CHAPTER VIII

INFORMATION SYSTEM SECURITY CONTROLS

CHAPTER-VIII
INFORMATION SYSTEM SECURITY CONTROLS

The Department failed to conduct third party independent testing. Security Audit was not conducted for some IFMS-K applications. The budget application used for the state budget was running in an unlicensed DB2 version. The system allowed multiple logins in various web-based applications. IFMS-K is not identified as Critical Information Infrastructure (CII) under GoI guidelines. Disaster Recovery (DR) Plan and Data Retention Policy were not formulated and far DR centre to ensure data protection is not available.

8.1 Introduction

IFMS-K plays vital role in managing and safeguarding details of funds and transactions of Government of Kerala, making it a potential target for internal and external threats. Security controls are, therefore, crucial to ensure the protection of financial assets and sensitive information of Government and the public. Identification of vulnerabilities for enhancing security controls and ensuring compliance with applicable regulations and standards is essential in protecting financial assets, maintain integrity of financial transactions and uphold public trust in the system.

Key areas of security controls of information systems are:

- Physical security: Ensures that only authorised personnel have access to sensitive areas and that appropriate security measures are in place.
- Information Security: Protects against unauthorised access, data breaches, and cyber-attacks.
- Network and Network Infrastructure Security: Detects and responds to any suspicious activity.
- Internal Controls and Processes: Ensures that adequate controls are in place to prevent fraud, errors, or misappropriation of funds.
- Compliance with Regulatory Requirements: Compliance with relevant regulations, such as Government Accounting Standards, RBI guidelines, IT Act and any specific regulatory requirements.
- Incident Response and Business Continuity: Evaluates incident response plans, disaster recovery procedures, and business continuity strategies to ensure that appropriate measures are in place to respond to and recover from security incidents or disruptions in operations.

Security lapses noticed during audit of IFMS-K are detailed in succeeding paragraphs.

8.2 Non-conducting of System testing by third party

Government of India guidelines (January 2009) for Indian Government websites stipulates that each website/ application must undergo a security audit from empanelled agencies and clearance prior to hosting and also after addition of new modules.

Audit observed that no such third-party independent testing of the IFMS-K to identify design flaws was performed for assurance on the reliability of the system.

Government stated (March 2023) that third party security testing of applications under the direct control of the Department of Finance have been initiated.

While noting the action initiated by State Government, the fact remains that security testing has not been undertaken for the applications managed by Department of Treasuries.

8.3 Non-reception of Safe to Host Certificate

Government direction (October 2015) stipulates that 'Safe to Host' security audit certificate is mandatory for any websites to be hosted at State Data Centre. Government further reiterated (April 2019) the requirement of 'Safe to Host' security audit certificate for all e-governance application, from CERT-In[44] empaneled security auditing agency.

Audit observed that Safe to Host certificates were not received for any of the IFMS-K applications. Further, though the applications maintained by Department of Treasuries have been security audited, those maintained by Department of Finance have not been security audited.

Government stated (March 2023) that the treasury applications are security audited and subsequent versions are being audited by STQC. 'Safe to Host' certificate would be furnished by Treasury Department. Further, in case of other IFMS-K applications security auditing status and 'Safe to Host' certificate would also be furnished.

While noting the reply, the fact remains that the Safe to Host Certificate has not been arranged for the last eight years.

8.4 System permits Multiple Login

Simultaneous multiple logins from a single computer and same user logging in from different systems simultaneously are to be disabled in all web-based applications having public access to internet for security reasons.

Audit observed that multiple logins were allowed with no IP restrictions and the users could access applications from multiple computers simultaneously regarding applications managed by Department of Finance. Test check (BIMS,

[44] Indian Computer Emergency Response Team.

BAMS) also revealed that internet-based applications permitted multiple user sign in. This lapse has made the applications vulnerable to security incidents.

Government stated (March 2023) that IP binding is not possible for Internet based applications and possible only for Intranet applications.

The reply is not tenable. The Audit comment is not about IP binding of Internet based applications but about simultaneous login with same username and password from different computers which can be restricted.

Recommendation No. 38

Government should limit user sessions to single login per account and a single account from a computer at a time to enhance security.

8.5 Usage of unsupported DB2 Database Management System

Unsupported software lacks vendor support and access to regular updates and security patches leaving the organisation vulnerable to potential software bugs, security vulnerabilities, and other technical issues. Use of unsupported software potentially impacts effective management of data, streamlining of processes, and integration with critical applications or databases.

