Chapter II: IT Governance and IT Security

Audit examined and sought assurance on the overall IT Governance and IT Security of the CBIC ACES-GST Application. Audit focus was on the acquisition process, role and working of Boards/Committees, Service Level Agreements, Change Management Process and IS Security.

Scrutiny of the records revealed that a total of 12 prospective bidders purchased the RFP, but only a single bidder participated in the bid. Certain gaps were noticed during the scrutiny of SRS of different modules vis-à-vis the provisions given in the Act/Rules.

The Exit management plan and Helpdesk operation plan were obtained from the vendor with a delay. There was levy of liquidated damages for non-achievement of SLAs.

2.1 Inception of CBIC ACES-GST Application

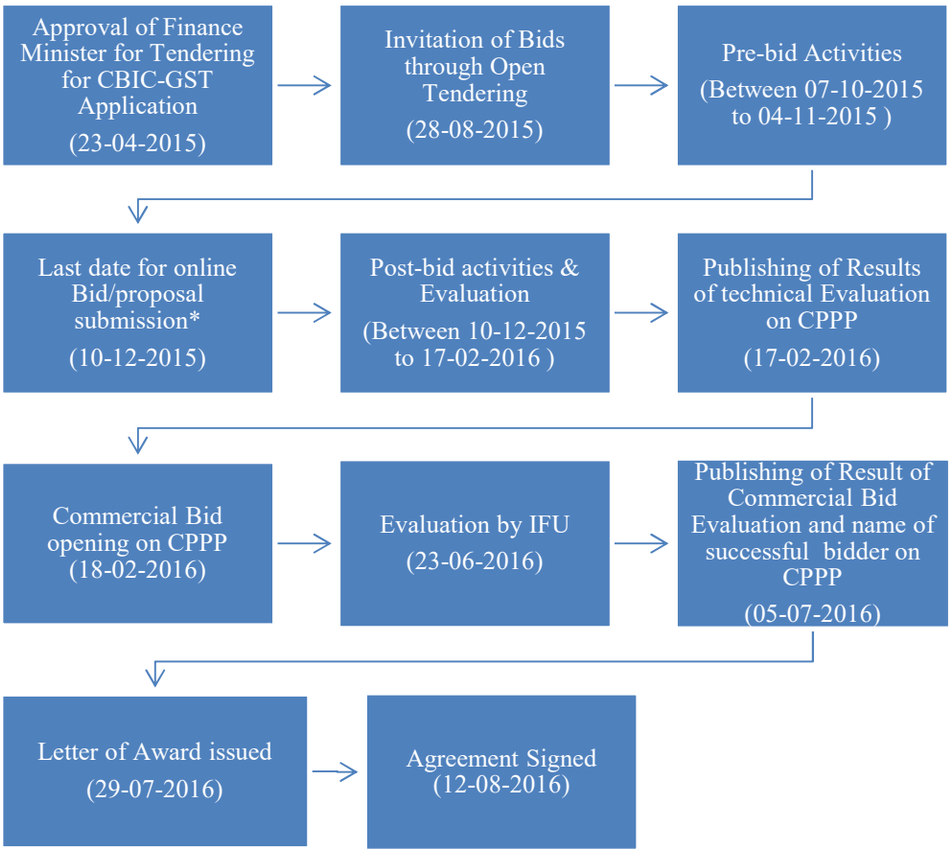
The Central Board of Indirect taxes and Customs (CBIC), Department of Revenue deals with the tasks of formulation of policy concerning levy and collection of Goods and Service Tax. The Directorate General of Systems and Data Management (DG (Systems)) has been entrusted with the implementation of the projects relating to Information and Communication Technology (ICT) in CBIC.

Since at the time of envisaging and roll out of the CBIC ACES-GST Application, GST laws had not yet been enacted and the details of the business processes to be followed in the GST was not completely worked out, the RFP floated vide RFP No. IV (39)/4/RFP GST 01/2015 for "Appointment of Vendor for Development and Maintenance of CBIC's Indirect Tax Applications (GST and ACES) and provision of Training and Helpdesk Services" provided a broad scope of the business processes that were likely to be followed in the GST regime.

Taxation being a dynamic concept, it was understood that the business processes may undergo changes from time to time and need to be automated at the shortest possible time periods, by the Centre, the States and GSTN. This would require regular, timely and effective interaction with all the stakeholders and periodic modifications in the system, applications, additions of new functionalities and servicing new requirements that ensured a smooth transition to the new tax regime.

2.2 Acquisition & Procurement

Chronology Chart - Timelines for Acquisition & Procurement of Vendor



*The last date for submission of bid was extended to 28.10.2015, 18.11.2015, 26.11.2015 and 10.12.2015.

The erstwhile CBEC (current CBIC) had initiated a GST Pilot in 2011 and GSTN was formed in 2014. In April 2015, as part of deliberations on preparedness for GST, the Department proposed development of an application, separate from the GST portal that would serve as the back-office solution for CBEC departmental users to process the registration, return and payment data captured by the GSTN portal. The planned timeline by the Department for development of the application & roll-out was from 10th August 2015 - 1st April 2016 and for maintenance between 1st April 2016 and 31st March 2021 for a period of five years. The proposal 'Preparedness for GST 01.04.2016' for the development of this application was put up by CBEC to the Ministry of Finance on 10.04.2015.

The proposal mentioned that PMU (M/s PwC) had prepared a Detailed Project Report and conducted a gap analysis based on a comparison of the 'As-Is' capacity of CBEC's existing IT infrastructure and the "To Be" state of the infrastructure, required to be in place by 2016. PMU had prepared a

cost estimate for the project ranging between ₹ 163.58 crore and ₹ 202.44 crore.

On 23 April 2015, the Finance Minister approved the proposal to initiate tendering for the development of applications of GST.

In August 2015, Directorate General of Systems (DG (Systems)) invited an open tender through RFP for selection of Implementation Agency for development and maintenance of CBIC's Indirect Tax Application (GST and ACES) and provision of Training and Helpdesk Services. The Vendor was to be selected under Cost-Based Selection.

A total of 12 prospective bidders had purchased the RFP. In September and October 2015, pre-bidding workshops were organized to address the queries of the prospective bidders. On requests of prospective bidders, the bid submission date was extended in four steps by 71 days i.e., from 30 September to 10 December 2015 by the Department. However, by the due date, only a single bid from M/s Wipro Ltd. was received even when 12 prospective bidders had purchased the RFP and the date of submission of bid was extended on the request of the prospective bidders. Tender opening process began on 23 December 2015.

Preliminary evaluation of the bid was conducted and Cover 1 (Integrity Pact, Authorization Letter and EMD) and Cover 2 (Pre-qualification Bid) were scrutinized during the evaluation process.

Technical bid was evaluated in January 2016 and February 2016 by the Technical Evaluation Group (TEG) with assistance from PMU (GST) and DG Systems officials. M/s Wipro Ltd. qualified this stage with a score of 80.6 against the cut-off marks of 70 for this stage as detailed below.

Table 2.1 - Preliminary evaluation of the bid

Sl No.	Evaluation criteria	Total Marks	Minimum cut-off (60%)	Marks obtained	Qualification status
1.	Bidder's Credentials	15	>=9	15	Qualified
2.	Approach & Methodology	10	>=6	7.6	Qualified
3.	Solution Architecture	23	>=14	16.1	Qualified
4.	Key Resources	40	>=24	32.9	Qualified
5.	Presentation & Demonstration	12	>=7	9	Qualified
Total		**100**	**70 (70%)**	**80.6**	**Qualified**

After qualifying the technical bid stage, the Commercial bid was evaluated by two separate Price Evaluation Committees (PEC) constituted (March 2016) to evaluate the reasonableness of the price quoted by the bidder.

