

Chapter-4
Information System Security

CHAPTER-4

Information System Security

4.1 Introduction

Traditionally, information available with the government has been safely managed by keeping it in paper records throughout its lifecycle i.e. creation, storage, access, modification, distribution, and destruction. However, to make all government services accessible to the common man in his locality, through efficient service delivery outlets, along with transparency & reliability, the government has steadily graduated towards using electronic formats of information.

IFMS is a web-based application for payment, accounting and reconciliation of Government transactions which integrates various existing standalone systems. IFMS envisages single point of data capture; hence assume greater importance to ensure the integrity and correctness of information. As treasury transactions are very sensitive in nature and is therefore imperative that the security, consistency and integrity of such data and transactions should be maintained at all levels.

4.2 Audit findings

In Uttarakhand, the IFMS went live from 1 April 2019. It is currently being operated through FDC located in the premises of Directorate Treasury, Pension and Entitlement, Dehradun. During Joint physical inspection of FDC and system review of IFMS, audit found following (**Table-4.1**) features to be installed and working in the IFMS and setup:

Table-4.1: List of observations noticed during joint verification of FDC

Sl. No.	Parameter	Audit observation
1.	Physical Access controls	During Joint inspection of FDC audit noticed that <ul style="list-style-type: none">Physical access to FDC was restricted by biometric door lock devices.Server room was secured with three layer biometric securities and only authorised personnel were given access to the server room.Preventive measures like fire extinguishers, air-conditioned machines, etc. were in place. No dust and loose articles were found in server room.
2.	Monitoring Vulnerability and threats	Intrusion Prevention System (IPS), Anti Malware, Firewall, email filtering to monitor vulnerability and threat through Fort iGATE 2600F Series Firewall was installed at FDC and system logs were being recorded.
3.	Database security	Audit observed that: <ul style="list-style-type: none">Database server was installed on separate dedicated machine, hosted in private network of UKSWAN.Three – tier connection methodology was adopted as all connections to database were routed through Application / Integration Server.Database was configured to allow only trusted IP address.All users' sessions were encrypted through Secure Socket Layer (SSL) handshake keeping data secure in transit.The development database / application was kept separate from production database / application.

4.2.1 Non-conduction of Performance and Quality Audit from STQC

Standardization Testing and Quality Certification (STQC) Directorate, is an attached office of the Ministry of Electronics and Information Technology, Government of India, which provides Quality Assurance Services for software testing, information security and IT Service Management by conducting Testing, Training, Audit and Certifications.

Audit observed that it was the responsibility of selected bidder¹ to carry out Performance and Quality Audit from STQC before IFMS went live. But the system went live on 01 April 2019 without the required certification from STQC. During audit, DTPE also accepted that the users of IFMS were facing slowness issues. Therefore, in absence of necessary STQC certification, risk of quality and performance issues in IFMS could not be ruled out.

The Government in its reply accepted the facts and stated (August 2023) that some digitization work was going on and shall be completed by 2023-24. STQC will be done once digitization work was completed. Reply was not acceptable as the contract with the vendor, who had already been paid for the deliverable 'Performance and Quality Audit from STQC', already expired on 31st March 2023.

4.2.2 IS security systemic deficiencies

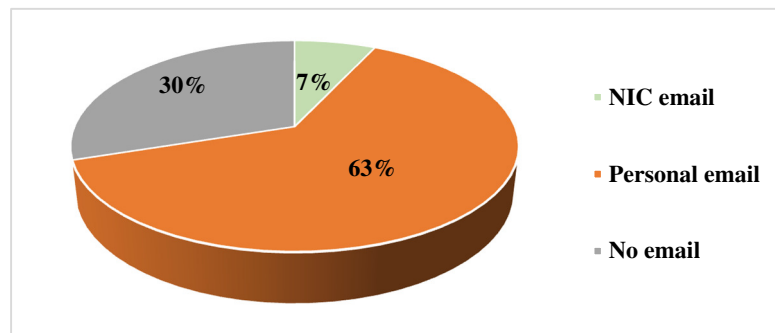
During system review, audit noticed following deficiencies in the system:

(i) Use of personal email IDs by DDOs

As per directions of GoU, "All DDOs shall use Government e-mail in IFMS portal provided by State NIC for all official work and communication. Usage of personal email is strictly forbidden in IFMS". Audit observed that 2912 (63%) out of 4586 DDOs were registered with their personal e-mail IDs as there was no check available in IFMS to ensure that DDOs register in IFMS through government e-mail IDs only. This created a potential security risk as government data was being stored in servers outside government control.

The Government, during exit conference (June 2023) accepted the audit observation and stated that a campaign to create government e-mail IDs for remaining DDOs shall be launched and subsequently e-mail IDs of DDOs shall be updated in IFMS.

Chart-5: Use of email IDs



¹ M/s IWS.

