Chapter II: Systemic issues

2.1 IS Strategic Plan

DoS does not have any IS Strategic Plan for the strategy involved migration from distributed operations to a centralized implementation, thereby consolidating the infrastructure and hosting the applications centrally. However, the Strategic Plan referred to by the Department was the IS Consolidation Project, which was proposed in 2004 and implemented by 2011. The department also does not have any long term IS Strategic Plan for the future, after the completion of the planned migration to centralized system.

Ideally, a large government department would be expected to have a formal IS Steering Committee comprising of various stakeholders including the IT department. The Committee would be responsible for the overall direction of IS. Once the Committee agrees on a future direction for IS, the decisions need to be formalised and documented in the IS Strategic Plan. The organization needs to develop IS plans according to its corporate strategy and match its IS needs for a given future period. This can provide the department with increasing potential for:

I. Enhancing the value of existing products or services,
II. Providing new products and services, and
III. Introducing alternative delivery mechanisms.

To benefit from IS requires foresight to prepare for the changes, and planning to provide an economical and effective approach. IS planning provides a structured means of addressing the impact of technologies, including emerging technologies, on an organization. Through the planning process, relevant technologies are identified and evaluated in the context of broader business goals and targets. Based on a comparative assessment of relevant technologies, the direction for the organization can be established.

CBEC's IS management style is repeatable but intuitive with few definable processes and creates a risk of undetected non-compliance in a rapidly changing business and technology environment. There were few qualitative changes in the management of IS while migrating from ICES 1.0 to ICES 1.5 as observed by C&AG since 2008 Performance Audit. Though DoS informed that they have drawn up risk registers and identified the risks, the register(s) were not produced to audit for scrutiny. Similarly management of benchmarks for measurement of the Key performance indicators that cover timeliness and quality of services were deficient as indicated by the systemic issues and those based on scoping and functionality of the application.

Recommendation: *The department may consider constituting a Steering Committee for developing IS plans according to its business strategy in consonance with its future IS needs.*

CBEC in its reply (January 2014) stated that after completion of the Consolidation Project, the Department has been focusing on building additional functionalities and interfaces amongst different applications. The Annual Chief Commissioners' conference held on 17-18 July 2013 deliberated on DRISHTI (Driving Information Systems for Holistic Tax Initiatives) - IT Vision for improving the efficiency and effectiveness of Indirect Tax Administration. Under this initiative, it is proposed to set up a High Powered Committee (HPC) which will examine all issues to evolve appropriate roadmap for actualization of DRISHTI. The Charter of this HPC will include:

(i) Identification & Formalization of the strategic objectives for achieving DRISHTI;

(ii) Identifying data to support the business objectives;

(iii) Recommending appropriate IT architecture to support business services;

(iv) Suggesting security, obsolescence and archival policy, and

(v) Evaluating the need for a Consultant to implement DRISHTI.

In addition, DRISHTI also envisages setting up of a small group headed by Member (Computerisation) CBEC, to study issues which require immediate attention and decide the sequence/priority for implementation, in view of current resource constraints in Systems.

CBEC further (February 2013) informed that approval for formation of HPC has been received by them on 20 February 2014.

However, CBEC neither furnished any record relating to formation of HPC along with its terms of reference nor provided the copy of the latest IS Strategic Plan to audit.

2.2 Monitoring by Senior Management

CBEC had committed to having an internal monitoring mechanism comprising of a high level Project Steering Committee chaired by the Member (IT) and Operations Committees chaired by Director General (Systems). These Committees would also include representatives from stakeholder communities and external consultants. However, DoS has stated (June 2013) that although such a Steering Committee was formed at the time of project implementation, it lacked the necessary focus and the implementation was done under the supervision of the Member (Computerisation) and Director General (System).

The Directorate presently has monitoring committees like IS Security Steering Committee, Change Advisory Board, Infrastructure Review Committee, etc. for monitoring specific areas.

CBEC in its reply (January 2014) stated that no comments are required on this issue. However, in their reply (February 2014) it was stated that DoS adopted 25 key indicators from system monitoring perspective, some of which are compliance indicators and others are numeric/percentage indicators. These cover availability, incidents, changes, security, user access and business continuity. These are reviewed by Information Security committee every quarter during the quarterly security review meetings. In addition to the SI (System Integration) team which generates daily, weekly and monthly system reports for CBEC for monitoring the system performance, user response time, e-filing and e-payment etc., there is a Change Advisory Board (CAB) comprising exclusively of CBEC officers that meets every week to approve major and significant changes to the system. All the changes to the system are entered into Service Manager Tools and audited by third party auditors bi-annually.

Reply of CBEC is not acceptable, as no records/reports in respect of changes were produced to audit to substantiate their claim. Copies of the Service Level Agreement with third party auditor or their bi-annual audit report were also not produced to audit.