Both the committees found that the overall price quoted by the bidder in the original bid (₹ 190.17 crore) was quite close to the mean value (₹ 183.01 crore) of the cost range estimated (₹ 163.58 crore to ₹ 202.44 crore) by PGMA[4] (earlier known as PMU[5]). However, the bidder suo-moto offered to reduce the bid amount to ₹ 184.00 crore plus taxes.

DG (Systems) sent the original as well as revised commercial bid to IFU[6] on 23 June 2016 for approval. Revenue Secretary during the appraisal meeting (24 June 2016) of the Standing Finance Committee (SFC), Department of Revenue, suggested to get the reasonableness of price evaluated by an independent Price Evaluation Committee (PEC) comprising of officers from NIC, CBDT, DeitY and IFU. The independent PEC submitted its report to DG (Systems) on 05 July 2016 and recommended the price of ₹ 184 crore quoted by M/s. Wipro Ltd. as reasonable. Administrative approval and financial sanction were received on 01 August 2016 from Finance Minister. DG (Systems) issued the Letter of Award to M/s Wipro on 29 July 2016 and the Master Service Agreement was signed between DG (Systems) and Vendor on 12 August 2016.

Audit noted that M/s Wipro Ltd. who was awarded this contract, was the developer and maintainer of the ACES legacy system and would have better familiarity with tax administration workflow vis-a-vis the other 11 prospective bidders. The single bid contract of ₹ 184 crore was awarded to M/s Wipro Ltd., with the CBIC's notings citing the validity of the due process followed and reasonableness of awarded value being mean value of the estimated price range, and also that retendering may not leave sufficient time to develop the necessary GST application and to take over the ACES system on the expiry of the existing contract.

On this being pointed out by Audit (April 2022), the Ministry accepted (August 2022) the observation.

Recommendation 1: In future, the Department should ensure adequate competition and minimize vendor lock-in by ensuring that more bidders participate in the bid for tendering for the next contract. This may be done by devising appropriate procedures to ensure a more level playing field between the prospective bidders and the existing System Integrator (SI). Also, this tender may be initiated well in time so that in the event of receipt of only one bid, the Department has sufficient time to retender, if felt necessary.

[4] Programme Governance and Monitoring Agency; PwC Pvt Ltd.
[5] Programme Management Unit
[6] Integrated Financial Unit

2.3 Technical requirements of the CBIC ACES-GST Application

The Vendor was expected to design, develop and deploy the application in line with the high-level solution architecture and be able to deliver all the functionalities, technical and operational features as mentioned in the RFP, meeting the desired service levels. The application was envisaged to be highly decoupled, modular, scalable and integrated software application, deployed centrally at the Data Centre (DC) and Disaster Recovery Site of CBEC (now CBIC), having the necessary interfaces for all the stakeholders through appropriate channels.

Application would be web-based and would integrate to a backend database with logical partitioning for effective data retrieval and storage. It was also proposed that the entire application should have flexible and scalable architecture with a well defined 'Business Logic layer' and 'Data Access Layer' to support the efficient handling of data and business logic between the 'Application Layer' and the 'Database Layer'. The application would be supported by an 'Enterprise Service Bus', which would enable effective data exchange and interaction between various interfacing bodies.

Given that the business requirements may remain fluid over the period of time, owing to the dynamic nature of the GST regulations, the functionalities and features of CBIC ACES-GST System were envisaged to be granular and modular enough for the administrators to enable or disable any particular functionality, at any given time, as per the requirement, without the need for a developer / code level change / custom UI change. While the key modules had been specified, it was a necessary requirement that the application should enable complete integration between different modules to enable building of workflows which may leverage information across the modules.

2.4 Scope of work for Vendor

The scope of work was to be carried out in multiple tracks:

Track 1: Takeover and operations and maintenance of ACES

Track 2: Design, development and implementation of CBIC ACES-GST System

Track 3: Operations and maintenance of CBIC ACES-GST System

Track 4: Training of CBIC officials

Track 5: Helpdesk operations

2.5 IT Governance and Management

IT governance enables organizations to manage their IT risks effectively and ensure that it meets the needs of the business today and that it incorporates plans for future needs and growth. It is an integral part of enterprise governance and includes the organisational leadership, institutional structures and processes, and other mechanisms (reporting & feedback, enforcement, resources etc.) that ensure that IT systems sustain organisational goals and strategy while balancing risks and effectively managing resources.

Table 2.2 - Summarised Audit Finding Matrix

Sl. No.	Sub-Objective	Summary of Audit Checks	Status	Findings
1	How does the organization identify and approve or reject new/old business requirements?	Project management office	Minimal record production	2.5.1 2.5.3
2	How does the leadership direct and monitor the performance of project?	Steering Committee, Fortnightly and monthly meetings, variations in cost, schedule and performance indicator from as planned, proper approvals, project milestones	Minimal record production	2.5.2 2.5.4 2.5.4.1 2.5.4.2 2.5.4.3 2.5.5
3	How does the CBIC monitor and manage their risks?	Incident Management Team, Vulnerable areas, Performance Testing, Risk Management Plan, Risk mitigated, Root Cause Analysis (RCA)	Scope restriction	-

To direct and monitor the performance of project, the RFP envisaged creation of a Project Management Office and a Steering Committee as detailed below:

2.5.1 Project Management Office (PMO)

A Project Management office with a designated full time Project Manager from the Vendor and key persons from other relevant stakeholders including officials from the Purchaser and other representatives by invitation, was to be set up during the start of the project.

PMO was required to maintain weekly statuses, minutes of the meetings, weekly/monthly/project plans, etc. PMO was also to meet formally on a weekly basis covering, at a minimum, the following agenda items:

- Project Progress
- Issues and concerns
- Unresolved and escalated issues
- Change Management - Proposed changes, if any
- Any other issues that either party wished to add to the agenda.

Audit had requisitioned (July 2021) the documents related to setting up of project management office (PMO); however, the same were not provided. Based on the available documents provided by the Department, Audit could not find any mention of setting up of a Project Management Office which was to include a designated full time Project Manager from the Vendor and key persons from other relevant stakeholders including officials from the Purchaser and other representatives by invitation.

2.5.2 Steering Committee

The Steering Committee, envisaged as a forum for seeking and getting approval for project decisions on major changes was to consist of senior stakeholders from the Purchaser, its nominated agencies, consultants for the Purchaser and the Vendor. The Vendor had to participate in Steering Committee meetings and update the Steering Committee on Project progress, Risk parameters (if any), Resource deployment and plan, immediate tasks, and any obstacles in the project. During the development and implementation phase of the project, fortnightly Steering Committee meetings were to be held. During the operations and maintenance phase, the meetings were to be held at least once a month.

Audit noted that the Steering Committee was constituted but its composition and details of its functioning were not provided to Audit to assess whether this committee functioned as envisaged in RFP.

In this regard, audit observation was issued (April 2022) and the Ministry during the exit conference while noting the audit recommendation for compliance stated (September 2022) that all available office records were furnished before the audit team. PMO is functional and weekly/periodic review meetings are continuing since inception of project and also stated to share the same with audit again; however, the same was awaited (December 2022).

Recommendation 2: The Department should ensure that the PMO and steering committee are functioning as envisaged, to monitor the progress of implementation of the project.

2.5.3 Gaps in Software Requirement Specifications (SRS)

The SRS were prepared for all modules, which formed the basis for development of the modules. Audit test checked the SRS of all the modules vis-à-vis the Act/Rules to evaluate whether all the provisions were considered while preparing the SRS. Audit found that most of the provisions have been addressed in the SRS, subject to the following gaps.

