Chapter 4- Review of IT Security

Audit Objective 3

To review the IT security mechanism to ensure that it was capable of reasonably protecting all business critical information and IT assets from loss, damage or abuse.

To review the Disaster Recovery Plan (DRP) /Business Continuity Plan (BCP) to ensure the continuity of the organization's business in the event of unforeseen events.

Crew Management System is a part of the Freight Operations Information System (FOIS) having interface with other modules/applications of FOIS and covers important activities such as assignment and booking of crew for various trains, validation of competency of crew for train operations and captures critical data which is very important for safe train operations. Apart from that, CMS also manages data pertaining to various allowances of crew. As such it is very important to adopt adequate preventive, detective and corrective measures to protect CMS for its confidentiality, integrity, availability and to ensure safe, smooth, timely and continued train operations.

Railway Board formulated its Baseline IT Security Policy in April/May 2008 within which subsidiary procedures and instructions were to be drawn by CRIS/zonal railways/individual units. The Baseline IT Security Policy addresses different aspects of IT Security including environment and location security, equipment security, physical access control, data access right, user identification and privilege management, password management, Business Continuity Plan, data backup, application development and maintenance security, protection against virus and malicious software, internet/email security, software and patch management etc.

Audit has noticed that subsequent to the RB's Baseline Security Policy, no IT Security Policy or subsidiary procedures and instructions relevant to CMS have been drawn over 13 ZRs[63]. In reply, Railway Administration of NR, ER, SECR and SER reported that the matter pertains to CRIS/ CAO (FOIS) office.

However, Audit of CMS application security was conducted broadly keeping in view the IR's Baseline IT Security Policy/CRIS Information Security Policy. Audit observations in this regard are as under:

4.1 Physical Access controls

Physical risks to the system include physical damage, theft and disclosure/copying of information. Physical controls of IT systems ensure prevention of unauthorized access to IT system or their malfunctioning.

[63] ***SR, CR, NWR, NR, ER, NER, SWR, NCR, SECR, WCR, SCR, WR and SER.***

As per IR's Baseline IT Security Policy, computer rooms should be restricted area, only authorized persons should be allowed entry into the premises and suitable access control system should be put in place. All visitors to the computer rooms should be monitored all times by an authorized member of the Railway staff.

During the visit to various lobbies of 12 ZRs[64], it was noticed that adequate measures[65] were not adopted to prevent and detect the entry of unauthorized persons to lobbies and to protect the IT Assets from theft/damage. Over different zones, detective security measures like CCTV cameras were either not installed or inadequate number of CCTVs were installed as details given in ***Appendix XXV.***

In reply (September 2015), RB stated that necessary instructions have been issued to the zonal railways.

CMS Users: CMS is used at different levels by different types of users having different privileges. It is mainly used by System Administrator, Database Administrator, Database user and Software (Application) Access users. The Software Application Access users include Super user for creating Supervisor user for lobby, Supervisor user (Loco/Traffic) for creating Train Clerk (TNC) user for lobby and for approving sign on/off, TNC user for booking of crew on various Traffic Advices and Crew Console user for Kiosk which enables every Crew Console user to access CMS through Kiosk for sign on/off, viewing his personal details etc.

As per Baseline IT Security Policy of IR, every user ID should uniquely identify one user. Group or shared user ID should not be created unless permitted explicitly and approved by the Department IT Security Manager. Each password should have a minimum length, restricted words/format and a validity period among other restrictions. All information system privileges should be revoked at a time a member is transferred or ceases to serve railway. Moreover, data access rights should be granted on need to know basis. In this regard, audit observations are as under:

4.2 Logical Access control – password policy

A system in the form of software control aimed at protecting computer resources (data, programs etc.) against unauthorized access is classified as logical access control. In this regard, following issues were noticed in audit:

[64] ***WR, SWR, ER, SR, SER, NWR, SCR, ECoR, NCR, NER, ECR & WCR***
[65] ***Like Electronic Door Lock, Bio-metrics Door Lock, Swipe Card, Security Guard etc.***

Password Policy

As per CRIS's Information Security (Password) Policy, password length should be minimum six characters for user account and 10 characters for Administrator account and should be a combination of upper and lower case characters, digits and permitted special characters.

- Test check revealed that CMS neither ensured a password consisting of lower/upper case characters, digits and special character nor ensured minimum 10 characters password for System Administrator/Database user and accepted minimum six character simple password such as '123456'. At application level, CMS allowed single character user ID as well as password to enable crew to login/access the system, without forcing change of password at first login and periodical change of password.
- Analysis of data pertaining to different types of users revealed as under:

User Type	Details
Crew Console User (Drivers/Guards)	Between 11.91 *per cent* and 100 *percent users* of all ZRs were using same password which, though in encrypted form, was the default password.
Loco Inspector/Senior Loco Inspector/Chief Loco Inspector	Between 74.01 *per cent* (SEC) and 98.53 *per cent* (ER) users of all ZRs were using same password.
CMS Users (Supervisor/TNC)	Between 36.68 *per cent* and 87.82 *per cent* users over all ZRs were using same password.