Audit observed that the Budget 2.0 application used for the preparation of State Budget in Department of Finance was running in an unsupported DB2 version 8 of IBM. As per official website of IBM, extended support of DB2 version 8 ended on 30 April 2012.

Government stated (November 2024) that steps for database migration is in progress.

Recommendation No. 39

Government should fix a timeline for completing the data migration and ensure supported Database Management Systems are used.

8.6 Delay in implementation of Single Sign-On

Single Sign-On (SSO) is a technology that lets users log in to multiple applications and websites with one set of credentials. SSO makes the authentication process more efficient for users.

During IFMS-K review meeting (April 2017) it was decided to implement proper security features in IFMS-K using Single Sign-On. NIC was to provide technical opinion on the matter. In the IFMS-K review meeting (July 2017), the Department of Treasuries was directed to complete the Lightweight Directory

Access Protocol (LDAP)[45] and SSO in all applications of treasury within two weeks.

Audit observed that even after a lapse of eight years, SSO is not completed.

Government stated (December 2022 and March 2023) that LDAP for intra-treasury was started implementing during the beginning of year 2018 and was later disabled during 2020-21 due to server issues. Later, after installation of new servers during 2021-22, AEBAS[46] based OTP for multi-factor authentication was enabled in the Intra-treasury applications and implemented SSO using *Parichay* for internet-based applications during the current financial year and hence there was no undue delay in the implementation of SSO for IFMS-K applications.

The reply is not tenable, as this does not fulfill the purpose of Single Sign-On. Audit verified various intra-treasury applications (*eg*: CoreTIS, CoreTSB, CRA, PIMS *etc*.) during July 2024 and noticed that the users had to still login to these modules separately each time. For the internet-based applications (BIMS, BAMS, WAMS *etc.*) of IFMS-K, even though NIC's SSO is implemented, it was optional. For certain other applications such as SPARK, BDS *etc*., the NIC's SSO was not implemented.

8.7 Non-identification as Critical Information Infrastructure

Information Technology Act, 2000 defines Critical Information Infrastructure (CII) as a computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety. The Information Technology (National Critical Information Infrastructure Protection Centre (NCIIPC)[47] and Manner of Performing Functions and Duties) Rules, 2013 mandates that the basic responsibility for protecting CII system shall lie with the agency running that CII. The NCIIPC has identified Government among others as critical sector and laid down guidelines for identification of CIIs based on a set of parameters such as the total number of transactions per day, the value of all types of transactions per day, number of connected devices and network size, number of customers of different categories *etc.* NCIIPC shall monitor and forecast national level threats to CII for situational awareness for early warnings alerts. IFMS-K qualifies to be identified and notified as CII.

Audit observed that the department was yet to assess the criticality of the system and take measures to notify IFMS-K as a CII under GoI guidelines, depriving the project of an enhanced security infrastructure commensurate with its significance.

---

[45] An open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

[46] Aadhaar Enabled Biometric Attendance System.

[47] NCIIPC is an organisation of the Government of India created under Section 70A of the IT Act, 2000 and designated as the national nodal agency for Critical Information Infrastructure Protection vide Gazette Notification G.S.R 18(E) dated 16 January 2014.

Government stated (November 2024) that steps for notifying IFMS-K as a CII under Government of India guidelines are in the initial phase of discussion with NIC.

Recommendation No. 40

Government should fix a time frame to notify IFMS-K as a Critical Information Infrastructure.

8.8 Non-formulation of Data Retention Policy

Data protection is the process of safeguarding important information from corruption, compromise or loss. It is a set of strategies and processes used to secure the privacy, availability, and integrity of the data. A data protection strategy is vital for any organisation that collects, handles, or stores sensitive data. A successful strategy can help prevent data loss, theft, or corruption and can help minimise damage caused in the event of a breach or disaster. A Data Retention Policy (DRP) has to have provisions for classification of data, risk assessment of data, data retention period, data security aspects, disposal of data once the retention period is over and ensure that the data centre architecture supports the DRP.

Audit observed that the department is yet to formulate an appropriate Data Retention Policy (DRP). There were no documents available regarding the period for which the transactional data would be retained in live database and as of how the data pertaining to lapsed period is to be handled.

Government stated (November 2024) that an appropriate Data Retention Policy specifying the period for which the transactional data would be retained in live database and management of the data pertaining to lapsed period shall be formulated sooner after deliberation with the stakeholders.

Recommendation No. 41

Government should fix a time frame to implement a Data Retention Policy.