Table 2.3 - Module wise details of gaps in SRS

Name of the module	Validation provisions not included in SRS	Reference
Investigation	Validating the condition of returning documents/books or things seized by authorized officer within thirty days after the issue of notice	Section 67(3) of CGST Act
	Capturing the details of release of goods if No notice is issued pursuant to search	Section 67(7) of CGST Act
	Ensuring time limits and extension of time limits for release of goods as mentioned in the Act	Section 67(7) of CGST Act
Registration	Absence of Validation to compute Aggregate Turnover from the Returns filed	Section 10 of the CGST Act, 2017 read with Notification No. 14/2019-Central Tax dated: 07.03.2019
	Absence of provision in the SRS to alert the tax officer when all pending Returns have been filed by the taxpayer and full payments made within the prescribed period instead of replying to the SCN for non-filing of Returns.	Rule 22(1), Proviso to Rule 22(4) of the CGST Rules, 2017 .
	Absence of provision in the SRS to ensure that deemed approved registrations are duly signed or verified through electronic verification code.	Rule 10(5) read with Rule 9(5) of the CGST Rules, 2017.
	Absence of validation to ascertain the effective date of liability in respect of registrations obtained as a result of transfer, succession, demerger, amalgamation.	Section 22(3), 22(4) of the CGST Act, 2017.
	Absence of Suspension functionality and validation to restrict the registered taxpayers from making taxable supplies and consequent passing of credit.	Rule 21(A)(I) of the CGST Rules, 2017 .

Considering that these requirements are laid down in law, there needed to be a validation process built in the system to ensure compliance with the provisions of law.

Recommendation 3: The Department should conduct a review to ensure that all the provisions laid down in Act/Rules/notifications, including the changes introduced at different times are accurately mapped and updated in the SRS for development of functionalities.

On this being pointed out by Audit (September 2021), the Ministry accepted the recommendation and stated (August 2022) that the suggested functionalities in both the modules will be developed.

2.5.4 Project Milestones

As per RFP (Clause 9.1), project milestones were to be measured from the Project Start date (referred to as "T"[7]).

During audit, to assess whether the project was developed and implemented as per the agreed plan and timelines, CBIC was asked to indicate the planned date and actual date for development and implementation of each module. In response, the Department provided the information in respect of Registration, Returns, ACL, ACES GST Migration, Refund modules. For the remaining modules, the Department stated that the DSR (Adjudication, Recovery and Appeal), Investigation Modules were implemented through Change requests. Mobile App and Audit Modules were in the SRS signoff stage as discussed in subsequent paras. Further, Taxpayer at Glance (TAG) and Export Modules were at discussion stage.

2.5.4.1 Development and utilisation of modules

The status of modules of CBIC ACES-GST Application after five years (September 2021) of the agreement was as under:

Table 2.4 - Status of development of modules

Name of the module	Functionalities implemented	Functionalities yet to be implemented
Registration	• View Taxpayers' registration forms and supporting documents	• Associated Risk (based on the no of cases registered against the PAN Holder)

[7] Defined as the date of receipt of the Letter of Acceptance of Award or Seven (7) days after issuance of the Letter of Award by CBIC.

Name of the module	Functionalities implemented	Functionalities yet to be implemented
	• Approve/Query/Reject Registrations for more information • Amendment of Registrations • Surrender of Registration • Cancellation of Registrations • Revoke Registration • Aadhaar linking and Physical Verification • Jurisdiction allocation logic (TCS and UIN)	• Suspension functionality • Composition Forms and composition Validations
Returns	• View All Forms with Downloadable option • Transitional Provisions - functionality for Non Filers (Partially deployed)	• Best Judgement Assessment • Scrutiny of Returns • Summary Assessment for forms relating to ASMT 01 TO ASMT 18 • GSTR - 4 Annual Return • ITC-02A
Payment	• Payment Receipt • Acknowledgement generation (PMT- 01) • View Ledgers (ITC and Liability Registers) - Sync with GSTN	• Transmission of reconciled data from Accounting Authorities • Verification of payment details • Synchronization report • Integration of data with other modules
ACES Migration	Not Applicable	
Export	Export module was in discussion stage and was yet to be developed. The module was in the draft SRS stage.	
Tax Payer At Glance	Discussion stage only. Draft SRS was awaited from the Vendor	
Refund	• Refund Application • Acknowledgement • Deficiency Memo • Provisional Refund Order • Payment Order • Refund Sanction Order • Complete and Partial Adjustment of Liability	• RFD-10 Application for refund of UIN • RFD-7 (Part-B) Order for withhold and release of Refund • RFD-01C Correction of mistake done in RFD-01B • Payment to CWF • RFD 10A CSD • RFD10B Duty Free Shop

Name of the module	Functionalities implemented	Functionalities yet to be implemented
	• Notice for Rejection (SCN) • Reply of SCN view option • LUT (Letter of Undertaking)	
Investigation	• Phase I completed- all investigation activities	• Post investigation activities of Phase I • Phase II - Prosecution, compounding, interception of goods in transit
Adjudication	• Phase I- Issue of Show Cause Notices (SCNs) - for Refund and Anti-evasion, Adjudication processes • Issue of OIO (Forms DRC 01 and 3 to 8) • Process of fixing personal hearing and transfer of cases to/from call book	• DRC[8] -02 • Issue of SCNs • Summary assessment • Scrutiny of returns • Audit and Special Audit
Appeal, Review and Revision	• Phase I functionalities (Forms APL[9] 1 to 4) and • Review of Adjudication orders	• Phase II functionalities - 21 use cases • Remand orders (Forms APL 5 to 8, RVN 01)
Recovery	• Recovery of legacy arrears • Payment in instalments (Forms DRC 7A,8A, 20,21)	• Recovery process emanating from other sources (DRC Forms 9 to 19, 22 to 25) and • Recovery Register
E-Way Bill- Unblocking	• Fully implemented	• Nil
Audit	• SRS signed-Off	• Development of the entire module
Mobile Application	• SRS - Phase I signed Off	• SRS - Phase II and development of entire mobile application

Apart from the unblocking functionality of E-Way Bill, which was fully developed, the modules for Registration, Payment, Refund, Investigation, Adjudication, Appeal, Review and Revision processes were substantially completed and were independently functional, though some functionalities were yet to be developed. The Recovery module was only partially completed. The critical recovery register was not yet developed and the current stage of development covered only two segments of the

[8] Demand and Recovery forms
[9] Appeal forms

underlying workflow processes. The development of Export, Taxpayer at a glance and Mobile application modules were at a nascent stage.

Against this backdrop, our review of the utilisation of the modules by field formations suggested that the functional portion of the modules for adjudication, investigation, appeal were being used only to a very limited extent.

(i) As regards the adjudication module, the MIS reports for 2020-21 for Bengaluru zone indicated that while payment against SCNs was made from the GST front-end and Form DRC-03 (Intimation of payment made by taxpayer) were filed in 29,527 cases during 2020-21, no case was processed through the system. The MIS reports indicated that DRC-05 (intimation of conclusion of proceedings) or DRC-07 (Summary of orders) had not been issued for any case. Where taxpayers had made voluntarily payment using DRC-03, acknowledgement of acceptance of payment was issued in Form DRC-04 only in 53 cases. Similarly, on a pan India basis, a report for one month (July 2021) indicated that only 44 cases have been processed through the system by issuing DRC-07 and only 3,029 cases had been cumulatively processed so far.

(ii) The investigation module also was not being utilised. A visit to one Commissionerate (Bengaluru East) indicated that no cases had been processed through the system. The register for investigation cases (335J) was maintained manually. A review indicated that cases were being primarily processed through e-Office.

(iii) In the absence of the Appeal Register (which was yet to be developed), the extent of usage of Appeal module could not be assessed. Audit observed from Bengaluru-I Appeal Commissionerate that there were no cases in the appeal archive list of two ranges.

