aspects relating to 'Security' and 'Transparency', is resulting in proliferation of e-procurement portals in many countries which have numerous lacunae and pitfalls. In fact, many of the projected benefits of e-procurement are contingent upon the measures adopted in the e-procurement system (especially the e-procurement application software) to ensure security and transparency. A list of 'Salient Benefits of e-Procurement' is enclosed as Annexure-II. Needless to state, unless these lacunae and pitfalls are properly addressed with appropriate security and transparency related measures, e-procurement could actually be worse than the traditional manual

procurement/tendering process in respect of preventing manipulation and corruption.

The issues and remedial measures relating to secure e-procurement highlighted in this paper are based on the author's direct involvement for over twelve years in the process of innovation, original research and development of cutting-edge 'e-procurement application software'. Another noteworthy aspect is that while there is technical literature available, such as 'Reference Document-3', on the elements and tools (such as PKI-based digital signatures, symmetric and asymmetric keys/ tools for data encryption) which go into building an e-procurement application, there is very little detailed literature available on the 'technical intricacies' of a 'secure e-procurement application'. 'Reference Documents 1 and 2' are perhaps the most comprehensive documents addressing this need, which are available in public domain. Both these reference documents are inspired from the research and writings of the author. The present paper is another such document.

During the forthcoming IPPC5 conference, the author intends to make a presentation on the same subject with emphasis on a few select 'Critical Security Issues and Loopholes relating to e-Procurement Web-Application', which will elucidate some of the issues highlighted in this paper, as well as, set the backdrop for the paper.

OBJECTIVE

The objective of this paper is to highlight in a concise manner a few 'Security' and 'Transparency' related lacunae or 'Red Flags' in e-procurement, so that Government entities which implement e-procurement do so in a proper manner.

Note-1: While some references of legal acts are in respect of India, the main points made under the various 'Red flags' would be applicable for all countries.

Note-2: While highlighting the lacunae in the existing e-procurement systems, the author has deliberately avoided giving references of specific projects in different countries, although this information may be available with the author. It is left to the concerned authorities in each country to conduct a technical review of their respective e-procurement implementations, and take corrective action.

THE RED FLAGS

Overall Guiding Principle for Addressing the Red Flags: In terms of 'security and transparency', e-procurement should be better than the 'manual tendering' process, or at least as good. It certainly cannot be accepted if it is worse in this respect. Well established practices of manual bidding (or tendering), especially those relating to security and transparency, should have corresponding functional equivalents in e-tendering/ e-procurement application.

(Red Flag No.1): In many current e-procurement systems, the 'Bid-sealing/ Bid-encryption' methodology is non-existent, or poor/ flawed.

Background: In the manual process of bidding or tendering, bids are sealed in paper-envelopes to ensure 'confidentiality' of the bid before the Public Tender Opening Event (Public-TOE) from not only competitors, but also officers of the procuring entity. Sealing a bid in a paper envelope makes the bid data 'unreadable'. There has to be a functional equivalent of this in the electronic system also.

A re-engineered functional equivalent of a 'sealed envelope' can be an 'encrypted bid'. The process of encrypting the bid data achieves the objective of making the bid data 'unreadable', until it is decrypted during the Public-TOE.

However, if no such functional equivalent is provided in the re-engineered electronic system, or a vulnerable form of bid encryption is provided, it would vitiate the sanctity of the public procurement process under the garb of re-engineering.

On-the-Ground Situation in Flawed e-Procurement Implementations: The flawed e-procurement implementations fall into two broad categories;

Category-1: In such systems, the online bids which are submitted by the bidders are not encrypted at all. This would tantamount to bids being submitted without sealed envelopes. Administrators of the e-procurement portal and those having access to the database can peep into the contents of bids to help some preferred bidder(s), and thus compromise the 'confidentiality' aspect of the process. Such e-procurement systems are too unsecured and basic to be used for public-procurement.

Category-2: Bids are encrypted, but the bid encryption methodology is inappropriate for the requirement of secure public procurement. Now, essentially, there are two broad methods of data-encryption (ie bid-encryption in the context of e-procurement), viz – 'symmetric' and 'asymmetric'. Specifically, where asymmetric key (eg public-key of the bid-opening officer of the procuring entity) is used for bid-encryption, clandestinely made copies of bids can be stolen through spyware and secretly decrypted before the Online Public-TOE resulting in compromise of confidentiality. Similarly, bid-confidentiality can be compromised where the 'main bid-encryption' is done at database level, and only SSL encryption is done during the transit phase

from bidder's system to the e-procurement portal. In such systems, there are many other allied deficiencies relating to functionality and transparency. If system-generated symmetric-key is used for bid-encryption, it also has vulnerabilities as a copy of the key may be accessed by the system administrator for clandestine decryption prior to the Online Public-TOE. For a more detailed explanation of the issues, the reader may refer to -- a) Reference-1 (e-Procurement Integrity Matrix, especially sections II, III and partially IV); Reference-2 (e-Procurement Guidelines, Annexure-I, especially sections 2, 3, and partially 4); Reference-3 (Applied Cryptography, pp 33).

To justify the application of PKI for bid encryption in spite of the associated security vulnerabilities as briefly explained above, a 'misconception' is often propagated by vested interests that the Information Technology Act 2000 (Reference-4), ie IT Act, recommends the use of PKI for data encryption (ie bid encryption in the context of e-procurement). This is not correct. The IT Act does not prescribe any method of data encryption. The focus of the current IT Act is on use of 'digital signatures' for – authentication, non-repudiation and data-integrity of electronic records. Digitally signing an electronic document or record (or data) does not encrypt the data, i.e., it does not 'secrete' the data. The digital signature (which is created by first producing a one-way hash of the data being signed, and then encrypting the hash with the private-key of the signer) is distinct from the original record (or data) of which the signature has been created. The signature thus created can be kept separate from the original data. In this case, the original data (or record) remains as readable after the signature, as it was before the signature.

It may please be noted that highlighting the vulnerabilities of PKI- based bid-encryption in the context of public procurement should not be construed as a sweeping criticism of the use

of PKI for any form of data encryption. The criticism is only in respect of its use for bid-encryption in the specific context of public procurement. The merits and demerits of any tool or methodology have to be weighed with reference to the relevant context or situation.

Note-3: Each country is enacting its own electronic signature act. The Indian IT Act 2000 is also inspired from the corresponding UN Model law. The General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 adopted the Model Law on Electronic Commerce, adopted by the United Nations Commission on International Trade Law.