In view of the fact that user ID is visible to all and password can also be easily guessed, possibility of unauthorised access/login by proxy users cannot be ruled out as is further evident from the facts mentioned under paragraph number 2.5.4.5 in the report that a crew was found logged in during his absence.

Thus, the basic security measures, prescribed in the IR's Baseline IT Security Policy/CRIS Information Security Policy, were not adopted to ensure security and safety of CMS resources.

In reply (September 2015), RB admitted audit observations for remedial action.

(Annexure – 35, 36, 37)

4.3 Poor User Profile Management

Administrative/supervisory privileges were assigned to dummy users and privileges assigned were not commensurate with the requirement of user's designation, supervisory privileges were compromised and this could lead to loss of data integrity/misuse of system and wrong booking of crew. CMS users were created in obscure/lobby names and outsourced staff was not given separate user ID. This may lead to failure in identifying the actual person who populated the data, failure in fixing responsibility for wrong CMS operations. Audit observations/Instances of irregularities noticed in this regard are as under:

- **Irregular privileges to outsourced staff:** Over SR, data feeding in CMS at crew booking lobbies[66] was outsourced through a contractual agency but no separate user IDs and passwords were allotted to outsourced staff and common user id and password was shared by every CMS user in a lobby.
- Over SCR, in 1,16,383 cases, the person who booked the crew also accorded supervisory approval which indicated that in most of the cases the outsourced staff had granted supervisory approval which was in violation of the prescribed procedure and, therefore, irregular.
- Over ER, all the staff including outsourced staff of lobbies test checked used common user-id and password.
- **Irregular privileges to railway CMS User**: During data analysis, audit noticed over different zones that Administrative/Supervisory privileges were assigned to non-existent/dummy railway users or the privileges assigned were not commensurate with user's designation. Users were found created in obscure/lobby name which did not disclose identify of the actual user. ***(Appendix - XXVI)***

(Annexure - 38)

- **Different roles/functions performed by CMS users, using Supervisory ID**

  As per CRIS's CMS documentation, different roles have been provided for Train Clerk and Supervisor and the same are supposed to be performed by actual users.

- As per CMS User Manual, Supervisory function of approving sign on/off activity of crew is to be performed by crew Supervisor. An analysis of data pertaining to crew calling, booking and approving their sign on revealed that over 11 ZRs[67], out of 2071319 cases, in 669393

[66] ***Tambaram, Chennai Egmore, Chennai Central, Tiruvottiyur, Arakkonam and Jolarpettai***
[67] ***ER, NR, NWR, WR, NFR, CR, SCR, SER, SECR, SR, NCR***

cases, User IDs of Calling Clerk, Booking Clerk and Supervisor were the same.

(Annexure - 39)

- During lobby visits of Delhi division of NR, it was noticed that unified[68] user IDs were created for performing CMS operations and at majority of the lobbies, Assistant Loco Pilots/Loco Pilot Shunters (ALP/LPS) were using unified[69]user ID and password of their Crew Controller/Supervisor for crew booking and approving their sign on/sign off. Similar position was also noticed over SR, SWR and other zonal railways.

  Thus, non-performance of Supervisory functions by actual user could be affecting the operations of CMS as brought out under paragraph numbers 2.5.4.5, 3.1 etc. and thereby security of the system was also compromised which may expose the train operations to risk.

- **Creation of multiple user IDs (multiple profiles) and non-deactivation of CMS Application users account**

  A analysis of the CMS users data as well as scrutiny of CMS operations/records at lobbies revealed that users had multiple IDs, users created were in excess of the requirement, ex-officials were active as CMS user as is evident from the details given in ***Appendix-XXVII.***

  Thus, database of users has not been timely updated and can be misused by using IDs of ex-officials.

4.4 Non-monitoring of activities of Database Administrator (DBA)/Lack of audit trail

CMS development and maintenance functions are performed by CRIS CMS group at New Delhi which includes, among other functions, programming the application, testing of development/modification of software, managing database/updating database, managing users etc.

As per the information made available to Audit, seven users have DBA privileges. Further, 40 CRIS users had Administrative privileges at application level and one of them had Administrative privileges with multiple ID. Users having DBA privileges can access the CMS tables and effect modification in the database from backend without any monitoring of their activities as neither any logs/audit trail for monitoring activities of DBA were maintained nor other measures like restricting the access to single person were adopted to avoid any unauthorized and undetected changes in the database.

[68] ***A user having privileges of Supervisory functions and Train Clerk functions***
[69] ***A user having the privilege of Supervisor and Train Clerk (TNC)***

Absence of requisite logs/audit trail or other corrective measures (like restricted access) would result in failure to monitor/track unauthorized activities of users having Administrative privileges.