In response to the audit observation (September 2021), the Department replied (December 2021) that various outreach measures were initiated, which included various communications being sent to CBIC officers, online training and familiarisation programs, organising workshop at the Commissioner level and instructions that using e-office was not a replacement to the CBIS GST application. It also stated that outreach and awareness programs were conducted not only on a regular basis but also on a need basis. However, the issue of lack of usage was being pursued vigorously.

2.5.4.2 Delay in development of Mobile Application module

As per the MSA, Vendor had to develop a hybrid Mobile Application for Android, iOS and Windows platforms, to be accessible on Tablets and smartphones as part of Phase-I development of the CBIC ACES-GST application. It was to be designed to be platform independent and to work on both Online and Offline modes. The Mobile Application was to be extended to the Officers on field/site visits for creating and uploading their reports online on completion of physical verification etc., in addition to specific reports on revenue collected, returns filed, etc. All the 14 MIS Reports as available in the Web Application were to be considered for Mobile Application development.

The indicative timeline as envisaged in the MSA for deployment of the Mobile App in production was 31 May 2017. However, there was no progress on development of Mobile App until January 2019, when a Working Group consisting of 13 officers from CBIC was constituted to deliberate upon and to finalise the Business Requirements. Initially, the mobile devices were intended to be provisioned by CBIC for all their 24,612 officers but later, based on the hardware and software requirement discussions during March/April 2019, it was decided during May 2019, to adopt the Bring Your Own Device (BYOD) concept.

The vendor committed (11 September 2019) to delivery of Mobile Application in two phases with the revised SRS Sign-Off date for Phase-I as 30 September 2019 and Go-live as 30 November 2019. Phase-I was envisaged to cover MIS Reports as well as some modules and functionalities while the remaining was envisaged for Phase-II. However, after iterations, the vendor shared (14 January 2020) the SRS Version 2.0 without the Field Site Visit (FSV) dashboards and prototypes, which were to be submitted and vetted separately. CBIC partially signed-off SRS Version 2.0 on 16 January 2020 without UI Screens (pending technical feasibility report of developing the MIS reports in Mobile application by M/s Wipro Ltd) and accorded final approval (February 2021) for SRS - Phase-I with all the Reports and the UI screens.

As regards Phase-II of the Mobile Application, based on Working Group meetings and suggestions (June - July 2020) the Business Requirements Document (BRD) was finalised in December 2020 and there has been no further progress beyond the BRD finalisation. CBIC reviewed (November - December 2020) the progress status of the two Phases of Mobile Application and based on the bottlenecks identified, decided to put on hold further development until the Vendor deploys additional development resources and reverts on technical feasibility of developing

MIS reports (with reference to volume of data, graphical representation and hyperlinks).

Therefore, from a functional perspective, with substantial amount of time and effort expended, only the SRS for development of first phase of Mobile Application had been signed-off and initial screens were still being demonstrated. The development of the Mobile Application envisaged as phase I of the CBIC-GST application had already suffered a time over run of more than three years. Additionally, development of the Mobile Application in the manner envisaged seems unlikely, given that further development was on hold as technical feasibility of MIS functionalities was yet to be established and Vendor was unable to provide technical resources.

On this being pointed out (September 2021), the Ministry, while accepting the para, stated (August 2022) that all efforts were being made to accelerate the development and deployment of the mobile application.

2.5.4.3 Delay in development of Audit module

As per the MSA, the vendor had to roll out an Audit Module for usage by Audit formations of CBIC by May 2017. Processes significant for Audit module were identified, important among them being annual selection of units for audit, creation of Audit Planning Register, quarterly audit schedule and allocation, preliminary/desk review, data analysis, evaluation of internal controls, verification report, post verification and preparation of draft audit and final audit report. DG (Systems) identified that there was significant difficulty in converting business processes into system design and implementation due to technical/system limitation. The preparation of SRS commenced in May 2017 and underwent multiple revisions. The Department undertook extensive deliberations with Vendor for determining the scope of audit module and gaps in the SRS with reference to the RFP.

Finally, DG (Systems) signed-off the Audit SRS in January 2020. However, the vendor stated that the following functionalities included in the signed off SRS, were not covered in the RFP and would be considered 'out of scope', i) Issue ADT-03 ii) Issue ADT-04 iii) Audit Register iv) Broadcast (bulletin board) v) Desk Review analytics. After deliberations, it was agreed that except for Broadcast (bulletin board), all other issues were part of scope.

Thus, delay in defining and agreeing upon the scope of Audit module, delay in finalization of audit forms/processes for inclusion in SRS coupled

with the delay in finalization of the GST Audit Manual (that came into existence in July 2019) contributed, largely, to the delay in the SRS signoff.

In response to the audit observation (September 2021), Ministry, while accepting the para, stated (August 2022) that the Audit Module had been rolled out on 1st April 2022.

The implementation of the Module will be reviewed in subsequent Audits.

Recommendation 4: The Department should strengthen the IT Governance and Management mechanism to ensure that the project timelines are adhered to and rolled out modules are effectively used as envisaged.

2.5.5 Payment Schedule

RFP (Clause 9.2) defined the milestone wise payment schedule for payment of Application Development Cost, Payment of Operation & Maintenance Cost & Helpdesk Cost, and payment of Enhancement Cost & Training Cost. Payment for each activity was to be made as a percentage of total cost when the defined milestones for the afore-mentioned activities was reached. Based on the documents provided to Audit, the payments made against the different payment milestones for development of different modules, as summarised by Audit, is given below:

Table 2.5- Details of payments made against each payment milestone

(Amount in ₹lakh)

Sl. No.	Payment Milestones	Billed Amount (A)	Descoped Amount (B)	Claimed Amount (C)	Amount Pending (D)	Liquidated Damages (E)	Actual Payment {F=A-(B+C+D+E)}
Registration Module							
1.	SRS Signoff (10%)	34.22	0	0	0	0	34.22
2.	UAT Deployment (20%)	68.44	0	0	0	0	68.44
3.	UAT Signoff (50%)	171.10	6.84	3.42	0	4.43	156.41
4.	Production Deployment (10%)	34.22	1.36	0	0	0.06	32.8
5.	Go-Live (10%)	34.22	1.36	0	0	0	32.86
	Total	**342.2**	**9.56**	**3.42**	**0**	**4.49**	**324.73**

Sl. No.	Payment Milestones	Billed Amount (A)	Descoped Amount (B)	Claimed Amount (C)	Amount Pending (D)	Liquidated Damages (E)	Actual Payment {F=A-(B+C+D+E)}
Returns Module							
1.	SRS Signoff (10%)	68.44	20.53	0	0	0	47.91
2.	UAT Deployment (20%)	136.88	83.95	0	2.96	0	49.97
3.	UAT Signoff (50%)	342.21	209.89	0	24.52	1.38	106.42
4.	Production Deployment (10%)	68.44	41.97	0	5.58	0.006	20.88
5.	Go-Live (10%)	68.44	41.97	0	4.90	0	21.57
	Total	**684.41**	**398.31**	**0**	**37.96**	**1.38**	**246.75**
Refund Module							
1.	SRS Signoff (10%)	17.11	0	0	0	0	17.11
2.	UAT Deployment (20%)	34.22	1.71	0	1.71	3.42	27.38
3.	UAT Signoff (50%)	85.55	11.40	0	10.83	0.83	62.49
4.	Production Deployment (10%)	17.11	2.21	0	2.23	0	12.67
5.	Go-Live (10%)	17.11	1.82	0	3.39	0	11.9
	Total	**171.10**	**17.14**	**0**	**18.16**	**4.25**	**131.55**
ACL Module							
1.	SRS Signoff (10%)	34.22	0	0	0	0	34.22
2.	UAT Deployment (20%)	68.44	0	0	0	0	68.44