Furthermore, reputed international textbooks on cryptography have also clearly highlighted the limitations of asymmetric key based data encryption, especially in respect of its 'slowness' and 'vulnerability'. For a more detailed explanation of the issues, the reader may refer to -- section 2.5 titled 'Communications using Public-Key Cryptography' of 'Applied Cryptography' by Bruce Schneier (Reference-4, pp 33)

Brief Remedial Suggestions:

As stated above, internationally acceptable forms of bid encryption include – symmetric-key, and asymmetric-key (also referred to as PKI in some countries). Bid-encryption using 'bidder-created symmetric key/ passphrase' has distinct advantages (including being free of the vulnerabilities mentioned above), and has been used for the purpose of bid-encryption in the software of Electronic Tender developed under the guidance of the author. Where 'Requests for Proposals (RFPs)' for e-procurement systems allow both forms of bid encryption, the RFPs should specify that security vulnerabilities as described in sections II and III of the 'e-Procurement Integrity Matrix' (Reference-1) and sections 2 and 3 of Annexure-I of e-Procurement Guidelines (Reference-2) must be satisfactorily addressed by the e-procurement

application software provider with proper explanation. These explanations should be thoroughly vetted and tested by the Government department using the system as a procuring entity

(Red Flag No.2): In most e-procurement systems, instead of 'Online Public Tender Opening Event' (Online Public-TOE), or Bid Opening Event, there is only a rudimentary 'Online Bid Opening'.

Background: In the manual process of bidding or tendering, the sealed bids are opened in public, ie in the presence of the bidders who have submitted bids for a particular tender. Salient points of each bid are read out aloud, and each page of each opened bid is counter-signed by one or more tender-opening officers of the procuring entity. This is to ensure transparency and fair play. As per established principles of public-procurement, it is intended that in this event, each bidder should know what the other bidders have quoted, so that no unfair and clandestine changes are made later due to any connivance between a bidder and the procuring entity officers.

A re-engineered functional equivalent of the manual Public-TOE would be an 'Online Public TOE', in which the bids are opened online by the authorized tender opening officers of the procuring entity in the simultaneous online presence of bidders, along with other important procedures such as digitally counter-signing of the bids online by the TOE-officers in the simultaneous online presence of bidders.

However, if no such functional equivalent is provided in the re-engineered electronic system, or bids are merely opened online (without the simultaneous online presence of

bidders), and then subsequently put up for display, or corners are cut for example by not having online countersigning of the opened bids by the TOE-officers in the simultaneous online presence of bidders, it would vitiate the sanctity of the public procurement process under the garb of re-engineering.

E-procurement systems, where online TOE is conducted in this non-transparent fashion, without the simultaneous online presence of the bidders, gives rise to the possibility of bid-data tampering.

On-the-Ground Situation in Flawed e-Procurement Implementations: In a very questionable manner, most e-procurement systems have done away with the Online Public-TOE. As mentioned above, in such systems bids no doubt are opened online, but not in the simultaneous online presence of bidders. The procedures of manual tendering which are interactive in nature and conducted in the presence of other bidders, are thereby done away with. After opening, the bid contents may (or may not) be put up for display to the bidders. In either case, it gives rise to the possibility of bid tampering.

Brief Remedial Suggestions:

A comprehensive and transparent Public Tender Opening Event is the 'backbone of transparency and fairness' of the Public Procurement process, manual or electronic. It must be ensured that e-tendering/ e-procurement application has comprehensive functionality for a transparent Online Public-TOE. Well established practices of manual tender opening (with legal and transparency related significance) should have corresponding functional equivalents in the electronic system for transparent e-tendering/ e-procurement.

Some relevant processes of a fair and transparent Online Public- TOE should include:

- i. Opening of the bids in the simultaneous online presence of bidders with proper online attendance record. Merely opening bids online and then subsequently displaying some results to the bidders does not fulfill the requirements of a transparent Online Public-TOE.
- ii. Security Checks to assure bidders of non-tampering of their bids (during storage), et al during the online TOE itself.
- iii. One-by-one opening of the sealed bids in the simultaneous online presence of the bidders.
- iv. Allowing bidders to download the electronic version of the salient points of each opened bid (opened in the simultaneous online presence of bidders) simultaneous with the opening of that bid. (This would be the functional equivalent of reading out aloud the salient points of each opened bid in the manual system)
- v. There should be a procedure for seeking clarifications by the TOE officers during Online Public-TOE from a bidder in the online presence of other bidders, and recording such clarifications
- vi. Digital counter-signing (by all the tender opening officers) of each opened bid, in the simultaneous online presence of all participating bidders
- vii. Preparation of the 'Minutes of the Tender Opening Event' and its signing by the concerned officers in the simultaneous online presence of the bidders.

For a more detailed explanation of the issues, the reader may refer to -- a) Reference-1 (e-Procurement Integrity Matrix, especially sections V (3) and VI (8)); Reference-2 (e-Procurement Guidelines, Annexure-I, especially sections 5 and 6).

(Red Flag No.3): Most e-procurement systems do not have the functionality to accept 'encrypted (ie sealed) detailed bids'.

Background: In the manual process of bidding or tendering, for example in a single-stage-two-envelope tender, both the technical bid-part and the financial bid-part are separately sealed in paper-envelopes to ensure 'confidentiality' of each bid-part.

In the e-procurement system also it is expected that both bid-parts would be encrypted before being submitted.

However, if no such functional equivalent is provided in the re-engineered electronic system, it would vitiate the sanctity of the public procurement process under the garb of re-engineering.

On-the-Ground Situation in Flawed e-Procurement Implementations: Some systems 'do not encrypt the technical bid at all', ie neither the electronic template of the technical bid, nor the detailed technical bid. In such systems, typically 'only summarized financial data in electronic templates' may be encrypted. This is against the established practices of ensuring confidentiality of technical bids.

Brief Remedial Suggestions:

As in the manual tendering process, all bid envelopes, viz technical, financial, and pre-qualification, as applicable should be sealed, ie suitably encrypted by the bidders in the e-tendering/ e-procurement system. In e-procurement systems, a bid envelope may consist of an electronic-form (for capturing the summary or salient aspects of a bid, especially those which are typically read out during the public TOE in the manual system), as well as, an accompanying

detailed bid (which could be a large file). All bid parts must be encrypted and digitally signed. If required, printed brochures, manuals, physical samples etc can be submitted offline.

For a more detailed explanation of the issues, the reader may refer to -- a) Reference-1 (e-Procurement Integrity Matrix, especially sections II (3) and VI (6,7); Reference-2 [e-Procurement Guidelines, Annexure-I (especially sections 1.2, 6.1, 6.2) and Annexure-III].

(Red Flag No.4): Many e-procurement systems do not have the functionality for digital signing of important electronic records which are part of the e-procurement application.