8.9 Absence of Business continuity/ Disaster management plan

Disaster Recovery (DR) aims at protecting the organisation from the effects of significant catastrophic events. It allows the organisations to quickly resume mission-critical functions after a disaster. The goal for any organisation with DR is to continue operating as close to normal as possible in case of system crash, calamities like theft, fire, floods, *etc*.

As part of the implementation of Government Receipts Accounting System (GRAS), servers and other IT equipment were procured and installed at State Data Centre-1 (SDC-1)[48] as primary Data Centre and National Data Centre (NDC), New Delhi as Far Disaster Recovery (DR) site on 31 January 2014.

[48] Co-Bank Tower, Thiruvananthapuram.

However, later, new server and IT equipment were installed at SDC-2[49], and made operational from May 2021 as primary Data Centre. Four servers and one Network Attached Storage (NAS) were shifted to SDC-1, and database replication started there as near DR site from 09 January 2022.

8.9.1 Non-availability of Far Disaster Recovery Centre and futile claim of service charges

A Far DR site should be located at a significant distance from the primary site or production environment. This geographic separation helps to mitigate the risk of a single point of failure. It ensures that if a disaster such as a natural calamity or infrastructure failure affects the primary site, the Far DR site remains unaffected, allowing critical operations to continue. Far DR site plays a vital role in ensuring the resilience, data protection, and continuous operations of treasuries, particularly in the face of unforeseen disasters or disruptions.

The IT equipment installed at NDC, New Delhi for far DR could not conduct real time data transfer and the Technical Committee in its meeting (May 2021) recommended that the far DR at NDC, New Delhi to be discarded and the equipment installed there is to be disposed of as scrap.

Audit noticed that initially no charges were levied for Data Centre Services at NDC, New Delhi. Later, it was informed by NIC that, starting from 01 August 2018, DR services would be provided on payment basis, with payments required in full advance for the services. Therefore, NIC claimed an amount of ₹0.83 crore for hosting the Far DR at NDC, New Delhi.

Audit observed that due to non-availability of Far DR, real time data transfer could not be ensured.

Government stated (November 2024) that the Kerala State IT Mission has already allotted space for setting up a Far DR at Secunderabad and the configuration process is underway. Government also stated that communication with NIC is going on to settle the issue without any financial commitment to Government.

Recommendation No. 42

Government should fix a time frame to establish a Far DR and also for settling the claim of NIC.

8.9.2 Absence of a Disaster Recovery Plan

A Disaster Recovery Plan (DRP) is a documented strategy that outlines the steps and procedures to be followed to recover critical systems, data, and operations in the event of a disaster or major disruption. It provides a roadmap for an organisation to effectively respond, recover, and resume normal operations following an incident. As per MeitY[50] guidelines on Disaster Recovery Best

[49] Technopark Campus, Thiruvananthapuram.
[50] Ministry of Electronics and Information Technology, Government of India.

Practices, while documenting DR Plan, Departments should take a holistic view and focus on recovering the application services and not just servers. The technical recovery plan for each application/ service should be documented in a way that all the activities that need to be performed during recovery should be defined in a sequential manner.

Audit observed that the Department has not formulated and documented any Disaster Recovery Policy or Business Continuity Plan**.**

Government stated (November 2024) that Disaster Recovery Plan is being prepared as part of ISO 27001 Certification process.

Recommendation No. 43

Government should fix a time frame for Disaster Recovery Plan.

8.9.3 Non-conducting of Disaster Recovery drill

DR Drill is a routine activity done by an organisation to check if there is business continuity in case the Data Centre is down due to an unexpected event. Conducting a proper disaster recovery drill involves a systematic and well-planned approach to simulate a real disaster scenario and test the effectiveness of the treasury's disaster recovery plan.

Audit observed that there was no record of periodic test check conducted to determine whether recovery plans would work in case of any disaster. Details of training to IT personnel to respond effectively in emergency situations were also not produced.

Government stated (March 2023) that DR drill was conducted on 09 July 2022 by shifting the database connection to the Near DR location at SDC-1 and work on it and switch back to Production site (SDC-2). A full-fledged Near DR implementation work is going on a war footing. Once it is implemented, the treasury operation can resume in a short time from Near DR if the production DR at SDC-2 fails.

Recommendation No. 44

Periodic DR drills may be scheduled, conducted and recorded and post-drill analysis may be undertaken to review the lessons learned.

8.10 Ineffectiveness of software error reporting mechanism

Department of Treasuries introduced (August 2020) a software error reporting mechanism wherein error reporting was colour-coded as Red, Yellow and White Reports with descending order of importance of software issues and urgency for remedial action as stated below:

- Red report- Software issues of serious nature or issues relating to financial transactions that demanded immediate corrective and preventive action or there would be damage.