Sl. No.	Payment Milestones	Billed Amount (A)	Descoped Amount (B)	Claimed Amount (C)	Amount Pending (D)	Liquidated Damages (E)	Actual Payment {F=A-(B+C+D+E)}
3.	UAT Signoff (50%)	171.10	0	0	0	9.41	161.69
4.	Production Deployment (10%)	34.22	0	0	0	0	34.22
5.	Go-Live (10%)	34.22	0	0	0	0	34.22
	Total	**342.20**	**0**	**0**	**0**	**9.41**	**332.79**
ACES GST Migration Module							
1.	SRS Signoff (10%)	34.22	0	0	0	1.67	32.55
2.	UAT Deployment (20%)	68.44	0	0	0	0.19	68.25
3.	UAT Signoff (50%)	171.10	0	0	8.55	0.98	161.57
4.	Production Deployment (10%)	34.22	0	0	1.71	0.11	32.4
5.	Go-Live (10%)	34.22	0	0	13.68	0	20.54
	Total	**342.20**	**0**	**0**	**23.94**	**2.95**	**315.31**

Source: Data provided by Department (as of March 2022)

The remaining modules were developed either through change requests or were at planning/SRS stages.

The total amount paid to the vendor (against original contract amount) till date has not been made available to Audit. During the Exit conference (September 2022), the Ministry stated that Project Budget files for consolidated expenditure and budget thereof were provided to the audit team at DG (Systems) Delhi and also stated that they would share the same with Audit again; however, the same was awaited (December 2022).

2.6 Exit Management Plan (EMP)

Table 2.6 - Summarised Audit Finding Matrix

Sl. No.	Sub-Objective	Summary of Audit Checks	Status	Findings
1.	Whether exit management policy/plan is established in accordance with the RFP	Exit management plan within 90 days from the effective date of the agreement. Re-drafted the Exit Management Plan every six (6) months and kept up to date.	Checked	2.6.1

2.6.1 Exit Management plan not submitted by the Vendor

As per RFP, the vendor was required to submit an Exit Management plan in writing to the Purchaser or its nominated agencies within 90 days from the effective date of the Agreement in relation to the various phases of the Project. The Exit Management plan needed to be re-drafted every six months to keep it up to date. Each version of the Exit Management plan was to be approved by the Purchaser or its nominated agencies. As per RFP, in case of the Agreement being terminated, the Purchaser reserved the right to ask the Vendor to continue running the project operations for a period of 6 months after termination orders were issued and the Vendor should be obliged to provide such services for such period without any additional cost and expense to the Purchaser and without any impediment in the quality of services.

During audit, it was noticed that the Vendor did not submit any Exit Management plan which was also confirmed by the DG (Systems). In absence of an Exit Management plan, there was no assurance that the outgoing vendor would co-operate smoothly for effective continuity of the business. DG (Systems) did not provide reasons for non-submission of Exit Management plan by the Vendor and did not take any action for non-fulfilling of necessary obligations of the agreement.

When pointed out by Audit (April 2022), Ministry accepted the observation and stated (August 2022) that DG Systems had now obtained an Exit management Plan from the Vendor. The Ministry during the Exit Conference also indicated that they would (September 2022) share a copy of the plan with Audit; however, the same was awaited (December 2022).

2.7 Service Level Agreement (SLA) and Liquidated Damages

SLAs for CBIC application were designed on the basis that the Application Vendor would provide code of the application to be deployed in the

production environment to the System Integrator (SI) team. The SI[10] was the sole owner of the production environment and responsible for managing the entire infrastructure including the DC/DR sites, DC/DR Infrastructure, LAN & WAN.

CBIC was responsible for monitoring of overall timelines, SLAs and calculation of penalties/ liquidated damages. The Vendor was expected to accomplish the Scope of Work under the agreement as per the Timelines and as per the Service Levels mentioned in the RFP. If the Vendor fails to achieve the Timelines or the Service Levels due to reasons attributable to the Vendor, the Vendor shall be liable to pay liquidated damages as per the percentage of capping provided in the RFP.

Table 2.7 - Summarised Audit Finding Matrix

Sl. No.	Sub-Objective	Summary of Audit Checks	Status	Findings
1	SLAs were properly defined	SLA parameters	Partial record production	2.7
2	How SLAs are monitored	Deviations from committed SLA and Adherence level	Partial record production	2.7.1.1 2.7.1.2 2.7.1.3 2.7.2 2.7.3
3	Penalty (liquidated damages) provisions in case of non-compliance	Liquidated damages		
4	Role of Project Management Consultants if any	Incidents happening again and again	Partial records production	-

Performance requirements by the Vendor as per the Service Level Agreement (SLA) were logically segregated into the following categories:

- Project Implementation - These SLAs were applicable from the start of the project to the Go-Live of Phase II. These SLAs were for ensuring that the project went live as per the agreed timelines and quality
- Operations and Maintenance
- Call Centre (Helpdesk and technical support)
- Training
- Security

[10] Consortium of Tata Consultancy Services, Tata Communications Limited and Hewlett Packard

Against a total of 32 parameters pertaining to five SLAs, the Department provided SLA records for only 14 parameters as mentioned in the Table-2.8 below:

Table 2.8 - SLA Parameters

Sl. No.	SLA Category	SLA Parameter	Document Provided (Yes/No)
1	Levels for implementation phase	(i) Team mobilization and commencement of work	No
		(ii) Key Resource Deployment	No
		(iii) Key Resource Availability	No
		(iv) Delay in achievement of implementation/ enhancement Milestones	No
		(v) Data Migration	No
		(vi) User Acceptance Testing during implementation/ enhancement	No
2	Service Levels for Operational and Maintenance Phase	(i) Availability	No
		(ii) Response Time	No
		(iii) Change Requests / Enhancements	Yes
		(vi) Enhancement team availability	No
		(v) Handholding support	Yes
3	Help Desk and Technical Support Incident/Helpdesk (L1)	(i) Availability of telephone line	Yes
		(ii) Availability of Online complaint system	Yes
		(iii) Call Wait Time	Yes
		(iv) Call Abandonment	Yes
		(v) Total hold time on call	Yes
		(vi) Ticket acknowledgement	Yes
		(vii) Calls forwarded for feedback	Yes
		(viii) Call feedback rating	Yes
		(ix) Assignment of tickets to the	Yes

Sl. No.	SLA Category	SLA Parameter	Document Provided (Yes/No)
		concerned team for resolution	
		(x) Correct assignment of severities to tickets	Yes
	Help Desk and Technical Support Incident / Ticket Resolution (L2 & L3)	(i) Helpdesk ticket/Incident Response time	No
		(ii) Time to Resolve	No
		(iii) Time to Resolve	No
		(iv) Time to Resolve	No
		(v) Percentage of reopened incidents	No
		(vi) Submission of Root Cause Analysis (RCA) Report	No
		(vii) Timely updation of KEDB	No
4	Training	(i) On-time delivery of training as per training schedule agreed with CBIC	Yes
		(ii) Training Quality	Yes
5	Security	(i) Vulnerability assessment & Penetration Testing	No
		(II) Vulnerability assessment & Penetration Testing	No

Recommendation 5: The Department should immediately provide records for all the 32 SLA parameters to Audit.

Audit could not derive assurance regarding compliance to SLA due to lack of records. During scrutiny of the limited SLA records given to audit, the following observations were noticed:

2.7.1 Service Levels for Operational and Maintenance Phase

Out of the five SLA parameters under Operational and Maintenance Phase, Audit was provided documents in respect of two SLA parameters - Response time of application, Change Requests/Enhancements and Handholding support.