2.3 Human Resource Development

One of the terms of reference of the Empowered Committee formed to monitor and supervise the IS Project implementation was to decide on issues relating to personnel matters and policies concerning staff assigned to work on Systems Projects. According to paragraph 5 of the Cabinet Committee on Economic Affairs (CCEA) note, there would be an ongoing process of review of the manpower and skill set requirements during the course of the project. Further, the Secretary (Revenue) had stressed (Paragraph 4.1 of the Cabinet Committee on Non-Plan Expenditure (CNE) minutes dated 09 August 2007) that mechanisms should be evolved for vendor management and the process of Project Monitoring should not be left entirely to M/s Price Waterhouse Coopers (PWC). Moreover, at the CNE/CCEA stage, the Additional Secretary (IT) had suggested that sufficient internal competencies need to be built, in addition to PWC and IIT-Delhi.

However, on being asked whether there is any strategic plan for selection, recruitment and retention of personnel for its ICT Systems, DoS stated (June 2013) that they are not aware of any such strategic plan on these issues.

Presently, nearly 98 percent of customs transactions are being processed through ICES and the department is entirely dependent on its IS systems for assessment and collection of customs revenue. Therefore, by not having a personnel policy for recruitment of technically qualified officers to manage the IS systems, the department is failing to build internal competencies and limiting its options for better management and monitoring the IS Systems to the third party vendors/ service providers who manage the IS systems.

Recommendation: *A personnel policy for development of internal competencies for management of the CBEC's IS management, by recruitment, development and training of IT personnel may be developed for smooth operations of the department's mission critical IS systems.*

CBEC in its reply (January 2014), while accepting Audit's suggestion regarding development of a personnel policy for development of internal competencies for management of CBEC's IT systems by recruitment, development, training and retention of IT personnel for continued smooth operations of the department's mission critical IT system, stated that the present engagement model for monitoring and supervising the project involves IRS (C&CE) Officers supported by Project Management Unit (PMU) manned by Price Waterhouse Coopers (PwC). The PwC consultants only provide assistance to the CBEC officers and as such, there is no delegation of responsibility to the PMU. In fact, all the projects are actively monitored and supervised by the Project Teams headed by Addl. Directors General (Joint Secretary rank officials) from CBEC. For the technical inputs, a formal engagement in the form of Technical Experts Group (TEG) is operational and a team comprising of three Professors from IIT Delhi help the teams on a regular basis.

CBEC further stated (February 2014) that IT setup in the CBEC is headed by Member (Computerisation) and consists of Director General Systems supported by 8 Addl. DG/Commissioners, 15 Additional/Joint Directors, 14 Deputy / Asst. Directors. Approval for formation of HPC has been received only on 20.02.2014. As regards the TEG, the same was functional only during the implementation phase of the consolidation Project and is not functional currently. For technical inputs, IIT New Delhi is consulted wherever felt necessary. The PMU only provides support to individual project teams headed by Addl. DGs or Commissioners and do not form a part of the functional hierarchy in the CBEC's IT Organisation.

CBEC in its replies admitted that till the course of audit, HPC, PMU and TEG were not functional in DoS. Further, CBEC has not provided a concordance or gap estimation of roles played by DoS officials and the outsourced service providers vide SLAs.

2.4 Training Policy

According to paragraph 6.2.2 of IT Security Procedures Ver.1.7, CBEC users shall be imparted training on Information Security on a periodic basis and refresher courses will be conducted to re-train the already trained employees on new threats and countermeasures.

As per DoS, Change Management and Network Management trainings were imparted to more than 19,000 users in 2010 and security awareness training for Third Party Vendors was conducted in June 2012. However, no documentation on the Network trainings were produced to audit, and except for Feedback forms of the Security awareness Training for Third Party personnel, no other details like number of personnel trained, course content, duration of training, names of vendors covered, etc. were furnished to audit. Audit observed that the department has not imparted any periodic training on Information Security to CBEC users after 2010, although it was required to do so according to paragraph 6.2.2 of its IT Security Procedures. Further, DoS stated that the department publishes a bi-annual Information Security Newsletter 'SURAKSHIT' on its website and gives a security tip of the day to its users on the CITRIX (ICES 1.5 browser platform) homepage. It was noticed that after the inaugural issue of 'SURAKSHIT' was published on the CBEC website in January 2013, there has been no subsequent issue of the newsletter till the date of audit.

Similarly, DG Inspection sought information on officials and officers who are trained to use ICES proficiently for CBEC's five year strategic plan on 1 Feb 2013. The RFD FY13 already covers this activity; however, the measurement and success indicators are not correlated with the policy decision already taken by the Government in case of use of ICT and ICES.