In reply (September 2015), RB endorsed CRIS remarks that audit observations have been noted for necessary action.

4.5 Non-installation/Updation of Antivirus and Operating System Patches

As per CRIS's IS Policy, System Administrator of respective groups/Users should ensure that appropriate anti-virus software[70] and latest Operating System (OS) patches[71] are installed in server and other component managed by them and are timely updated. Moreover, as per IR's Baseline IT Security Policy, Antivirus should always be enabled and regularly updated on personal computer and computers connected with internal network via remote access channels.

- A review of the CMS on 2nd March 2015 revealed that Windows OS based server did not have updated antivirus software (anti-virus last updated on 24th February 2015).
- Patches on servers having Linux/AIX OS were last updated/installed on 27 January 2012.
- Thin clients/Windows based PCs were in use over different zones for CMS operations. Over SR, the version of antivirus software used (Quick Heal Anti-Virus Pro 2014) in the selected Kiosks was outdated and not renewed since 4th May 2014. Over SCR, anti-virus software was in use in the CMS machines of Hyderabad (HYB) lobby but not in the CMS machines of Secunderabad (SC) lobby. At Jind lobby of NR, PCs in use for booking had trial version of anti-virus.
- Anti-virus software was not installed/updated in the CMS machines of lobbies over CR, ER, ECoR, NCR, NER, SER, NWR, SWR and ECR selected for Audit.

Thus, lack of updated antivirus software/updated software patches can be exploited and lead to disruption of smooth CMS operations.

4.6 Deficiencies in Business Continuity Plan/Disaster Recovery Plan (BCP/DRP)

The objective of producing and maintaining a BCP/DRP is to ensure the integrity of the organization's IT assets and to reduce the risks

[70] Anti-virus or antivirus software is computer software used to prevent, detect and remove malicious software.

[71] A patch is a piece of software designed to update a computer program or its supporting data, to fix problem or improving the performance of the system. This also includes fixing security vulnerabilities.

arising from unexpected disruption of the critical systems and to have continuity in business activities.

CMS system has a centralised Computer Data Centre at New Delhi which is being managed by CRIS since inception of the system from 2007-08. CRIS started the process of having a BCP/DRP in June 2012 for ensuring uninterrupted operations of CMS and till the end of January 2015, the work of implementation of BCP/DRP was still under process.

At zonal/divisional/lobby level, all ZRs did not have a structured and documented BCP/DRP. Route and media diversity/alternative communication channels for ensuring 24x7 connectivity were not available at lobbies of different zones. Connectivity/link failure, slow speed of network between central server and CMS client machines were the main reasons for disruption of continuous CMS operations over lobbies of different zones.

Arrangements for alternative power supply were not adequate at a number of lobbies. CMS equipments/devices were not covered under AMC at majority of the lobbies.

Working spare equipment/devices were not available for immediate replacement of defective equipment at different lobbies.

Fire Extinguishers had outlived their shelf life/were not installed and Smoke Detectors/Fire Alarm Systems were not installed. ***(Appendix - XXVIII)***

In reply (September 2015), RB endorsed CRIS remarks that their Disaster Recovery setup at local site (Data Centre/production environment) has been commissioned.

The reply of RB is not acceptable because only phase-I of the CRIS DR Plan has been commissioned at local site (viz. Data Centre/Production environment) and phase-II of the DR plan for having a DR site at remote location has not been implemented. As the local DR setup (as well as Data Centre/Production environment setup) is prone to a number of risks which may not achieve the objective of having a DR site for continued CMS operations on 24x7 basis, the implementation of phase-II of DR Plan needs to be expedited for having a DR setup at remote location.

Moreover, the need of providing adequate infrastructure and adopting corrective and preventive measures at different zones has not been addressed which has either resulted in or could result in disruption of continuous CMS services.

4.7 Non/Irregular Maintenance of CMS data backup

As per CRIS IS Policy, all projects are required to maintain remote/offsite back up of data for ensuring continuous operations of various railway projects. CRIS's CMS group, which is maintaining centralized database of CMS, did not have any formal Documented Backup Policy addressing issues like identification of criticality of the data/information, procedures for backing up data, verification of backed up data for ensuring its integrity and timely recovery, security of the onsite/offsite data backup, period for maintenance of backed up data etc.

As per the duty list defined for various CMS group members, daily back up and weekly backup of data was to be maintained by CRIS. As per audit review of Backup process being followed by CRIS in January 2015, daily backup was not being taken up. CRIS was also not maintaining any remote site backup. Backup of CMS was stated to be tested randomly but due to lack of records/logs as to when the testing was done, this aspect could not be verified.

Thus, lack of any proper Data backup procedures in the CMS system entails the risk of jeopardizing the operation of CMS in the wake of emergent situations.

In reply (September 2015), RB endorsed CRIS remarks that remote site backup will be maintained.