Background: In the manual process of bidding or tendering, a bidder signs every page of the bid being submitted. This is for ensuring authenticity of each page of the document being submitted. Also, any subsequent change in the document (in the form of erasure or overwriting) has to be authenticated with signature of the bidder otherwise the change is unauthorized or can be the result of tampering. The need for a similar process is certainly not obviated in the e-procurement system. Unauthorized changes in an electronic document will not even be visible to the eye, unless adequate precautions have been taken.

A re-engineered functional equivalent of the physical signatures on a paper document can be the use of Digital-Signatures (based on PKI, or Private-Key-Public-Key pair). With proper implementation, a digitally signed electronic document can establish three things about the signed data-- authenticity, non-repudiation and integrity. With proper implementation, the integrity aspect establishes the non-tampering of the electronic document.

However, if no such functional equivalent is provided in the re-engineered electronic system, or weak or partial provisions are made, it would vitiate the sanctity of the public procurement process under the garb of re-engineering.

On-the-Ground Situation in Flawed e-Procurement Implementations: Some e-procurement systems do not use digital signatures at all. Some systems use it for only signing the bids. Some systems have facility for limited signing but corresponding facility for verification is missing, thus making the act of signing effectively useless.

To justify as to why they are not using digital signatures, 'misconceptions' are often propagated by vested interests (or out of ignorance) about the use of digital signatures. Some of these misconceptions are outlined below.

Misconception	Clarification
Digital signatures are expensive	It is incorrect to say that digital signature certificates are expensive. Cost has to be seen with reference to the context. Where tenders of value running into millions of USD (or even tens of thousands of USD) are involved, a bidder should not mind spending the equivalent of USD 10 to 30 for a digital certificate which will last him for a year or two. This would be equivalent to the cost of going by a cab from one's office to another office in the same city! The same certificate can also be used for other purposes.
Digital signatures cannot be used from web-cafes	This is incorrect. There is no technical constraint in the use of digital signatures from web-cafes.
For a foreign bidder (ie potential offshore supplier) to acquire digital signatures from the country of the procuring-entity, he has to travel to the country of the procuring entity	This is certainly not true for a country like India. The position can be checked for other countries. There are well established procedures, at least in India, for a foreign supplier's representative to get a certificate without travelling to India.

<p>User id and password can be as robust and reliable as any other method, including PKI</p>	<p>PKI-based digital signatures are being used for one or all of the following purposes / functions:</p> <ul style="list-style-type: none">a) To 'login' to e-GP portal/ applicationb) To establish the identity of the signatory of the electronic record/ document (eg an electronic bid, or bidding-documents)c) To sign the 'content/ data' of the electronic record/ document (eg an electronic bid, or bidding-documents)d) To protect against 'tampering' of the electronic record/ document (eg an electronic bid, or bidding-documents) , ie ensuring its 'integrity' <p>While other forms of electronic authentication (or electronic signatures) such as 'only password' (user id normally being a common factor) may achieve purpose 'a' mentioned above (with possibly lower security than PKI), it certainly cannot address other purposes mentioned above, and certainly not the aspect relating to non-tampering.</p>
<p>The UNCITRAL Convention (2006) considers other forms of electronic authentication equal to digital signatures</p>	<p>There are riders in the UNCITRAL Convention, and unless these are understood, misleading conclusions will be drawn. Furthermore, it may please be noted here that use of digital signatures is not just for the purpose of authentication. It also serves a very important role for establishing the 'integrity' (ie non-tampering) of electronic records. For example, while Biometrics may be considered as an alternative method of authentication, it would not serve the purpose in respect of ensuring integrity of electronic records.</p>

Brief Remedial Suggestions:

Use of digital signatures must be as per the letter and spirit of the IT Act 2000 (Reference-4) and its subsequent amendments for the purpose of -- authentication, non-repudiation and integrity of all important electronic records. Such electronic records should include -- tender notices and corrigenda, tender documents and addenda, online clarification of tender documents sought by the bidder, signing of bids (including modification and substitution bids) by the bidder, online counter-signing of all opened bids by the tender-opening officers in the online presence of bidders, online minutes of the tender opening event. Facility should be provided within the e-tendering/ e-procurement system to 'verify' digital signatures which have been affixed to the electronic records.

For a more detailed explanation of the issues, the reader may refer to -- a) Reference-1 (e-Procurement Integrity Matrix, especially section V; Reference-2 (e-Procurement Guidelines, Annexure-I, especially section 5, and Annexure-IV).

(Red Flag No.5): In most e-procurement systems, functionality of the system is limited [eg all types of bidding methodologies are not supported].

Background: In the manual process of bidding or tendering, depending on the circumstances and nature of a tender, one of the many bidding methodologies may be prescribed by a procuring entity, and the bidder would have to respond accordingly. These methodologies could include the following:

- a) Single-stage, single-envelope
- b) Single-stage, two-envelope
- c) Two stage (with facility for 'technical conformance', and if required, 'revised tender

documents')

d) Two-stage, two-envelope

e) Where required, the above may be combined with a Pre-qualification stage

f) In some cases, the procuring entity may allow submission of one or more alternative-bids

g) Each bid part (eg technical, financial) may be required to be submitted in a 'summary format' along with a 'detailed bid'. The latter could be a large file.

h) After having submitted the 'original' bid for each bid-part, a bidder has a right to submit:

- 'Modification' bid

- 'Substitution' bid

Or 'Withdrawal' bid for all his bid-submissions.

An e-procurement/ e-tendering system should provide the functional equivalent of the above methodologies.

However, if no such functional equivalent is provided in the re-engineered electronic system, or weak or partial provisions are made, it would vitiate the sanctity of the public procurement process under the garb of re-engineering.

On-the-Ground Situation in Flawed e-Procurement Implementations: In some e-procurement systems, only 'single-stage-single-envelope' bidding is supported, which may be good enough only for stores items. Similarly many systems do not support the submission of 'supplementary bids (viz modification, substitution and withdrawal)' after final submission, but before elapse of deadline for submission. This is against the established practices of manual tendering, and at best such systems offer partial functionality.

Brief Remedial Suggestions:

The e-tendering system should support all established bidding methodologies. Depending upon the requirements of a tender any one of the multiple bidding methodologies as outlined below may be used:

- Single-stage, single- envelope
- Single-stage, two- envelope
- Two stage (with facility for 'technical conformance', and if required, 'revised tender documents').
- Two-stage, two-envelope
- Pre-qualification stage, where required
- Where required, submission of one or more alternative-bids, as applicable
- Each bid part (eg technical, financial) may be required to be submitted in a 'summary format' along with a 'detailed bid'.
- The latter could be a large file
- There should be provision of appropriate file size (at least 10 MB) in the application with data encryption
- After having submitted the 'original' bid for each bid-part, a bidder should have the facility to submit:
 - 'Modification' bid
 - 'Substitution' bid
- Or 'Withdrawal' bid for all his bid-submissions.