CBEC in its reply (January 2014) stated that:

1. Audit team was informed that documentation related to the LAN/WAN and change management trainings imparted to approx. 19,000 users was available with LAN-WAN project team and the same could be provided on request. Audit's contention that details regarding number of personnel trained, course content, duration of training, names of vendor covered under the third party Security Awareness Training were not furnished to the audit is factually incorrect. All these relevant details were shown to audit party during the course of their visit to the office.
2. Training material on Security Awareness as mandated by section 6.2.2 of CBEC's IT Security Procedure was made available to

NACEN, CBEC's training academy for meeting end user training needs.

3. CBEC has launched the inaugural issue of the newsletter – SURAKSHIT in January 2013. The second issue of the Newsletter was published in July 2013 and is also available on CBEC's website. The next issue is due to be published in Jan 2014.
4. The efficacy of ICES related training can be gauged from the fact that officers are working online on the ICES 1.5 application at an increasing number of locations (116 as on date) and increasing volume of documents being handled on EDI. In addition, day to day user management for role allocation and revocation is also handled by CBEC officers themselves as part of the application. Since the Customs cargo clearing process is an online process, the inability of Customs Officers to work on ICES would have impacted the clearance of cargo.

However, response on Audit's observation regarding lack of measurement and success indicators with respect to RFD 2012-13 has been sought from NACEN.

On being asked to furnish reports relating to number of personnel trained, course content, duration of training for the CBEC to audit and the level of officers of CBEC (Gr. A or B or C) trained in IT Security Awareness by NACEN, CBEC in its reply (February 2014) stated that users totalling 19,621 were trained which covered 108 Commissionerates of CBEC. It covered trainings regarding Change Management, LAN and WAN. The duration of the training was 2 days for Change Management and 1 day for WAN and LAN. In respect to hosting of SURAKSHIT in CBEC's website they clarified that the July issue of SURAKSHIT Newsletter was published as hard copies and circulated during the Chief Commissioners Conference held on 17th and 18th July 2013. As regard, the upload of softcopy, the newsletter was uploaded on the website on 8th October, 2013 after correction of the Hindi version by the publisher, which was received in the corrupted, non-readable form.

In response to CBEC's role in capacity building, training and updation in smooth functioning of the system, CBEC stated (February 2014) that while specialized trainings take place from time to time, the main thrust is on "on the Job" trainings, since ICES 1.5 is a dynamic application. The training material on ICES 1.5 has been shared with NACEN which organises regular training programmes for various levels/Grades of officers. Training on ICES 1.5 application is part of regular course curriculum at NACEN for IRS Probationers and other officers. NIC/NICSI personnel are posted at major

ICES locations who train officers as per requirement. Request based training at smaller locations are also carried out with the help of NIC and NICSI officers from nearby locations. Facility to provide hands-on training is available in ICES pre – production environment at all locations. Detailed instructions are issued as and when new patch/ functionality is implemented. Suitable advisories are also issued from time to time in respect of new functionalities to instruct and advise the officers and stakeholders regarding impact and handling of the proposed changes.

Regarding lack of measurement and success indicators with respect to RFD 2012-13, CBEC clarified (February 2014) that RFD 2012-13 required that Field Executive Officers be certified for IT skills in ACES & ICES. As per criteria value/target above 25 per cent of the strength was rated as excellent. NACEN certified 9490 out of total 26,330 executive officers achieved 'Excellent' assessment in terms of the Target Value prescribed in the RFD 2012-13. The efficacy of ICES related training can be gauged from the fact that officers are working online on the ICES 1.5 application at an increasing number of locations (116 as on date) and increasing volume of documents being handled on EDI. In addition, day to day user management for role allocation and revocation is also handled by CBEC officers themselves as part of the application.

The above may be presented for verification during future audits.

2.5 IS Security

ICT Systems of Custom's department have been awarded ISO 27001 Security Certification by Standardisation Testing and Quality Certification (STQC) from the Department of Information Technology (DIT) in July 2011 and Data Security Council of India (DSCI) Excellence Award 2012 for security in e-Governance. DoS has updated IS policies and procedures in accordance with the requirements for the ISO 27001 certification and IS security audit is carried out bi-annually by Third Party Auditors (TPA), M/s Price Waterhouse Coopers.

Audit observed that some features of operational password policy like password composition requirements, account lockout from unsuccessful login attempts, etc. were different from the documented password policy (paragraph 9.2.3 - User Password Management) of the Information Security Procedures V1.7. The operational password policy has different security features for ordinary users (business) and privileged users (administrators etc.), whereas the documented password policy does not provide for separate policies for different categories of users. Neither does it provide for relaxation of number of failed login attempts for ordinary users, as found to have been allowed in the operational policy. DoS stated that the Procedure document is presently under review and these changes are being incorporated in the annual revision. DoS reply confirms that changes regarding an issue having security implications have been implemented without corresponding provisions in the presently valid version of the documented procedures.