2.7.1.1 Response time of CBIC ACES-GST Application not implemented - Non-achievement of minimum target performance level

As per the RFP (Clause 10.5.1 of Vol.-I), the response time of 95% business transactions should have been within the limit of 2 seconds at Data Centre. If the Application Vendor fails to adhere this limit, he is liable to pay the liquidated damages at the agreed percentage of the quarterly payments.

Further, as per the SLA, the SI was expected to work in association with application Vendors to achieve the desired performance levels i.e., response time of the application should be less than 2 second for at least 95% of all business transaction. In case of any breach on SLA post the implementation, the SI should be liable for the applicable penalty.

During test check of the structured data provided, it was noticed that the data relating to this SLA (Quality of Service) was not provided for the quarter (April to June 2020) which indicated that this SLA was not implemented. The fact was also corroborated by the third party auditor's remarks in the SLA data viz. "The SLA is not applicable as application baselining is pending. SI team have shared the emails for low response time". Further, in case of non-achievement of the minimum targeted levels, Liquidated Damages should be invoked by the DG Systems, however, the same were not imposed against either the Application Vendor or SI Vendor.

In response, the DG System (August 2021) provided copies of correspondence that took place between SI Vendor (Consortium of TCS, TCL and HP) and Application Vendor (M/s. Wipro Ltd.) wherein the SI Vendor had regularly informed Application Vendor and the CBIC about the response time of GST Service URL and RMS access log URL where it exceeded the prescribed limit of 2 seconds. DG System further accepted (October 2021) that as per the process SI was sending regular emails to the application team for doing benchmarking of the application so that the SLA can be regularized and additional activities are done on the databases as well to ensure that there are no observations in application due to underlying infrastructure.

It is evident that Department has not actively pursued baselining of application with the Vendors and without such baselining, response time related SLA cannot be enforced. In absence of such baselining, neither the Application Vendor nor the SI Vendor is held accountable for failure to reach the targeted performance level (response time).

When the observation was pointed out (July 2022), the Ministry accepted (August 2022) the observation.

Recommendation 6: The Department should actively coordinate with both the Vendors (SI and Application Vendors) for baselining of application performance of the CBIC ACES-GST application, at the earliest.

2.7.1.2 Change Requests / Enhancements

As per the RFP (Clause 8.4 of RFP (Vol I)), all planned changes should be coordinated within the established change control process ensuring that appropriate communication on change required, approvals received, schedules adjusted etc. For any changes to the software, the Vendor had to prepare detailed documentation including proposed changes, impact to the system in terms of functional outcomes/additional features added to the system etc. Once a timeline had been agreed for implementation of a change request, then any delay from the planned timelines, reasons for which were solely attributable to the Vendor, would be penalized as mentioned in the Service Level RFP.

During scrutiny of records, it was observed that the applications for an Amnesty Scheme, Sabka Vishwas Legacy Dispute Resolution (SVLDR) and E-Way Bill module were developed as change requests. Audit noticed that there was delays (4 days to 60 days) in development of these change requests and the department imposed appropriate SLAs and LDs.

2.7.1.3 Deployment Plan for Handholding Resources

As per RFP (Clause 5.1.4 Sl. No. 14), the Vendor was required to train the resources on CBIC ACES-GST System application and deploy resources (111 hand holders) at 79 locations across the country to act as handholding support for the department users. These resources were required to assist the department users in their day to day operations on CBIC ACES-GST System. The attendance of the handholding resources would be managed by the Local Commissionerates and Target service levels had been defined for the attendance of the resources in the Service Level Agreement Section. Further, as per Schedule-III (Delivery Schedule) of MSA, the Vendor was required to submit handholding resource deployment plan by 01 September 2016 or 15 days after intimation from CBIC whichever was earlier.

Audit sought (July 2021) the handholding resource deployment plan submitted by the Vendor and actual deployment of the handholding resources. However, the Department did not provide the handholding resource deployment plan. In the absence of this, Audit could not ascertain that the Vendor had submitted a deployment plan and the handholding services were provided as per Delivery Schedule of MSA.

However, scrutiny of the payment files revealed that Vendor started the service in May 2017 and till April 2018 there was consistent shortage in the deployment of handholding resources.

2.7.2 SLA for Help Desk (L1)

As per RFP (Clause 5.1.5 of RFP Vol.1), for Helpdesk services to be provided to CBIC, the Vendor was required to setup:

- A National Call Centre (L1 Helpdesk) for handling queries from the departmental users as well as the dealers
- A Technical support team (L2/L3 Helpdesk) for providing timely resolution to the queries that could not be resolved by L1 Helpdesk

The L1 Helpdesk was set-up with an existing call Centre intended to provide 24/7 hours of support and enables both departmental users and dealers to register their complaints/suggestions. As per MSA, there are 10 SLA parameters for L1 Helpdesk Services with Liquidated damages with 20% of capping of the quarterly payments to be made to the Vendor for L1 Helpdesk service. If the liquidated damages cap was breached for two consecutive quarters, CBIC had the right to terminate the contract.

During scrutiny of the payment files relating to Helpdesk services for the period from December 2016 to March 2020, the following observations were noticed:

(i) Delayed submission of Helpdesk Operational Plan

As per Master Service Agreement (Delivery Schedule-III) dated 12 August 2016, the Vendor was required to submit Helpdesk Operational Plan by 15 September 2016 or 15 days after intimation from CBIC, whichever was earlier. The same was submitted to CBIC by a delay of one year on 01.09.2017.

On this being pointed out by Audit (July 2022), the Ministry accepted the para and stated (August 2022) that operation of the helpdesk was initiated as per contractual date and as the material period was very dynamic, the Vendor submitted the operational plan once the process got streamlined.

(ii) Non-achievement of SLAs

As per Service Level Agreements, there are 10 parameters for L1 Helpdesk Services. During the period from December 2016 to June 2017, Vendor provided helpdesk services for only 5 SLA parameters. Similarly, during quarters July-Sept 2017 and Oct-Dec 2017, the Vendor provided services for eight and nine parameters respectively. Hence, it was evident that the Vendor had not been able to achieve the required level of performance in

respect of helpdesk services for more than 12 months since the helpdesk went live in December 2016.

On this being pointed out by Audit (July 2022), the Ministry accepted the para and stated (August 2022) that SLA report was vetted by the PGA and that the Contract had maximum capping of 20% imposable LD. As such, bills were cleared on the maximum applicable SLA of 20 %. DG (Systems) made continuous efforts to make the Vendor comply with the contract provisions. These efforts resulted in the Vendor submitting the remaining SLA parameter data in the earliest possible time.

(iii) Levy of Liquidated Damages

As per RFP (Clause 10.2), the overall liquidated damages (LD) will be capped at 20% of the quarterly payment for call centre services for L1 Helpdesk.

The Helpdesk service went live in December 2016; the first invoice was submitted for the period from 07 December 2016 to February 2017 and thereafter invoices were submitted for subsequent quarters. Audit scrutiny revealed that due to non-achievement of desired targets of services and non-providing of some services, liquidated damages were more than 20% for the period from December 2016 to September 2018 (22 months) and ranged from 28.18% to 645%. However, due to capping of LD at 20% of the quarterly payment, the penalty was restricted.

RFP (Clause 10.2) indicates that if the liquidated damages cap is breached for two consecutive quarters, CBIC has the right to terminate the contract. Audit scrutiny revealed that for 22 months between December 2016 and September 2018, the calculated Liquidated Damages persisted beyond 20%.

On this being pointed out (July 2022), the Ministry stated (August 2022) that pertinently the aforementioned 22 months were marked by lot of changes in the law and the subsequently the application. In such a situation of constant flux, even changing the Vendor would not have resulted in any significant change in the quality of service.

Audit notes the reply of the Ministry.