(ii) Non-incorporation of audit trails

An audit trail (also called audit log) is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, event, or device. During system walk through, audit noticed that audit trails were not being incorporated in IFMS due to which details of changes made through IFMS were not traceable through front end. For example: Lifecycle of a bill including details of rejections and subsequent actions taken on the bill were captured in the form of logs at back-end but were not available at front end for DDO user.

Government accepted the fact that audit trail was not visible through front end and stated (August 2023) that report of audit trail will be made available to DDOs soon.

(iii) Weak Password policy

Password policy provides that password should be a combination of upper and lower case characters, digits and punctuation characters as well and other characters. Audit noticed that the system was not enforcing use of lower case while constructing password.

The Government accepted the fact and assured (August 2023) of its compliance in future.

(iv) Non implementation of Biometric authentication during Login

As per Software Requirement Specification (SRS) of the project, Biometric authentication (in form of fingerprint capture) of registered users of DDO System² and Treasuries was to be implemented in IFMS. However, it remained non-implementable even after three years of operationalization of IFMS.

The Government accepted the importance of biometric authentication and stated (August 2023) that integration with Aadhaar was proposed. Once implemented, Aadhaar based biometric authentication will be done by the users at the time of login.

(v) Network Security

Audit observed that IFMS was being operated on UKSWAN managed by Information Technology Development Agency (ITDA), Dehradun. Despite request to DTPE and ITDA to provided network security audit certificates of UKSWAN to Audit, they were not provided. In absence of audit certificate, Audit could not ascertain the network security of IFMS.

4.2.3 Absence of Business Continuity Plan (BCP)

Formulation of BCP was the major component to be implemented under IFMS project. It ensures that the system runs smoothly and resumes its operations within definite time period in case of disasters and other emergency events. Audit noticed that BCP had not been framed and adopted for IFMS, even after four years since operation. In its absence, the staff/ users were unaware of the procedure to be followed in the event of disruptions/

² DDO is primarily a front-office type of web application and is accessible over the internet using a web browser.

disasters. They were also not trained in preventing, mitigating, and responding to emergency situations.

The Government accepted the criticality of BCP during exit conference (June 2023) and directed DTPE to frame the BCP as soon as possible.

Reply was not acceptable as framing of BCP was the responsibility of vendor who had already been paid for the same. In absence of BCP, business continuity of IFMS remained at risk in case of disruptions/disasters.

4.2.4 Disaster Recovery site not set up

Disaster Recovery (DR) aims at protecting the Department from the effects of significant catastrophic events. It allows the Department to quickly resume mission-critical functions after a disaster. Various possible disasters that can take place are – human error, epidemic, power outage, fire or explosions etc. The distance for a DR site can vary depending on the types of disaster - such as earthquakes, floods, terror attacks, etc. The Department should choose a DR location that fits its business model and regulatory requirements.

Audit observed that as per the DPR of the project, DR site was to be set up at State Data Centre (SDC) at ITDA. In the same DPR, it was envisaged that once the SDC at ITDA becomes operational, all IT infrastructure and IFMS operations at Finance Data Center³ (FDC) would be relocated to SDC and the former would act as an archival site. The proposal to make SDC the DR site was reiterated in a meeting held with DTPE, NIC & ITDA under chairmanship of Finance Secretary on 03 December 2021.

Audit noticed that the two provisions of DPR were mutually contradictory as in case of shifting of IFMS operations from FDC to SDC, the latter could not act as DR site which by definition had to be present at geographically different location. Moreover, both FDC and SDC were located near to each other, around 6.5 kilometers apart and in a region vulnerable to disasters (Seismic zone IV). Recently, flash flood like situation was created in the region due to cloudburst on 25 August 2021. Thus, despite IFMS being operational since 1 April 2019, no efforts had been made to set up a DR Site, in absence of which the critical financial operations of GoU remained vulnerable in case of any disaster.

During exit conference (Jun 2023), Government accepted the importance of DR site and stated that IFMS application, presently hosted in FDC was planned to be shifted to SDC in ITDA. Further, ITDA was planning to create a ‘far’ DR site for all the applications hosted in SDC.

Reply was not acceptable as Dehradun lies in seismic zone and prone to natural disasters like earthquakes, floods, cloud bursts etc. In absence of a functional DR site, business continuity of IFMS remained at risk in case of disasters.

³ In DPR, Integrated Data Center

4.2.5 Backup and recovery controls

National Information Security Policy and Guidelines, 2014 provides that organization must ensure that backup copies are maintained for all operational data to enable reconstruction should they be inadvertently destroyed or lost. Also, Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.

Audit noticed that the data generated in IFMS was replicated on real time basis in SDC of ITDA. In the FDC of DTPE, scheduled backup was done in which backup of data schemas was taken on daily basis and full backup was taken after every 15 days. However, despite three years of go-live of IFMS, Department had not formulated the backup policy and tested the system by restoring it through back-up data. Also, the Department did not determine the data retention period, in absence of which data kept on accumulating and could impact the performance of system such as increased response time, etc.