***Recommendation**: Any changes in the operational features of logical security elements like password policy may invariably be implemented only after due authorisation and documentation of the changes.*

CBEC in its reply (January 2014) stated that the decision for a phased implementation of the password policy in respect of ICES users was duly authorized and is recorded in the Quarterly Security Review Meetings. Audit was informed that the policy was implemented for other category of users.

CBEC further stated, as mentioned in CBEC's Security Procedure Document, the document is reviewed annually. However, it is the business call of CBEC to make these changes in a phased manner. Since indirect tax, especially Customs, has a dynamic work environment, it is not possible to change the documentation multiple times in a year. All changes follow the change management process and changes required in the documentation are incorporated in the relevant document during the annual review. It is also reiterated that the needs of business would dictate issues like implementing changes in the password policy even as they are subsequently incorporated in the procedure documents as part of the annual review.

At the time of audit, the audit team was informed that the relevant document was undergoing the annual review.

CBEC further stated (February 2014) that the Change Management document is for internal circulation within CBEC only and there are reservations in sharing the complete document. It is, however, available for inspection at CBEC premises. The Security Procedure document is a document for restricted circulation within CBEC only.

The reply is not acceptable because the audit was conducted in the CBEC premises but DoS did not produce the documents.

2.6 Internal control and audit

According to paragraph 6 and Annex 4 of Cabinet Note dated 26 November 2007, TPAs would be deployed for functional audit; accordingly, M/s PWC have been engaged for conducting half-yearly Information Security Audits and quarterly audits of IT Assets and Service Level Agreements (SLAs) entered into by various service providers/vendors. Audit observed that the Internal Audit and Corrective Action-Preventive Action Procedure Ver.1.2 does not have any provision for audit/review of any of the applications of the IT System, either by departmental officers or by TPAs. DoS stated that STQC has audited the ICES application and Oracle has conducted a code review of ICES. However, audit by STQC covers only the security aspects and a code review examines the correctness of programs. Neither STQC nor Oracle reviewed the adequacy of business processes covered and the correctness of business rules mapping, which have been found to be deficient in the ICES 1.5 application, as enumerated in succeeding paragraphs.

Audit is of the opinion that in an IS organisation a critical application like ICES with massive revenue implication requires a regular audit of the database, OS, infrastructure, application hardware for:

I. IT security audit

II. Malware analysis

III. Source code review

IV. Application configuration review

V. ICT infrastructure configuration review

VI. Application-OS-hardware-network performance reviews

VII. Vulnerability assessment and penetration testing (VAPT)

VIII. Analysis of system generated logs for application change management

IX. Web application security (WAS) assessment

X. Validation of the patches deployed and protocol functionality

XI. Analysis of SLA (Service Level Agreement) indicators and the tools to monitor and calculate the SLA indicators

XII. Review of technology deployed to ensure continuity of IT system

XIII. IT Act Compliance

XIV. National Cyber Security Policy compliance

In view of the extensive outsourcing of various projects and maintenance activities, the strategic control of Service Level Agreements review, source code review and performance audit of the IT infrastructure and application needs to be mandatorily with the Government. Accordingly, SLAs may be urgently reviewed.

Recommendation: *The department may consider examining its core application (ICES 1.5) audited periodically for detecting deficiencies and suggesting improvements in the application. The strategic control must necessarily be with the Government and accordingly, the SLAs may be urgently reviewed.*

The department accepted the recommendation and stated that the Department will examine the skill set required for such audits and assign the task to appropriate Directorate under CBEC. Terms of reference of each of the Directories are under review on account of Cadre Restructuring of CBEC and appropriate agency will be assigned the task in due course.

No action has been taken on the audit recommendation as yet, therefore, the assurance can only be seen in subsequent audit.

2.7 Deficiency in CRA module

(i) After the implementation of ICES 1.5, SSOIDs were issued to CRA officers to access ICES 1.5 from specified locations for auditing BEs and SBs. However, it is observed that while making a selection for SBs, only cancelled and purged SBs are getting selected for audit. This was brought to the notice of the department in May 2012 and February 2013, apart from eleven other inherent drawbacks of CRA module (Annexure B) through this report but has not been rectified.

(ii) Section 28 of the Customs Act 1962 was amended with effect from 8 April 2011 by Section 42 of Finance Act 2011, increasing the period for raising a demand in respect of imports from six months to one year from the date of clearance of goods. However, the corresponding changes have not been incorporated in CRA module available in the ICES system where it is possible to make a selection of auditable documents only for upto six months from the current date.