(iv) Incident Management Performance short of target

As per RFP (Clause 10.6.2), high severity incidents are those which have critical business impact and should be resolved within 30 minutes. Average severity incidents are those which have a significant business impact and should be resolved within 4 hours whereas low severity incidents are those having minimal business impact and should be resolved within 16 hours

from the time taken to troubleshoot and Helpdesk tickets from the time the call has been logged at the Helpdesk till the time the problem is resolved/fixed. Root Cause Analysis (RCA) for all High and Medium Severity incidents was to be prepared and submitted within 5 working days from the date of resolution of incidents and the Know Error Database (KEDB) had to be updated within 5 days of the resolution date.

Scrutiny of refund grievances data revealed that 19,266 incidents of high and medium severity under refund module were created during the period from 2018 to 2021 (up to 7 August) as detailed below:

Table 2.9 - Year wise refund incident severity status

Year	Severity	Total number of Incident created	Incidents where delay was noticed	Incidents resolved within prescribed time frame	Delay range (Delays > 30 minutes in High, Delays > 4 hours in Average, Delays> 16 Hours in Low severity)	Incident still open
2018	High	9	8	1	16 Hrs 23 Minutes to 37 Days 16 Hrs. 52 Minutes	0
	Average	191	186	5	04 Hrs 50 Minutes to 94 Days 1 Hrs. 19 Minutes	0
	Low	173	164	9	23 Hrs 53 Minutes to 64 Days 15 Hrs. 44 Minutes	0
	Blank	8	8	0	1 Day 0Hrs. 54 Minutes to 113 days 15 Hrs. 09 Minutes	0
2019	High	1787	1780	7	01 Hrs.to 99 Days 02 Hrs. 53 Minutes	0
	Average	341	336	5	4Hrs. 16 Minutes to 168 days 3 Hrs. 57 Minutes	0
	Low	1091	1061	30	16 Hrs. 1 Minutes to 592 days 3 Hrs. 26 Minutes	0
	Blank	10	9	1	22 Hrs. 42 Minutes to 89 days 13 Hrs.	0

Year	Severity	Total number of Incident created	Incidents where delay was noticed	Incidents resolved within prescribed time frame	Delay range (Delays > 30 minutes in High, Delays > 4 hours in Average, Delays> 16 Hours in Low severity)	Incident still open
					7 Minutes	
2020	High	5918	5903	15	31 Minutes to 249 days 11 Hrs. 44 Minutes	2
	Average	120	119	1	4 Hrs. 15 Minutes to 100 days 22 Hrs 9 Minutes	1
	Low	1879	1786	93	16 Hrs. 1 Minutes to 267 days 4 Hrs. 39 Minutes	0
	Blank	16	16	0	19 Hrs. 19 Minutes to 149 days 5o Minutes	1
2021	High	7507	7492	15	31 Minutes to 138 days 19 Hrs. 22 Minutes	800
	Average	161	161	0	21 Hrs. 24 Minutes to 98 days 1 Hrs. 6 Minutes	4
	Low	41	38	3	19 Hrs. 50 Minutes to 56 days 23 Hrs. 32 Minutes	3
	Blank	14	14	0	2 days 20 Hrs 39 Minutes to 100 days 1 Hrs 8 Minutes	0
Total		**19266**	**19081**	**185**		**811**

Source: Data provided by Department (as of July 2021)

It is evident from the above table that out of 15,221 incidents of high severity, 15,183 (99.75%) incidents were resolved after the prescribed limit of 30 minutes. In the category of 'average severity' incidents, 802 (98.64%) out of 813 incidents were resolved after the prescribed time. Similarly, in the category of 'low severity' incident 3,049 (95.76%) out of 3,184 incidents

were resolved with a delay. Audit also noticed that 48 incidents were not assigned under any severity and remained blank.

This indicated overall delayed management of the incidents and inability to close them within the prescribed time.

In response to the audit observation (September 2021), the Ministry stated (August 2022) that the Department has deducted maximum LD of 20% in all the quarterly payment made up to July-September 2021.

Recommendation 7: The Department needs to monitor and put constant pressure on the Vendor to resolve incidents within the prescribed timelines according to the incident category. Since LD is capped at a maximum of 20 percent this is not acting as an effective disincentive for the Vendor.

2.7.3 SLA for Training

As per RFP (Clause 5.1.4 Sl. No. 1), the Vendor was required to train the departmental users to enable them to effectively operate and perform relevant functions using the CBIC ACES-GST Application system. There are two service level parameters (i) 'On-time delivery of training as per training schedule agreed with CBIC' without delay and (ii) 'Training Quality' in terms of feedback to be taken from Nodal officer. The liquidated damages (LD) for not achieving training related timelines were capped at maximum of 20% of the training cost, which might be reviewed after six months from the Effective Date and at such intervals as might be decided by CBIC.

As per Master Service Agreement (MSA), training for 200 batches (one batch each of 25) was planned to be conducted. Further, as per Delivery Schedule-III, the Vendor was required to submit the Training Plan by 30 September 2016 or 15 days after intimation from CBIC, whichever is earlier, and start the training sessions after the Training Plan was approved by CBIC.

(i) Non-achievement of SLA for providing training service

Scrutiny of records revealed that training for 164 batches was conducted from January 2017 to September 2017 and 36 batches were pending for training till September 2021. During the above period, the performance of the Vendor was not as per the required level and liquidated damages were imposed to the maximum (20%) capping limit, whereas the calculations done by the Project Governance and Monitoring Agency (PGMA) (M/s PWC) was above the 20% capping and ranged from 27% to 149%. However, the Department was bound to impose only 20% as capped

liquidated damages despite the performance level being low by the Vendor.

On being pointed out by Audit (July 2022), the Ministry stated (August 2022) that the prevalent time had new tax regime change. Any new vendor would have had to be engaged in due lengthy RFP process and ultimately it would have faced the similar situations. Further, the Department also undertook an exercise to create a pool of master trainers from the available departmental officers who were further entrusted with training programmes. This effected in more numbers of training schedules being conducted by the CBIC officers and less dependency on the vendor.

(ii) Non-revision of SLA definitions, target levels and liquidated damages

As per RFP, SLA definitions, target levels and liquidated damages were to be reviewed after six months from the effective date and at such intervals as may be decided by the Purchaser. However, Audit noticed that the Department did not review and revise the same.

After being pointed out by Audit (July 2022), the Ministry, while accepting the para stated (August 2022) that CBIC had now reviewed the contract and SLAs. The competent authority had also approved an addendum to the RFP accordingly.

Recommendation 8: The Department should ensure that implementation of all aspects of SLA are effectively monitored; the Department and the Vendor perform their respective roles in accordance with the contractual provisions and non/late performance is effectively reviewed and resolved within the agreed time limit.

On this being pointed out by Audit (July 2022), the Ministry accepted the recommendation and stated (August 2022) the Department has deducted maximum L.D of 20% in all the quarterly payment made up to July-September 2021.

2.8 Change Management

In IT organisations, a structured change management process is normally used to manage and control changes to assets, such as software, hardware, and related documentation. Change controls are needed to ensure that all changes to system configurations are authorised, tested, documented and controlled so that the systems continue to support business operations in the manner planned, and that there is an adequate trail/record of changes.

Table 2.10 - Summarised Audit Finding Matrix

Sl. No.	Sub-Objective	Summary of Audit Checks	Status	Findings
1.	Whether appropriate communication between Vendor and CBIC on change required has taken place;	CR Policy, Procedures for initiation, review and approval of CR, Change Control Board, Review of logs and Reports, Change Order timelines.	Partial record production	2.8 2.8.1
2.	Whether proper approvals have been received by the Vendor from CBIC;	Change Order, Pre- and post-change system and user documentation.	Scope restriction	-
3.	Whether schedules have been adjusted or re-prioritized to minimize impact on the production environment.	Back up documents for the change order, Emergency change.	Scope restriction	-

RFP has elaborated the procedures for initiation, review and approval for change along with mapping of responsibility for these tasks. As per RFP (Clause 8.4), the Vendor had to prepare detailed documentation including proposed changes, impact to the system in terms of functional outcomes/additional features added to the system etc. The Vendor shall obtain approval from CBIC for all the proposed changes before implementation of the same into production environment and such documentation is subject to review at the end of each quarter of operations and maintenance support.