The e-tendering/ e-procurement system must effectively cater to all these possibilities without compromising security and transparency in any manner at any stage, for any bid part

(such as pre-qualification, technical, and financial).

For a more detailed explanation of the issues, the reader may refer to -- a) Reference-1 (e-Procurement Integrity Matrix, especially sections VI (6); Reference-2 (e-Procurement Guidelines, especially sections '1.2, 3.1, Annexure-I (sections 1.2, 5.1, 6.1), Annexure-II, Annexure-III).

(Red Flag No.6): Many e-procurement systems are such that it results in abdication of powers of the concerned officers of the Government Procuring Entity.

Background: In the manual process of bidding or tendering in a large Government or public-sector procuring entity, there can be multiple indenting departments, multiple tendering authorities (ie entities which can invite tenders in their name), and tens (and sometimes hundreds) of officers involved with different activities relating to various tenders.

A re-engineered functional equivalent of the above administrative hierarchy is required if the concerned officers of the Government procuring entity are to perform their duties without abdicating their powers to others.

However, if no such functional equivalent is provided in the re-engineered electronic system, or weak or partial provisions are made, it would vitiate the sanctity of the public procurement process under the garb of re-engineering.

On-the-Ground Situation in Flawed e-Procurement Implementations: In many e-procurement/ e-tendering systems, the concerned departments and officers are not able to themselves execute their duly assigned roles as in the manual process, and are constrained to re-assign/ abdicate their roles and responsibilities to a few tech-savvy technicians or the

personnel of the service-provider of the e-tendering system.

Furthermore, in some situations this also results in handing over the private-keys (PKI) of the concerned officers to others, which is a violation of s-42(1) of the IT Act (Reference-4), and equivalent provisions, para 3(b) of Article-6 of the UN Model Law (Reference-5).

Brief Remedial Suggestions:

Changing over to e-procurement does not imply that the powers and duties (including those under the Official Secrets Act) of the officers for the core tendering processes can be passed on to 'third-party service providers', or to a few technical personnel within the procuring entity. Each officer, who currently enjoys powers and has responsibilities relating to procurement activities, should be able to exercise the same under the e-procurement system. The e-procurement system should support such functionality by facilitating a comprehensive hierarchy of officers, with specific role authorization facility.

For a more detailed explanation of the issues, the reader may refer to -- a) Reference-1 [e-Procurement Integrity Matrix, especially sections V (1, 2) and VII (7); Reference-2 (e-Procurement Guidelines, especially Annexure-I, (section 5.1)].

Note-4: The Red Flags described above essentially relate to the design and functionality of the e-procurement application. The two red-flags described below are not directly related to the core e-procurement application. However these are important allied concerns.

(Allied Red Flag No. i) : Diluting the Focus on Security, Transparency and Functionality of the core e-Procurement System by diverting attention to Integration with Backend ERP/ other Financial Systems:

Background: The prime objective of e-procurement strategy should be to first build secure, transparent e-procurement systems with all the required vital functionality. Once this is achieved, additional advantages can be gained through integration with back-end ERP/ Financial systems. This is important as approximately 80% of the public expenditure is through tenders which constitute less than 20% in number (Large-Value-Small-Number tenders). On the other hand, tenders which constitute less than 20% in value, make up for more than 80% in number (Low-Value-Large-Number tenders, or e-Purchasing). Because of the smaller number of 'Large-Value tenders', the existing financial systems are reasonably equipped to handle the financial record keeping part. Integration with backend ERP/ Financial systems would predominantly streamline 'e-Purchasing' which constitutes less than 20% of public procurement in value-terms, and is anyway not an area of major scams.

On-the-Ground Situation in Flawed e-Procurement Implementations: In some countries, without first strengthening and stabilizing the core e-procurement system(s), the attention is being diverted to integration with ERP/ Financial systems. In the process, the core e-procurement system(s) have very rudimentary security and transparency related functionality. This trend can prove risky in the sense that it can jeopardize the stated principles of public procurement, and compromise security and transparency.

Brief Remedial Suggestions:

Use of rudimentary e-procurement modules of ERP systems, or integration of rudimentary e-procurement applications with back-end ERP/ Financial systems should be avoided.

Integration with back-end ERP/ Financial systems can be taken up once the main e-procurement system(s) have stabilized.

If integration with backend ERP/ Financial systems is necessary, it must be ensured that there is no compromise whatsoever in the security, transparency related functionality and robustness of the core e-procurement system.

(Allied Red Flag No. ii): Misconceptions and Myths about Certified and Tested e-Procurement Systems

Background: Many e-procurement systems with weak functionality try to cover-up their vulnerabilities by using the following as a fig-leaf :

- Obtaining Certification for Security Tests like -- CERT, OWASP, FBI Top 20, etc
- Obtaining Certifications like -- ISO 27001 et al

While the above tests are important and useful, these are *not sufficient*. These tests are general in nature, and do not have anything specific to address the intricacies of e-procurement.

Furthermore, customization invalidates any previous certification. If e-procurement software is customized for each project, the above mentioned general security tests performed on some previous version of the software, lose their relevance.

Brief Remedial Suggestions:

- a) The main tendering processes of Government organizations are all within a standard framework, so there should be no need for customization for each project except possibly for 'integration with other applications'.
- b) Government of each country which is planning to adopt e-procurement should prepare detailed guidelines similar to the documents referred to herein as Reference-1 and Reference-2.

c) Government of each country should empower a department under their Ministry of Information Technology or equivalent to conduct 'e-procurement functionality and security related tests' as referred to in the Reference-2 document.

REFERENCES

1. “e-Procurement Integrity Matrix”. (2010). Transparency International India (TII).
URL: http://transparencyindia.org/integrity_matrix.php
2. “e-Procurement Guidelines.” “Guidelines for Compliance to Quality Requirements of e-Procurement Systems.” (2011, August 31). Department of Information Technology, Government of India.
URL: <http://egovstandards.gov.in/guidelines/guidelines-for-e-procurement/e-Procurement%20Guidelines.pdf/view>
3. Schneier, Bruce. (1996-2006). “Applied Cryptography.” John Wiley & Sons, Inc.
4. “Information Technology Act 2000.” Government of India.
5. “UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.” United Nations.
(Jitendra Kohli can be contacted at: jkohli@electronictender.com)

ANNEXURE-I

Typical Broad Steps in Government Tendering conducted manually (which are expected to have electronically conducted equivalents in an e-Procurement System):

(Buyer Perspective)