CBEC in its reply (January 2014) stated that for providing facility for accessing documents for the period of 1 year, very high processing infrastructure is required. Such retrieval is likely to impact the bandwidth and therefore DoS would examine the feasibility of such modification and resolve the issue.

CBEC was asked to provide the relevant report on configuration and memory management to audit. The same was not produced to audit.

(iii) Similarly, in the CRA module there is no system to go to and view any particular item in a BE containing more than one item except by viewing the details of each item in sequential order. For example, in a BE containing 100 items, to go to 100th item, one need to press 'Scroll/Enter' key 200 times.

CBEC in its reply (January 2014) stated that DoS is aware of this issue in the CRA module. CRA module is in line with the ICES application available during assessment to the assessing officer which requires application of mind on line by line basis. It is presumed that audit would the same. If further details are required by audit, it can be obtained through MIS reports available in the system. Therefore, no change is required in the existing process.

Reply of CBEC is not acceptable as audit only brought out the deficiencies of CRA module being an integral part of ICES; the main issue here is to comply with the audit requirements. Further, the inherent drawback in CRA module in ICES 1.5 had been stated in the paragraph number 2.7 (i). Moreover, the role of statutory auditor cannot be presumed as that of an assessing officer in terms of scope of audit as well as level of enquiry. Mandate of audit has been communicated to CBEC by audit in several fora including this report.

2.8 Monitoring of SSOIDs issued

DoS issues Single sign-on Identity (SSOID) to local users for accessing the EDI system on the basis of request received from the appointed nodal officer. After issue of SSOID, the System Manager/Commissionerate Administrator at the field formation level assigns roles/privileges required to perform any activity within the application and monitors SSOIDs activity.

Audit observed that the number of SSOIDs issued as on 31 March 2013 was not available with System Manager/Administrator at 10 of the 19 EDI locations where the Performance Audit was conducted, indicating that SSOIDs activity was not being monitored at these locations by the local system administrator. Further, Chennai Sea, Chennai Air, Tuticorin, Mumbai Zone II JNCH, Mumbai Zone III ACC (Import & General), New Delhi, ICD Tughlakabad, ACC New Delhi, ICD Mandideep, ICD Pithampur, Ahmedabad and Kolkata Port Commissionerates have stated that the System Manager is not required to submit any report on status of SSOIDs issued for the EDI location under the Commissionerate.

CBEC in its reply (January 2014) inviting reference to DG (System)'s letters dated 15 December 2008, 18 September 2014 and 23 February 2013 stated that a procedure for monthly review of all system users is implemented at EDI locations as changes are warranted on account of transfers, promotions and retirements. Contention of field offices that System Managers were not required to submit status reports on SSOID issued in their respective jurisdiction is not admitted.

Regarding the monitoring mechanism in the cases where field formations were not following the directions/instructions issued by the Board, CBEC in its reply (February 2014) stated that a central SI team monitors the SSOIDs issued to users. Every month, the central team proactively disables users retiring in that month on the basis of the date of birth of the user in the system. VPNID analysis for users is carried out to disable VPN Ids not used in the last six months. As a proactive measure, an electronic User Access Management (UAM) tool has been developed in-house and is currently under testing.

This would be verified in subsequent audit.

2.9 Inordinate delay in implementation of RMS export module

According to contract awarded by DoS to M/s Birlasoft Ltd. on 24 August 2004, and agreement signed on 20 July 2005, the vendor was to deliver, install and commission RMS Import, Export and Post Audit Modules within 115 days of award of contract. RMS import module was implemented at ACC, Sahar on 7 December 2005 and RMS export module at ICD Mulund and ICD Patparganj on 15 July 2013.

Thus, there was a delay of one year in implementing RMS import module and a delay of nearly nine years in introducing RMS export module.

On being pointed out, RMD, Mumbai stated (August 2013) that slippages were on account of justifiable reasons beyond the control of the vendor, such as, delay in finalisation of requirements, problems in data compilation, changes required in ICES application, etc. It has further stated that the requirements and codes for RMS export module were finalised after the implementation of RMS for import module and the export module was developed before April 2009 and was under testing at ICD Dadri. But it was not implemented as the IT consolidation project, involving migration to centralised environment, had started by then, which necessitated changes in RMS software for export as well as in the work-flow of ICES-export module.

According to the CBEC circular dated 24 June 2013, announcing the introduction of RMS for exports, it has decided to introduce RMS for exports in continuation of its ongoing Business Process Re-engineering initiative, of which introduction of RMS for imports was a part. It further states that by expediting the clearance of compliant export cargo, RMS for exports will contribute to reduction in dwell time, thereby achieving the desired objective of reducing the transaction cost and making business internationally competitive.