Once a timeline had been agreed for implementation of a change request, then any delay from the planned timelines, reasons for which were solely attributable to the Vendor, would be penalized as mentioned in the Service Level Agreement of the RFP. In case of major changes, approval would be sought in the Steering Committee meetings.

Audit requisitioned the records relating to establishment of Change Control Board (CAB), change control logs, development of back out process before any change request is implemented, Change Management procedures to control emergency changes to the system, change order documentation etc. But the Department did not provide the documents against the requisitioned records and only provided the list of change requests (CRs) carried out in the system and expenditure incurred on these CRs which are given below:

2.8.1 Change Requests / Enhancements

During scrutiny of the information provided by the Department, it was noticed that the department implemented 173 change requests valuing of ₹ 16.62 crore during the period 2017-18 to 2020-21 under different modules as detailed in the table below.

Table 2.11 - Change Requests

(Amount in ₹ lakh)

Sl. No.	Name of Module	2017-18		2018-19		2019-20		2020-21	
		No. of CRs	Value of CRs	No. of CRs	Value of CRs	No. of CRs	Value of CRs	No. of CRs	Value of CRs
1.	Registration	7	31.18	1	10.47	12	155.36	7	94.55
2.	Returns	10	47.02	15	81.44	19	377.67	9	55.38
3.	Payment	- (*)							
4.	Refund	2	28.20	7	54.61	14	53.14	7	126.37
5.	DSR (ADJ+REC+APL)	-	-	-	-	4	105.50	7	79.54
6.	Investigation	-	-	-	-	3	46.70	1	4.65
7.	Export (*)	- (*)							
8.	ACES GST	- (*)		2	21.63	12	12.56	3	7.53
9.	Mobile App	Mobile App is only at the SRS sign off stage.							
10.	Audit	Audit modules is at the SRS sign off stage.							
11.	Taxpayers at Glance (*)	- (*)							
12.	Access Control Logic	- (*)							
13.	Common CRs	16	3.44	-	-	1	7.87	-	-
14.	SVLDRS**	-	-	4	116.34	-	-	-	-
15.	E-way Bill	-	-	-	-	10	140.30	-	-
Total		**35**	**109.86**	**29**	**284.51**	**75**	**899.15**	**34**	**368.06**

(*)CR Details not Available

(**)SVLDRS was a new requirement which has been carried out through CR.

2.9 IT Security

IT security protects the integrity of information technologies like computer systems, networks, and data from attack, damage or unauthorized access.

Table 2.12 - Summarised Audit Finding Matrix

Sl. No.	Sub-Objective	Summary of Audit Checks	Status	Findings
1.	Whether Security of the IT system has been designed in an effective way?	User Access Management Process	Checked	2.9.1.1
2.	Business Continuity and Disaster Recovery	Business Impact Analysis, Risk Assessment Reports, Backing up data and programs, Patching compliance reports, Data replications scheduled, Resource requirements, Disaster Recovery (DR) Drill Plan, Crisis Management Team, Recover Point Objective (RPO) and Recovery Time Objective (RTO)	Checked	To be Covered separately in IT Audit of SI (Saksham) Project.

2.9.1 Access Control

Access Control Logic module (ACL) determines how the privileges are to be assigned to various users so that the business processes can be performed by the authorized users as prescribed. An ideal ACL should not only correctly assign the privileges to the proper officer, but should also provide required flexibilities for reassigning the roles, transfer the pending jobs etc., as desired.

Access control ensures that only users with the process credentials have access to sensitive data. Access to business information and data should be controlled in order to restrict the access to authorized users only. Any inappropriate access or unauthorized changes to application software, information or data must be restricted.

2.9.1.1 User Access Management (UAM)

User Access Management includes providing, maintaining and removing a user's access to various components of CBIC infrastructure such as network, applications and network devices in a controlled manner. Audit observed that the Department has a clearly defined policy/framework for access control in the application. Access in the Application is based on RFP and SRS drawn. Within the Application, access is given by the Administrator (ACL Admin) of the formation based on posting of a User in a formation. The procedures for User Registration, User Modification, Personal information modification of an existing user, Designation

Modification, Access for pending tasks in previous location, Additional Charge, Disable Request, Retired User, etc. are clearly delineated in the policy framework. A broad outline of the procedure is mentioned below:

SSO ID Creation - Nodal Officer initiates SSO ID creation request by filling SSO ID creation template and forwards the same from his/her official Icegate email ID / gov.in / nic.in ID to Saksham Seva.

UAM Team Verification - On receiving the request, the UAM Team verifies the channel of request, correct and mandatory fields in template and relevant documents of the user for verifying name, DOB (Date of Birth), DOJ (Date of Joining), etc.

Duplication Check - The UAM Team also verifies if a duplicate SSOID already exists for the user. If no existing SSOID is found, the UAM Team proceeds for creation of SSO ID.

Process post duplication check - The UAM Team sends email and the interaction to PMU Team for approval with observations of duplication check. PMU Team verifies the request and all attachments. After verification, the PMU Team forwards the request to UAM DOS[11] for seeking approval.

Maker Checker - The associate processing the request is designated as the Maker and the associate verifying the complete request is identified as the Checker. Post creation of SSO ID/Email ID, the Checker performs the validation check.

A similar procedure is followed in case of modification, activation and de-activation of user roles in the system.

In the production environment, Audit examined one case each of designation modification, deactivation of SSOID of retiring officer/official and disabling of SSOID of Vendor's staff. In these three test-checked cases, it was noticed that the procedures as per User Access Management were followed and no deviations were found.

2.9.2 IT Service Continuity Management Plan

CBIC came out with an IT Service Continuity Management (ITSCM) Plan (Version 2.3) dated November 2019 to ensure continuity of its business operations. The IT Service Continuity Plan (ITSCM Plan) outlines the contingency plans for business threatening emergencies, continuing business and complete recovery of its business applications in the event of a disaster at any of the data centers of CBIC.

[11] Directorate of Systems

CBIC released Information Security Policy (Version 2.3) dated July 2020 which defines the overall framework for implementing and sustaining a compliant and effective security program.

During the course of audit, the Department was asked to provide the information/documents relating to Information Security applied in the CBIC ACES-GST Application. In response, the Department provided the Information Security Policy, Back up Policy etc. Scrutiny of these documents revealed that:

(i) **Information Security Policy**

Scrutiny of the Information Security Policy revealed that the roles and responsibilities were clearly defined for protection of information assets within the IT Department. In the policy document, provisions for media handling (management of removal media, disposal of media, physical media transfer) are also covered.

The first version of IT Security Policy was issued in June 2009 and the last updated version was issued in July 2020.

(ii) **Backup Policy**

As per the Backup Policy document, the data is categorized as critical data (core business application & data) and non-critical data (Non-core business application and data). This data is to be backed-up fully on weekly, monthly and yearly basis with data retention on monthly and yearly basis. Back up of network devices is to be taken up on weekly basis and stored on local drive of a server/Physical Tape Cartridges. Configuration back up of data center core firewalls is manually taken on daily basis. Network devices logs is to be backed up through Arc sight logger server.

Back up Policy has been updated periodically. The first version was issued in August 2009 and the latest updated version was issued in July 2020.

Detailed audit of the above-mentioned aspects of IS Security would be taken up separately as part of a future audit of the Systems Integrator Saksham project.