- Yellow report- Important software issues both financial, non-financial that require appropriate software intervention, but demand no immediate corrective and preventive action as there is no immediate damage due to the existence of the issue.

- White Report- Suggestion for software modification and upgradation for enhancing system efficiency and quality of service delivery and suggestion and information on best practices.

The reports e-mailed were to be prominently superscribed indicating the category of report so as to ensure priority action on such reports. The reports were to be finally addressed by Information System Management Cell (ISMC) who shall maintain a register for recording and monitoring the software changes reported to NIC.

Audit observed that most of the communication regarding software issues were unofficially dealt with. Neither the pendency of tasks nor details of issues raised could be ascertained. It was also observed that though a mechanism of error reporting existed in the treasury, there was no mechanism in Department of Finance to deal with the same.

Government stated (March 2023) that all software issues reporting from treasuries are classified as Red, Yellow and White according to their importance. A register is set up for this purpose. Also, the issues reported are recorded through the e-office file system and necessary steps were taken for resolution.

The reply is not tenable. Audit scrutinised the register maintained at Directorate of Treasuries and found that only one entry has been recorded. Further, no e-file has been opened exclusively for error reporting. Moreover, the e-office file system is used for movement of online files. As such, through the e-office system, the ISMC would not be able to trace the pendency of tasks and details of all issues raised. Further, recording and monitoring the software changes could not be achieved through e-office.

Recommendation No. 45

A ticket based online issue reporting mechanism should be designed for entire suite of applications in IFMS-K, categorising issues based on nature and urgency and fixing timeline for resolution.

8.11 Absence of Database Administrator

Database Administrator (DBA) is responsible for performance, integrity, and security of a database. A DBA is essential in disaster recovery standpoint also. DBA has tools to establish controls over the database and the ability to override these controls.

As per clause 19 of the agreement with the supplier of DB2 database[51], they will provide training on DBA through IBM for three officials from Treasury department to get certificate on DBA. As per Government order (September 2013), NIC shall provide one exclusive DBA from NICSI for one year from the date of installation and the trained DBA shall be with department for a period of five years.

[51] M/s RP Techsoft International Pvt. Ltd.

Audit observed that Treasury department did not nominate anyone for the training and hence there is no certified DBA in the department. Instead, the department hired DBA from M/s RP Techsoft International Private Limited on a monthly payment basis. The service of DBA was discontinued by M/s RP Techsoft International Private Limited from 16 August 2019 and the post of DBA has been vacant in the Treasury Department since August 2019. Since then, the Department is depending on NIC for DBA activities.

Government stated (March 2023) that seven treasury officials were given basic training in DBA for six days with the support of IBM and it is expected that DBA services may be made available through them gradually. Moreover, in a recent tender process, the department hired 50 Man Day support as DBA for 12 months without any extra cost *w.e.f.* 01 February 2023 from another vendor of IBM.

The reply is not tenable as for a database where transaction data is of critical financial nature and of high volume, the availability of full-time, fully trained and experienced DBA who can operate database in a secure and error-free manner is essential.

8.12 Non-levy of liquidated damage charges from Database Administrator service provider

Government granted (January 2019) permission to hire the service of Database Administrator provided by M/s RP Techsoft International Pvt. Ltd. (at the rate of ₹85,000 + GST per month). The period of contract was for one year from 24 October 2018 to 23 October 2019. Clause 9.1 of Agreement with M/s RP Techsoft International Pvt. Ltd. stipulates that, the contractor should invariably provide a suitable substitute in the event of the incumbent DBA leaving the job due to his personal reasons. Any delay in providing a suitable substitute beyond three working days would attract liquidated damages at the rate of ₹10,000 per day on the contracting agency.

Audit observed that even though the service of DBA was discontinued from 16 August 2019, Treasury department did not take any steps to levy liquidated damages from the contracting agency. The failure of the Treasury department in levying liquidated damages for the delay of 66 days[52] from the firm had resulted in loss of ₹6.60 lakh to Government.

[52] 16 August 2019 to 23 October 2019.

Government stated (November 2024) that the matter had been brought to the notice of the firm and steps in connection with availing the refund is in progress.

Recommendation No. 46

Government may expedite follow-ups with the firm and promptly recover the amounts due by enforcing contractual obligations.

Thiruvananthapuram,
The 10 June 2025

(VISHNUKANTH P B)
Accountant General
(Audit II), Kerala

Countersigned

New Delhi,
The 01 July 2025

(K. SANJAY MURTHY)
Comptroller and Auditor General of India