Thus, a Business Process Re-engineering initiative launched at the same time as RMS for imports, having obvious benefits accruing from its introduction, as claimed by the department itself, was delayed by nearly nine years due to tardy implementation arising from attaching less importance to this module and taking it up for development after implementing RMS import module.

No ‘time release study’ was conducted by the Board upto June 2013 to measure the efficacy and efficiency of the system to reduce the dwell time cargo clearance. Board informed that they have instituted a ‘time release study’ in June 2013 in different Customs jurisdiction and the finding by different Customs jurisdiction is awaited.

CBEC in its reply (January 2014) also stated that:

(i) RMS is essentially seen as a trade facilitation measure and not a tool to garner extra revenue, more particularly so in respect of RMS-Exports. RMS Imports was implemented in December, 2005 and RMS application was made ready by the vendor and taken up for testing in 2009. As regards delay in implementation of RMS-Exports, it is clarified that the delay was not due to less importance being given to exports over imports but due to various operational reasons. Initially, the Customs application was run on a distributive environment and RMS 2.7 was developed to run on the old Customs application (ICES 1.0). However, in late 2008, CBEC set up a centralised infrastructure (Data Centres etc) for running Customs, Central Excise & Service Tax, ICES and RMS applications from a centralised environment. Ideally, all the three Customs Applications namely ICES, ICEGATE and RMS should have been one single integrated application. But since these projects were taken up by CBEC over a period of time, work was awarded to different vendors, who developed separate applications. It is a challenging task to make all the three applications compatible with each other; changes in one necessitate changes/modifications in the other applications.

(ii) Meanwhile, there was an exponential growth in the number of documents on the export side and there was a need to augment the infrastructure to enable the implementation of Export RMS. Implementing RMS exports without the requisite infrastructure would have adversely affected the export clearance. The infrastructure was finally augmented during August, 2012; and after resolving the compatibility issues, carrying out further integration testing, and necessary changes in the application, and after issuance of Circular by CBEC in June, 2013, Export RMS was finally implemented on 15th July, 2013 and to avoid inconvenience to the trade, the national roll-out was planned in phases.

(iii) At present, Export RMS is implemented in 85 locations. It is scheduled to complete implementation of Export RMS in the remaining 4 locations, where RMS- Imports is also operational, by mid-February, 2014.

CBEC in their reply (February 2014) further stated that RMS is a tool to maintain an appropriate balance between trade facilitation and enforcement. Audit has commented that no report(s)/record(s) were produced to audit to indicate if there were indicators adopted by CBEC on trade facilitation and the achievement against the set indicators after rolling out of RMS (import/export). In this connection, it is clarified that trade facilitation is a very broad term and there are many intangible and non-measureable benefits that accrue to an importer/exporter. For example, a robust RMS facilitates implementation of trade facilitation schemes like Accredited Client Programme (ACP)/ Authorised Economic Operator (AEO) etc., which has a much higher facilitation level of about 90-92. Further, CBEC's circular dated 02 September 2011 prescribed the facilitation levels of 80 per cent for ACCs, 70 per cent for Sea Ports and 60 per cent for ICDs. Efforts have been made to move towards the ideal facilitation levels. However, since facilitation and enforcement have to be balanced, the current levels of facilitation in the import module in the year 2013-14 for Air cargo was 62 per cent, Sea 45 per cent and ICDs 42 per cent.

On the exports front, the facilitation level was about 50 per cent prior to the implementation of RMS Exports. After the roll out of RMS Exports, the current facilitation level is 78 per cent. It may, however, be noted that the level of facilitation depends on various factors including the compliance requirements from other stakeholders such as DGFT and port-wise pattern/degree/trend of compliance/non-compliance by the trade. So even if customs alone improves its functioning, still the facilitation level may not reach the desired level, if there is a new compliance requirement from some other agency.

Implementing RMS exports without the requisite infrastructure would have adversely affected the export clearance. Keeping our commitment to provide better services to the exporters, CBEC focused on augmenting infrastructure before rolling out RMS Exports. The infrastructure was finally augmented during August, 2012; and after resolving the compatibility issues; carrying out further integration testing, and necessary changes in the application, and after issuance of Circular dated 24.06.2013 by CBEC, export RMS was finally implemented on 15th July, 2013. To avoid inconvenience to the trade, the national roll-out was planned in phases. This only confirms that the interest of the exporter was paramount in CBEC's automation plan.

CBEC accepted that there was substantial delay in implementation of RMS Export module due to various operational reasons including migration to ICES 1.5 version. However, even after migration to ICES 1.5 in June 2010 it took three years for RMS exports to roll out gradually in phases. It was mentioned that ICES/RMS was essentially for trade facilitation. However, no report(s)/record(s) were produced to audit to indicate if there were indicators adopted by CBEC on trade facilitation and the achievement against the set indicators after rolling out of RMS (Import)/RMS (Export).