- Requisition/ Indent Approval
- Advertisement of Bid-Invitation/ Tender Notice/ Notice Inviting Tender (NIT)
- Advertisement of Corrigenda, ie amendments to a Tender Notice
- Sale/ Distribution of Tender Documents
- Distribution of Addenda, ie amendments to Tender Documents
- Responding to Clarification to Tender Documents/ Pre-Bid Meeting
- Receipt and secure Storage of Sealed-Bids
- Conducting a transparent Public Tender Opening Event (TOE). Some salient steps in a transparently conducted TOE include:
 - a) Authorized representatives of bidder organizations who have submitted their bids are entitled to be present and have to sign in their attendance.
 - b) Each bid is opened one at a time in front of the participating bidders, and the concerned bidder is entitled to satisfy himself that his bid packet is intact and has not been tampered with.
 - c) If Bid security [earnest money deposit (EMD)] is applicable for a tender, then details of the EMD submitted, or exemption claimed with basis thereof is disclosed to the participants.
 - d) Salient points of each opened bid are read out aloud for the benefit of the participating bidders, and to ensure that no change is made in the bid contents later

through connivance. Participating bidders take notes of the competitors' bid contents which are being read out.

- e) Clarifications may be sought from a bidder whose bid has been opened and record is made of the query and the response.
- f) Each page of the opened bid is countersigned during the TOE itself (by each tender opening officer (typically up to 3) to ensure that no change is made in the bid contents later through connivance.
- g) After all the bids are opened and countersigned by the TOE-officers, the minutes of the meeting (ie TOE) are to be recorded.
- h) Each bid part may be opened in a separate tender opening event in which only the authorized bidders are allowed. This is supposed to be done in a very transparent manner with proper scheduling of events and proper information to the concerned bidders.
- i) Bid parts which are due for opening in a subsequent tender opening event are securely stored till that event.
- j) If in a particular TOE, if it is decided not to open the bid of a bidder, then such bids are returned opened.
 - Evaluation of Bids and seeking Technical Conformance/ Clarifications, where relevant
 - Receipt and secure Storage of Sealed Revised Bids, where relevant
 - Follow-on Public Tender Opening Event(s) , where relevant
 - Award of Contract

(Supplier Perspective)

- Searching/ Viewing advertisement of Bid-Invitation/ Tender Notice/ NIT
- Searching/ Viewing advertisement of Corrigenda Procurement/ Receipt of Tender Documents Receipt of Addenda
- Seeking Clarification to Tender Documents
- Preparation and Submission of Sealed-Bids
- Attending Public Tender Opening Event (related activities are already covered under 'Buyer Perspective'.
- Responding to Clarifications sought by Buyer, where relevant
- Preparation and Submission of Revised Sealed-Bids, where relevant
- Attending follow-on Public Tender Opening Event(s) , where relevant
- Receipt of Award (or regret)

ANNEXURE - II

Salient Benefits of e-Procurement

❖ Summary of 'Overall' Benefits of e-Procurement to a Buyer Organization :

- Reduction in Time
- Reduction in Cost
- Reduction in Tedium
- Wider Reach
- Enhanced Security (Conditional)
- Increased Transparency (Conditional)
- Availability of Supplier Profiles
- Enhanced Choice of Vendors/ Suppliers (Increased Competition)
- Streamlining of the Procurement Processes (Conditional)
- Should get Better Prices because of reduced overheads of Suppliers
- Assists the top-management in ensuring better Control over the procurement activities of the organization with minimal physical intervention (Better Control with enhanced Accountability) [Conditional]
- Choice and combination of bidding methodologies, including sealed-bid e-procurement methodologies, combined with e-ReverseAuction methodologies for betterment of prices [Conditional]

❖ Summary of 'Overall' Benefits of e-Procurement to a Supplier Organization :

- Reduction in Time
- Reduction in Cost
- Reduction in Tedium

- Wider Reach
- Enhanced Security (Conditional)
- Increased Transparency (Conditional)
- Availability of Buyer Profiles
- Streamlining of the processes for participating in tenders (Conditional)
- Assists the top-management in ensuring better Control over the bidding activities of the organization with minimal physical intervention (Better Control with enhanced Accountability) [Conditional]
- Extended opportunity to win a bid in a transparent manner, in cases where the purchase organization resorts to e-ReverseAuction after the electronic sealed-bid round [Conditional]

Combating Corruption – Technology as an enabler, Defence Business

Defence Business Group, BEML has been utilizing technology to combat corruption in all spheres of Defence base operation. Some of the areas where technology has come to our support more effectively are ;

1. ERP System:

All the operations of the Defence Group have now been brought under the Enterprise Resources Planning (ERP) system which electronically manages preparation of planning based on approved production programmes, generation of Bills of material for products planned, generation of shortage list duly considering the stock and outstanding orders of individual items, structured preparation of purchase requisition (PR), floating of tenders for procurements based on PR, receipt of quotes, preparation of comparative statements, placement of orders, receipt of items by the respective divisions, stocking of items, generation of Material requisition, issue of items for production, generation of production job cards, store crediting at each production levels, maintenance & updation of approved vendor list (AVL), order booking from customers, sales, receipt of payments against sales, payment to vendors, payroll, release of salary & wages, release of payment against sundry expenditure etc.

All the above activities are controlled in ERP System with proper interlocks protected with appropriate authorization requirements built in to prevent any inadvertent mistakes or deliberate wrong doings. The system does not permit any manual intervention without due authorization. Due to this, any possibility of malpractices is plugged in the all functions of the

The writer is Shri. P.R.Naik, Director on the Board of BEML Limited, Defence Business.

company is prevented to a large extent.

2. SRM System:

The Defence Business Group ensures all procurements above Rs.1.0 lakh value have been brought under E-procurements which necessitates floating of tenders, receipt & opening of quotes , preparation of comparative statements , placement of orders etc. to be done through an online system which are protected with digital signature. To enable the above, Defence Business Group has adopted Supplier Relationship Management(SRM) system which sits on ERP platform. By strictly adhering to the system, any possible malpractice with regard to procurement is eliminated.

3. PLM System:

Through the Product Life Cycle Management (PLM) system insisted upon by the Defence Business Group, all functions related to design, documentation, drawings etc. are controlled thro a common computer network which enables all users - not only the internal users such as purchase, production, quality, costing etc. but eventually even with vendors to access the above the documents through the network. This ensures the updated documents are only available to all the users there by preventing any accidental / deliberate errors in the item supplied by them. There by design / drawing related malpractices are eliminated.

4. Protected Communication system:

In addition to the above, adhering to a system of communications within / outside organization through a protected gateway and service provider insulated from possible hacking / cyber attacks ensures protection of information and prevents information leakage.