The Government in its reply (August 2023) accepted the fact that backup policy had not been formulated but daily, monthly, incremental and full backups were taken by the Database Administrator (DBA). Government in its reply claimed that backup activities were reviewed and tested on monthly basis, however no documents were provided to audit to substantiate the claims.

4.2.6 Critical financial data handled by outsourced personnel

To manage FDC, DTPE demanded the sanction of *seven* posts/technical cadre citing the necessity of deploying technically proficient regular personnel in view of the sensitivity of the work and the financial implications involved. As per GO dated 12 September 2019, three technical posts⁴ were sanctioned by the GoU and directed DTPE to formulate service rules before direct recruitment to aforesaid technical cadre and fill the created posts before 29.02.2020.

Audit noticed that instead of formulating the required service rules and direct recruitment to the sanctioned posts, all the technical staff at FDC was outsourced and hired on contractual basis. This not only created dependency on contractual staff but also involved significant security risk as the critical database including financial transactions and personal data were handled by outsourced personnel. This defeated the purpose of 'restricting the possible misuse and to protect the stored data' for which DTPE got the technical cadre sanctioned from the GoU.

The Government in its reply (August 2023) stated that outsourced personnel worked under the close supervision of the Domain Team which was manned by government employees. Most of the outsourced personnel were working with FDC since last ten years. Efforts were being made to have additional technical resources who would not only help

⁴ Two direct recruitment posts (System Administrator and Database Administrator) and one outsourced post (Senior Software Engineer)

in maintenance and enhancement of IFMS but work as back up of existing resources. In future, requisition would also be sent to the Government for hiring permanent technical staff after their service rule is framed.

4.2.7 Absence of documentation and policies

Web Application security is of paramount concern for all stakeholders. Guidelines for Indian Government Websites state that Department must formulate a security policy to address various security issues related to the website. Hence, a well-documented security policy was required for proper functioning of IFMS.

Audit observed that Department did not formulate any IT security policy for security of IT assets, software and data, backup, data retention and disposal, incident reporting, e-mail, Password, etc. Due to lack of documented security policy, every user was free to handle such issues in his own manner which could pose risks to IT security of IFMS.

The Government accepted the facts and stated (August 2023) that IFMS was being shifted to SDC and IT policies regarding infrastructure, network, password etc. would be adopted as of SDC. Whereas other policies like BCP, DR Policy etc. would be framed by DTPE in due course.

4.3 Poor feedback from end users of IFMS

Audit carried out an online survey to get feedback from end-users of IFMS at DDOs and Treasuries. Nearly 370 responses were received. Issues reported were related to Login, OTP delay, poor and delayed support from helpdesk, slow speed of site, server down, bill creation and accounting, lack of training, lack of user-friendliness, issue in various reports and modules, non-availability of legacy data, work-flow, vendor or party management, file-upload size, unnecessary 20 minutes' wait period after abrupt logout, duplicity of work due to hardcopies, save-session not enabled, mismatch in GPF, delayed voucher generation, duplicity of accounts of contractors in context of GST, Works module, and many other issues.

The Government accepted the feedback given by IFMS users and stated (August 2023) that few issues had been identified and fixed. Issues related to slowness of the system would be resolved once system is moved to SDC. Other issues would be fixed after hiring of additional technical staff.

4.4 Conclusion

Information security of IFMS application is of paramount concern to owners as well as users of the applications as treasury transactions are very sensitive in nature. Audit noticed that IFMS went live without required performance and quality certification from STQC. In IFMS, DDOs were registered with their personal e-mail IDs causing potential security risk. Department did not implement biometric authentication even after *three* years of operationalization of IFMS. In absence of audit certificate, network security of IFMS could not be ensured. Despite being in seismic zone, Department did not frame BCP/set up any functional DR site. In absence of BCP/DR site, business continuity of

IFMS remained at risk in case of disasters. Department did not formulate any IT security policy. In absence of documented policies, users were free to handle security related issues in their own manner which could pose risks to IT security of IFMS.

4.5 Recommendations


- *The Department should expedite the process of creating and updating government email Ids for remaining DDOs in IFMS.*
- *The Department should formulate Business Continuity Plan and set up Disaster Recovery site to ensure that the system runs smoothly and resumes its operations within definite time period in case of disasters and other emergency events.*
- *The Department should review and test the backup restore activity on regular basis so that data can be restored if inadvertently destroyed or lost.*
- *The Department should formulate an IT security policy for security of IT assets, software and data, backup, data retention and disposal etc.*

Dehradun
The 10 April 2024


(PRAVINDRA YADAV)
Principal Accountant General (Audit),
Uttarakhand

Countersigned

New Delhi
The 26 April 2024


(GIRISH CHANDRA MURMU)
Comptroller and Auditor General of India