Department's claim that there was an exponential growth in number of documents in the export side, substantiates audit's contention that CBEC neither envisaged the trend of exports nor assigned adequate priority to the Exports.

2.10 Performance of Post Clearance Audit (PCA)

In order to implement self assessment effectively and to ensure its benefits to the trade, the Board decided that current facilitation level under RMS should be enhanced significantly. Accordingly, as per the Board's circular dated 02 September 2011, it was decided to enhance facilitation level up to 80, 70 and 60 per cent in case of air cargo complexes, ports and ICDs respectively, by rationalizing risk rules and risk parameters. According to Board circular dated 13 June 2012, higher facilitation at the same time has led to the need for more scrutiny of BEs at PCA/ PCCV[1] stage. It is therefore felt that the percentage of BEs selected for PCA needed to be enhanced by concerned field formations. Board therefore directed that till the time OSPCA[2] was made applicable to all categories of importers, the percentage of BEs selected for PCA at a Customs house should be suitably enhanced to safeguard the interest of revenue. Board also desired that concerned Chief Commissioners of Customs should review the staff position in their jurisdiction and reallocate more manpower for audit work as increased facilitation in terms of reduced examination had led to lesser requirement of staff for examination of goods. It was therefore imperative that excess staff should be diverted for activities such as PCA and SIIB[3] in Customs Houses.

Audit observed that in respect of RMS facilitation levels and PCA functioning at 19 EDI locations, the percentage of RMS facilitation in Chennai Sea, Tuticorin, Kochi Sea and Mumbai Zone II NCH ports were lower than the level directed in the circular whereas in case of Mumbai Zone I NCH, Goa, Nagpur, ICD, Tughlakabad, ICD Patparganj and Kolkata Port, the percentage of RMS facilitation was much higher than the level specified in the circular as detailed in Annexure K.

However, the figures of RMS facilitation of nearly 100 per cent as provided by Kolkata Port and Airport, Mumbai NCH, Goa, ICD Tughlakabad and ICD Patparganj appeared unrealistic and were therefore cross-checked from ICES 1.5 data pertaining to these EDI locations for the year 2012-13. It was found that the figures furnished were incorrect in comparison to the actual RMS facilitation levels, which varied from 35 to 64 per cent, all below the benchmark levels according to the Board's circular.

[1] Post-Clearance Compliance Verification

[2] On Site Post Compliance Audit

[3] Special Intelligence and Investigation Branch

Further, in NCH Mumbai Zone I, Pune, Goa, Chennai Sea Commissionerates, ICD Tughlakabad, Patparganj, New Delhi NCH, Kolkata Port and Airport, the percentage of RMS BEs selected for PCA has gone down, contrary to the instructions of Board's circular dated 13 June 2012 as shown in Annexure L.

It was also noticed that no PCA wing has been constituted at ICD Mandideep and ICD Pithampur leaving no scope of detection of incorrect assessments by the department at these customs locations.

From the information on submission of MIS reports on PCA functioning as furnished by the 19 EDI locations, it was observed that Chennai, Tuticorin, Kochi Sea Customs, ICD Tughlakabad, NCH New Delhi, Kolkata Port, Kolkata Airport and Ahmedabad were preparing and submitting such reports, to the Chief Commissioner and/or DG (Audit), but only Sea Customs (Chennai and Kochi) and Tuticorin Customs were forwarding the report to RMD, Mumbai. In RMS facilitated assessments, the only way to ascertain whether the RMS facilitations allowed were correct or not is to audit the BEs post clearance. The trend of detections of errors in assessment in RMS facilitated cases by the PCA wing at each EDI location can provide vital information on the effectiveness of RMS. In the absence of such reporting to RMD, Mumbai, it is felt that vital inputs for improving the RMS are not being taken into consideration by RMD.

Further, DG Inspection sought inputs for CBEC's five year strategic plan on 1 Feb 2013 so that a robust RMS covering all ports and transactions could be in place. The RFD FY13 does not cover this activity.

The compilation of information on PCA activity received from field offices, as shown in Annexure M, revealed that the Board's instructions to reallocate more man power for PCA to increase scrutiny of RMS cases has not been followed in any location and showed increasing trend in pendency of cases in 8 out of the 10 customs locations for which data has been received. Among these, 2.83 lakh cases were pending with the Custom House, Delhi and 3.72 lakh cases were pending with JNCH, Mumbai.