Leveraging Technology for Transparency in Human Resource Functions

It is normally assumed that 'getting things done' is the only determinant for career success, no matter whether short cuts have been taken or compromises have been made in pursuit of personal accomplishments. However, in such quests for self glory and career progression, there could be real consequences and real costs if unethical behavior and corrupt practices have been followed. Doing business under tight time schedule and fixed budget may tempt local managers, and senior managers would be willing to turn a blind eye. But once a fraud is discovered the middle managers and frontline employees would pay a heavy price for deviating from ethical principles. In the final analysis, individuals who persist and persevere no matter what the temptations are, fare better than their less ethically perceptive peers, and scale greater heights in the corporate ladder.

Seamless availability of information on latest policies and procedures, and activities that have taken place in the Company and are planned, would provide a clear sense of organizational responsibility and an assurance that organization is efficiently administered and is free of any malpractices or corruption. These are important components of transparent corporate governance which essentially, is the principle of allowing those affected by administrative decisions to know about the resulting facts and figures and about the process that resulted in those decisions. Transparency is a fundamental element in abolishing corruption and controlling corruption is possible only when all stakeholders cooperate to ensure transparency especially the Human Resources (HR) Department.

HR transformation enabled by HR technology can result in realization of the strategic role of HR and specific measures such as e-learning, e-recruitment etc to make HR functions

The writer is Shri. Deepak Kumar Hota, Director on the Board of BEML Limited, Human Resources.

effective, efficient and at the same time transparent. HR department can use the internal web space to create company blogs and intranet pages, keeping employees in the loop about happenings in the Company. Thus the employees would feel that they are the integral part of the Company playing their roles towards achievement of business goals, improving morale and helping them to work towards a bigger goal.

The need for effectiveness and transparency in processes and service delivery mechanism is a long-felt one since large volumes of files are being managed and processed in all the offices. File Tracking Management System (FTMS) is a step to obviate shortcuts and prevent misdemeanors to a large extent. FTMS offers clear visibility of the file movement throughout the file approval process and helps to monitor the pendency of receipts and files and assist in their easy tracking.

Training Advisory Councils (TAC) formed at Divisional and Corporate levels have taken on the mantle of ensuring efficiency and transparency in nomination for training as per organizational requirements. Dissemination of training calendar and enrolling for training programmes online in HR portal would make this initiative more robust ensuring that training aligns with organizational requirements with requisite transparency in the process.

By housing key HR information in a secure and password protected employee self-service portal, employees can conveniently review and change their personal information, and receive information about themselves and the company. This will not only expedite the information gathering process, but more importantly, it would free up the HR department so that they can focus on more strategic activities. By automating routine HR tasks, organization can ultimately deliver far greater gains for the Company than was ever thought possible, since it enables HR professionals to give unfettered focus on developing the workforce and aligning their efforts with the corporate goals.



ಬೆಂಗಳೂರು ಅರಣ್ಯ ಸಂರಕ್ಷಣೆ ಮತ್ತು ಅಭಿವೃದ್ಧಿ ವಿಜ್ಞಾನ ವಾರ 2014
BENGALURU ARANYA RAKSHANA MURTHU ABHIVRUDHI VIGNANA VARA 2014

ಬೆಂಗಳೂರು ಅರಣ್ಯ ಸಂರಕ್ಷಣೆ ಮತ್ತು ಅಭಿವೃದ್ಧಿ ವಿಜ್ಞಾನ ವಾರ 2014
BENGALURU ARANYA RAKSHANA MURTHU ABHIVRUDHI VIGNANA VARA 2014

ಬೆಂಗಳೂರು ಅರಣ್ಯ ಸಂರಕ್ಷಣೆ ಮತ್ತು ಅಭಿವೃದ್ಧಿ ವಿಜ್ಞಾನ ವಾರ 2014
BENGALURU ARANYA RAKSHANA MURTHU ABHIVRUDHI VIGNANA VARA 2014

ಬೆಂಗಳೂರು ಅರಣ್ಯ ಸಂರಕ್ಷಣೆ ಮತ್ತು ಅಭಿವೃದ್ಧಿ ವಿಜ್ಞಾನ ವಾರ 2014
BENGALURU ARANYA RAKSHANA MURTHU ABHIVRUDHI VIGNANA VARA 2014

BEML LIMITED
KGE COMPLEX
WELCOMES
VIOLANCE AWARENESS WEEK-2014
FOR A GUEST LECTURE
SHRI K. SUBRAHMANYA
Hon'ble Feet Track Judge



*Vigilance Awareness Week 2014
Some Moments*

Combating Corruption – Technology as an enabler, Finance Management

It was about six months back that I attended a lecture on vigilance awareness in Hyderabad, where the impact of technology on corruption was discussed. The most common example came up for discussion- the booking of the humble railway ticket. Prior to computerization , examples were made of these petty railway officials by arresting them, dismissing them etc but the menace of this illegal gratification(the buyer and the receiver are to be faulted) could not be curbed. How ever once computerization of this rail booking was completed on an all India basis, this has almost been eliminated. I use the word almost because it still exists but this has become difficult and if this is discovered it is very clear as to who is responsible.

There are so many examples where technology can cover malpractices, however I shall try to comment on a few:

- 1) **Payment to Vendors through RTGS-** I rarely hear any complaint from vendors regarding this. In the earlier days there would be a disgusting nexus between vendor and all the links in the payment chain. Today with ERP in place, the payment chain exists inside the computer and on the due date the payment is made. With increasing sophistication in programs, vendors, vigilance and auditors can see each link in the payment chain clearly making the system accountable for lapses , if any. It will also clearly show where accountability is to be placed.
- 2) **Vendor bases-** Only those vendors who have been selected through a transparent process can be added to the IT system. The IT system will interact with only such

vendors. Today thanks to IT, vendors cannot have multiple bank accounts. The system will only deal with such.

- 3) **Attendance** – Appointment of ghost workers etc. Again a combination of RTGS and bio metric attendance can totally eliminate such a practice. Even if resorted to , it shows the links clearly and the people involved can be identified.
- 4) **Auctions and E Tenders** - The registered vendors can compete in a transparent manner in which the organization stands to benefit. The programs can be made so sophisticated that only those vendors complying with all tender terms can be allowed to enter the electronic platform

The list can go on and on . These are just a few common cases that have been highlighted. Asset management, shares that are now in Demat form, filing of IT returns electronically , all have contributed significantly to the elimination of corruption and fraud. This has resulted in our country moving up in the honesty index.

- 5) At Government level, Government of Karnataka has introduced SAKALA wherein the services of government can be had in a time bound manner, like KHATA, Birth Certificates, registration etc.

E-Governance has brought about good governance. Even the Police have started using computer applications to register complaints without visiting the Police Station, which also eliminates giving bribe to get the complaint registered. Follow up of the complaint is made easy and disposal of the complaint is also known to the complainant.