Further, scrutiny of the pending PCA bills at ACC Chennai and Tuticorin Commissionerates as on 31 March 2013 revealed that approximately 138 and 2,172 bills of entry respectively, had already become time-barred under Section 28 of the Customs Act 1962, thereby foreclosing the opportunity to raise demand even if incorrect assessments were detected. It was also noticed that there was no practice to queue the BEs considering 'Out of Charge' date as a parameter for selection of PCA BEs to minimise the risk of recoveries becoming time-barred due to high pendency, as found to be the case in the major customs ports.

CBEC in its reply (January 2014) stated that on All-India basis, the facilitation level of air cargo complexes was 70.39 percent during 2012-13. However, regarding observation on non-reporting of PCA functioning to RMD by 19 Customs locations, pendency of PCA work at 11 locations and non-rationalization of manpower by posting enough staff to PCA sections, CBEC stated that audit findings are being shared with respective Commissionerates for appropriate corrective action at their end. RMD has been interacting with field formations regarding PCA reports and taking cognizance of detections made by them.

CBEC, further, in its reply (February 2014) stated that during 2012-13, RMD has received PCA performance reports from 21 locations. As per the reports received, in 304 cases, recovery of ₹ 2.26 crore has been made. Based on the review of these reports, interdictions wherever necessary, were put in place in RMS to address the risks subsequently.

CBEC's response would be verified during next audit.

2.11 Ineffective Functioning of Local Risk Management (LRM)

The Risk Management System of ICES 1.5 has two components – National Risk Management (NRM) and Local Risk Management (LRM). While risk rules and targets at the National level are inserted and updated by RMD, Mumbai, the LRM Committees at custom sites are responsible for inserting and monitoring local risk factors through insertion of local targets. According to CBEC dated 28 June 2007, LRM Committee was to be constituted at each Custom House/ACC headed by an officer not below the rank of Commissioner of Customs. The Committee was to meet once in every month to discuss framing and review performance of RMS and to send periodic reports to RMD, Mumbai.

Audit observed poor functioning of LRM at almost all locations in discharging its function to monitor the performance of RMS and PCA. No LRM Committee has yet been constituted in Goa, ICD Patparganj, ICD Mandideep, ICD Pithampur and Kolkata Airport Commissionerates. In Chennai Air Commissionerate, the LRM Committee was constituted only in June 2013 after being pointed out by Audit. In ICD Tughlakabad, NCH Mumbai Zone-I, Nagpur, Nasik, Aurangabad, Ahmedabad Commissionerate, the LRM committee was formed three to five years after the issuance of the circular. The Commissionerates at Kolkata Port and Pune have no information regarding the LRM Committee meetings. Except for Kochi Commissionerate, LRM Committee meetings to review performance of RMS were being held infrequently at the remaining 10 of the 19 EDI locations where LRM functioning was examined in audit. Moreover, from the information furnished by RMD Mumbai, audit observed that Pune, Kolkata (Port), Kolkata (Airport), ICD Patparganj, ACC Chennai, etc. had been inserting substantial number of local LRM targets during the period 2010-2013 without having any constituted LRM committees which deliberates and authorises the insertion of local targets.

The department in their reply (January 2014) stated that presently RMS Import is functional at 88 ICES sites. The audit findings are being shared with the respective Commissioners of Customs for appropriate corrective action at their end. Regarding inserting local targets by Pune, Kolkata Port, Kolkata Airport, ICD Patparganj, ACC (Chennai) had been inserting local targets during 2010-13 without any review by the LRMC. DoS stated that LRMC is not a pre-requisite for insertion of targets/interventions to address local risks. The function of LRM is discharged by the Additional Commissioner (SIIB) who remains in constant touch with the trends in imports of various commodities and their valuation. He also deals on a day-to-day basis with any intelligence, feedback, violation of Customs or Allied Acts and any evasion of duty at the local level. LRM is required to take every possible action immediately including insertion of local targets in order to prevent any violation of law or evasion of duty.

CBEC, further, in its reply (February 2014) stated that as per paragraph 7 of the Board Circular dated 24 November 2005, “there will be a local Risk Management System catering to the needs of the Customs Houses. The local Risk Management System will carry out the live processing of the BEs and IGMs etc. The Commissioners of Customs are required to appoint the administrator for the ‘Local Risk Management System’ at the level of the Joint/Additional Commissioner for assigning user privileges on the Local Risk Management System. Local processing of BEs in RMS is based on the interdictions inserted at local level.”

Reply of CBEC is not acceptable because Board’s circular dated 28 June 2007 stipulates that a LRM Committee was to be constituted at each Custom House/ACC headed by an officer not below the rank of Commissioner of Customs. Accordingly, insertion of local targets by officers without constituting LRM committee is in contravention of Board circular dated 28 June 2007. No records/instruction issued by Board/DoS authorizing LRMs to insert local targets without review of LMRC was produced to audit.