Combating Corruption – Technology as an enabler, Rail & Metro Business

Corruption is the misuse of public power, office or authority for private benefit. This misuse manifests in many ways like bribes, influence, nepotism, fraud etc. In many parts of the world a major part of the problem in dealing with public sector or government bodies is corruption.

Recent innovations in information and communication technologies have given hope to the idea that new technologies in the form of e-commerce can be used to combat corruption in the public sector. Most public sector units desire their business partners to interface with them through electronic means for the reasons of efficiency, cost saving and transparency in the processes and also information sharing for the purpose of eliminating corruption.

Focusing on the information required for processing an e-commerce transaction is vital in the setting up of digital system for information processing. The following three attributes are necessary for total information requirement.

- 1) completeness
- 2) clarity
- 3) ease of accessibility

- The adequacy of available information to process a task is captured by the term completeness.
- Clarity is the expectation that information provided is in a form and language that is easy to understand
- Ease of accessibility indicates the ease with which people who need it can find and access

that information.

Many public sector units having large interface with the public or businesses have chosen to go online. Communication technology like internet and mobile phones enable greater access to information .But sometimes some of the websites are ineffective because their focus is on the single objective of providing electronic access to information and they are nothing more than electronic copies of printed brochures. However there are also websites which are more interactive and give the required information. This is the positive development.

Public sector units procurements are sometimes points of corruption. Manual procurements in the earlier days included printing of tender requirements and dispatching them through registered post to the approved vendors. This had some shortcomings like delay in the receipts at the receiver end, complaints of non-receipt of tenders, incomplete packages of information dispatched.

On the other hand receipt of tenders through manual mode used to bring in complaints like rejection of offer declaring as late though received in time, declaring non-receipt of offers though actually received, replacement of offers at receiving end etc. The evaluation of offers manually can bring in arithmetical errors in computation, probable misleading or suppressing information etc. leading to taking wrong decisions.

Use of technology enablers like e-procurement system increases the transparency by keeping a traceable record of transactions online.

A comprehensive e-procurement system includes main components viz: vendor information and registration, e-tendering, e-purchasing, vendor-rating, detail of past procurements including prices thereof etc.

The first component provides adequate public notification for registration of businesses with the Company through a formal process of assessment of their capabilities to meet the Company's requirement as and when they arise. The businesses no longer have to search through newspapers or public tender bulletins to know about the Company requirements of goods or services. They only need to register along with required documents indicating the areas of interest in which they can provide goods and services.

The e-tendering process specifies the goods or services requirement the Company is looking for, time limit for submitting an e-offer and the mode of submission of e-offers whether it be e-tender or e-auction. Emails will be sent to all registered and approved vendors of the Company in case of limited tenders and providing an equal opportunity to all firms to submit their bids.

At the conclusion of bidding process the e-system provides the result of who participated, time of submission of the offers and uniform evaluation of all bids received.

E-purchasing includes release of purchase orders online against the evaluated and accepted bids, the receipt of goods and their entries online, process of quality confirmation of the goods received and payments to the vendors.

Vendor rating reflects performance of the vendors and facilitates deletion of those vendors who have not participated in tendering process through submission of offer for a considerable period of time or have delayed the supplies or have supplied sub-standard goods or have backed out in the past.

The availability of past procurement details such as specifications, prices, terms & conditions including past suppliers etc. act as benchmark for subsequent purchases & help in

making proper purchase decisions.

More sophisticated online applications include e-tracking of the purchasing process from the receipt of goods or services at the Company, status of processing of the vendor bills processing till it is results into payments.

The benefits from e-tendering/e-procurement include convenience (location and time), shorter waiting periods, reduced administrative corruption, elimination of complaints from loss/ non receipt of tenders, purchase orders, vendor bills etc. and bringing in greater transparency and reduced corruption possibility compared to manually handled systems in view of historical transactions data available online

The process of building an online system requires the rules and procedures be standardised and made explicit across the Company and therefore capable of computer coding. This reduces the discretion and an opportunity for arbitrary action available in the manual mode.

Other technology enabled systems include barcode mechanism of physically tracking the components from the vendors to the Company premises thereby minimising the risk of transit losses and pilferage.

However executives require frequent exposures and refresher trainings to newer technologies available to minimise manual interventions and thereby increase the effectiveness of the technologies used. This is being provided as part of training requirement on a regular basis to all.

CD USER GUIDE

I.

Live Recording
of
One Day Workshop
on
e-Procurement
to
inaugurate
Vigilance Awareness Week - 2014
on the
Theme: 'Combating
Corruption-Technology
as an enabler'

II. ICT & e-Governance

National:

1. National Portal of India: <http://m.india.gov.in/>
e-government initiatives : <http://india.gov.in/e-governance>
2. Department of Electronics and Information Technology <http://deity.gov.in/>
3. My Government: <https://mygov.in/>
4. Open Government Data (OGP) Platform India: <https://data.gov.in/>
5. e-Governance Standards : <https://www.egovstandards.gov.in/>
6. e-Governance –strategies for today, Vision for future:
<http://www.egovindia.org/about.html>

7. Department of Administrative Reforms and Public Grievances.:
<http://www.darpg.gov.in/>
8. Open Government Platform(OGPL):<http://ogpl.gov.in/>
9. The Indian Government Tenders /information system:<http://tenders.gov.in/>
10. Online Information Guide, Government of India: <http://vikaspedia.in/index>
11. Central Public Procurement Portal, Government of India
<http://eprocure.gov.in/cppp/>
12. Fighting Corruption the Electronic Way
<http://egovreach.in/social/content/fighting-corruption-electronic-way>
13. Central Vigilance Commission: <http://www.cvc.nic.in/>
 - i) Implementation of e-tendering solutions –a check list:
http://cvc.gov.in/009vgl002_30042010.pdf
 - ii) Procurement of Works, Goods and Services - Guidelines on Tenders/Use:
http://cvc.nic.in/proc_works.htm
 - iii) Quarterly Progress Report: http://cvc.nic.in/cir_31072012.pdf
 - iv) How to become a Vigeye?
<http://www.vigeyegpms.in/vigeye/?module=main&action=firstpage>

14. Right to Information Act: <http://rti.gov.in/>
15. E-procurement Integrity Matrix, Transparency International India:
http://transparencyindia.org/integrity_matrix.php
16. Bhoomi Project Website: www.Bhoomi.karnataka.gov.in

International:

1. United Nations E-Government Survey 2014:
http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf
2. Technological Innovations to Identify and reduce corruption:
<http://www.u4.no/publications/technological-innovations-to-identify-and-reduce-corruption/>
3. Use of Mobile Phones to detect and deter corruption:
<http://www.u4.no/publications/use-of-mobile-phones-to-detect-and-deter-corruption/>
4. Golden Book of e-procurement Good Practice
http://ec.europa.eu/internal_market/publicprocurement/e-procurement/golden_book/index_en.htm

5. UNCITRAL Model Law on Public Procurement (2011)
http://www.uncitral.org/uncitral/en/uncitral_texts/procurement_infrastructure/2011Model.html
6. Purchasing and Procurement Center- 5 e-procurement advantages:
<http://www.purchasing-procurement-center.com/e-procurement-advantages.html>
7. Organisation for Economic Co-operation and Development:
<http://www.oecd.org/>
Methodology for assessing Procurement Systems:
<http://www.oecd.org/dac/effectiveness/45181522.pdf>
Using New Technologies to Fight Corruption:
<http://www.oecd.org/corruption/ethics/2409234.pdf>
8. The World Bank: Fighting Corruption with Information Communication Technology:
<http://web.worldbank.org/WBSITE/EXTERNAL/COUNTRIES/EASTASIAPACIFICEXT/0,,contentMDK:23094328~pagePK:146736~piPK:146830~theSitePK:226301,00.html>

9. Top 10 Areas Where Data Analysis is Adding the Most Value:
<http://www.audimation.com/articles/top-10-areas-where-data-analysis-is-adding-the-most-value.html?url=articles%2Ftop-10-areas-where-data-analysis-is-adding-the-most-value.html>

10. E-government as an anti corruption strategy:
<https://ideas.repec.org/a/eee/iepoli/v21y2009i3p201-210.html>

11. West, D.,(2006)'Global E-Government, 2006'.
<http://www.insidepolitics.org/egovt06int.pdf>

12. Park, Hun Myoung(2005)'A Cost benefit analysis od the Seoul OPEN system: Policy lessons for electronic Government projects', HICSS
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1385493&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D1385493

13. Prakash, A., and De,R(2007) 'Importance of development context in ICT4D projects: A study of computerization of land records in india
http://www.iimbernet.in/~rahulde/Prakash_De_ITandP2007Article.pdf

14. Shim, D.C., and Eom, T.H. (2009) 'Anticorruption effects of Information communication and technology (ICT) and social capital'. International Review of Administrative Sciences, 75(1):99-116.
<http://ras.sagepub.com/content/75/1/99.full.pdf>
15. Lau, E. (2001) 'E-government and drive for growth and equity'. Organization for Economic Cooperation and Development E-government Project.
<http://belfercenter.ksg.harvard.edu/files/lau-wp.pdf>
16. Wescott, C.G., 2003, e-government to combat corruption in the Asia Pacific Region, 11th international Anti-corruption conference, Seoul, Republic of Korea, 25-28 May 2003
<http://www.adb.org/sites/default/files/publication/28986/egovernment-asia-pacific.pdf>
17. Chene Marie, Use of mobile phones to detect and deter corruption (2012),
<http://www.u4.no/publications/use-of-mobile-phones-to-detectand-deter-corruption/>

18. Fung, A., Russon Gilman, H., and Shkabatur, J., 2010, Technologies of transparency for accountability: an examination of several experiences from middle income and developing countries, analytic report.
http://www.right2info.org/resources/publications/tech-oftransparency-for-account/at_download/file
19. Gronlund, A. et al, Increasing transparency and fighting corruption through ICT: empowering people and communities, SPIDER ICT4D Series No. 3 | 2010,
http://spidercenter.org/polopoly_fs/1.163640.1390315885!/menu/standard/file/Spider%20ICT4D%20series%203%20Increasing%20transparency%20and%20fighting%20corruption%20through%20ICT.pdf
20. Technology for transparency Network, Technology for transparency: the role of technology and citizen media in promoting transparency, accountability and civic participation (2010),
<http://ifap-is-observatory.itk.hu/node/498>
21. Tisne M., Harnessing the potential of new technologies in governance reform, Transparency and Accountability Initiative Note for World Bank (2010),
http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/TAI_Note_by_MartinTisneforpresentation.pdf

- 
22. UNPAN, E-government survey (2012),
http://www.unpan.org/egovkb/global_reports/08report.htm
 23. UNPAN, Knowledge Base of Innovative E-Government Practices ,
<http://www.unpan.org/DPADM/EGovernment/KnowledgeBaseofEGovernmentPractices/tabid/828/language/en-US/Default.aspx>

Acknowledgement

The support extended by the Functional Directors on the Board of BEML Limited, Chief Information Officer and Corporate Communication Department is acknowledged

VIGILANCE DEPARTMENT

BEML LIMITED

BEML SOUDHA 23/1, 4th MAIN, S.R. NAGAR,
BENGALURU - 560 027. KARNATAKA INDIA.

Ph : +91 80 22223066, Fax : +91 80 22963277,

e-mail : bemlvig@beml.co.in Website : www.bemlindia.com

ICT & e-Governance

e-Government Initiatives

C
O
R
R
U
P
T
I
O
N

P
R
O
N
E

A
R
E
A
S

Transaction Level

- Receipt of taxes and revenues
- Payment of benefits
- points of service delivery
- Copies of government records
- License and permits

CENTRE

- Apply / verification / registration for PAN ,TAN online
- Online TDS statement
- File Income tax/TDS/wealth tax online
- Online tax payment
- Check refund of tax refund online
- E-filing of central Excise/ Services tax returns
- Online status enquiry of Passport application
- Online pension payment order status enquiry
- IRCTC – online ticket booking
- Online issue of License and permits

STATE

- State Data Centres
- Nemmadi Project
- (Digitization of Land records: Bhoomi Project (Karnataka) Bhulekh (UP) MP Bhuabhilekh (MP)
- Bangalore One
- Treasuries Computerisation

INTEGRATED

- e-Biz
- EDI (Electronic Data Interchange) for trade (e-trade)
- India Portal

Administrative Level

- Appointments
- Transfers and postings
- Promotions
- Procurements
- Allocation of scarce resources
- Admissions
- Evaluations

CENTRE

- Common Entrance Exams
- Online Application of yearly exams
- e-Procurement
- CPPP (Central Public Procurement Portal)

STATE

- State Data Centres
- Nemmadi Project
- Bangalore One
- HRMS
- Shikshavathini
- Mobile One
- e-District
- e-panchayat
- Employment Exchange

INTEGRATED

- e-procurement
- CSC (Common Service Centers)
- India Portal

Policy Level

- Biased Policies
- Reluctance to reform acts & rules
- Excessive centralization of power
- Reluctance to enhance transparency
- Status Quoism

CENTRE

- RTI
- Project-VigEYE
- Aadhaar

STATE

- e-courts

INTEGRATED

- e-Courts
- e-gazette
- NSDG (National e-governance Delivery Gateway)
- India Portal