Chapter 4 IT Security

Audit Objective III– Review the IT Security to check the extent to which it is capable of reasonably protecting business critical information and assets from loss, damage or abuse

4. Railway Board formulated its Baseline IT Security Policy in April/May 2008 according to which subsidiary procedures and instructions were to be drawn by CRIS/Zonal Railways/individual units. The Baseline IT Security policy addresses various aspects of IT Security including Contingent Management Planning, use of licensed software and its updation, back-up policy, password management, version control mechanism, protection against virus/malware, setting up of IT Security Monitoring Teams and Incident Response Teams, environment and location security, equipment security, physical access control, data access right, user identification and privileges management, application development and maintenance security, internet security etc.

Audit of ICMS application security and related issues was conducted broadly keeping in view the IR Baseline Security Policy/CRIS IS Security Policy and best practices in IT environment. Audit visited 128 locations over various Zonal Railways and observed that:

4.1 Physical Access Control

Access of unauthorised persons at the ICMS locations visited by Audit was not restricted in SR[1], SWR[2], NR[3], NCR[4], NER[5] and ECoR[6].

4.2 Logical Access Control - User and Password Management

4.2.1 Though passwords of the users were recorded in encrypted form, answers to the security questions for reactivation of user accounts were captured in legible form as observed in four[7] Zonal Railways. Even registration passwords of the users were in legible form[8].

4.2.2 Password and user ID of the users created by CRIS were not communicated to CAO/FOIS office confidentially, but by writing them on the request letter itself, thereby compromising the password security.

4.2.3 The login page of the ICMS did not restrict the number of attempts of login by users. In the absence of strong password controls, unlimited login attempts make it easier to break-in into the system using random password generator software.

4.2.4 As per IT Security Policy of IR, the system administration password

[1] At all selected locations visited during Audit
[2] At three ICMS locations at Hubli, Mysore and Vasco
[3] At all the selected ICMS locations of Delhi, Ambala and Firozepur divisions visited during audit. At Delhi Divisional Control Office CCTV camera were installed but bio-metric system was not found in use.
[4] At all selected locations visited by Audit
[5] At all the selected locations visited by Audit
[6] At two locations visited by audit [Waltair Control and Bhubaneswar (FOIS) Cell]
[7] NFR, SCR, CR, NR, NER
[8] NR, SCR, CR, SECR

should be a minimum of 10 characters and should be a combination of alpha numeric and special character. It was however, noticed that password standards being followed by CRIS ICMS group at Centralized Data Centre did not conform to the laid down IT Security Policy.

4.2.5 Creation dates of 22 users preceded their start date by 1 to 30 days and Start date of 245 users preceded their creation date which did not appear logical and indicated lack of adequate controls.

4.2.6 Requests for creation of user ID were entertained by NR Headquarters office over telephone. Records relating to authorisation for creation of user IDs and password were not available at Zonal Railway Headquarters in NR.

4.2.7 Over NR, at six ICMS locations, ICMS users were created in excess of requirement when compared to the number of ICMS terminals and the operational shifts of the users. There were five users at New Delhi location and ten users at Delhi Main location, but 26 and 71 active users were created in ICMS.

4.2.8 Over NR and SCR, 47 active users having same mobile number and date of birth had two to four user IDs. Rest of the particulars like Secret Question, Name, Address etc. were either almost same or had minor variations which indicated that the different user IDs pertain to the same person. Thus, the system lacked controls to ensure creation of unique ID for each user.

4.2.9 Users were created with vague names like Mr.lko, Mr.umb, Mr.dlli, Mr.CCM Database, Mr.PRC, Mr.KCG, Mr.CRSE, Mr.HYB, Mr. DRM_NAG, Mr. CTE, Mr.secrcme, Mr. CEGE, Mr. CSTE-SECR etc.(location/designation names) in the user master table (NR, SCR, SECR).

4.2.10 A number of incorrect/irrelevant user types such as 'DC' and 'SC' were found in the master table[9] containing user details without any description of such types of user in the database.

4.2.11 Users who had crossed superannuation age were found active in the system. Users below the age of 18 years (viz. born after 1 November 1997 and were between nine to 15 years) were also active. This indicated that the users' date of birth was not validated at the time of data capturing.

Over NR, test check at ICMS locations also revealed that at Zonal Headquarters office, Ambala, Ambala Control office and New Delhi, User IDs of retired/transferred officials were still active. Superannuated active users in NR were application users and also had privilege to modify application data.

4.2.12 Details of users were incomplete and details such as state, mobile number, railway phone number, ICMS email ID, designation, secondary email ID, address fields were left blank. The data was, thus, incomplete and not usable when required. (NR, SCR, NER, SECR)

4.2.13 One user ID/password was shared by three train clerks posted at Jodhpur (NWR). User IDs and associated passwords authorized for specific personnel at ICMS locations at Chennai, Chennai Egmore and Basin Bridge Jn. of SR were

[9] MT_Users table

shared by more than one person. Four train clerks working at ICMS control office of Allahabad (NCR) had no individual user IDs/passwords and were using a common login ID/password. Over NR, WCR and SCER, each of the 13 locations[10] had just one User ID and each of the seven locations[11] had just 2 active User Ids. During location visits, it was noticed that all the users did not have exclusive user ID in NR[12].At Anand Vihar, on 18 April 2016, ICMS ID of a user[13] was in use even though she was not on duty during the morning shift. Over NER, user ID of a transferred official was in use at Kathgodam ICMS location.

4.2.14 Out of 26 active ICMS users created on CRIS accounts, having administrative privileges, 25 were active super users[14]. These users also included those who were transferred from CRIS ICMS group to other CRIS group(s), but were still active ICMS users with super user privileges. The super users with administrative privileges also included two dummy users created in the name of ICMSIRCA and PRSCHART. This indicated that no control was exercised to restrict access to ICMS in sync with the laid down functions/responsibilities/ duties of the users. This was in contravention to the IT Security Policy.

4.2.15 Analysis of ICMS Users' Registration Data revealed that 335 users were allotted registered code without user IDs to access the system. Out of these, 330 users were granted application level/report level access and 253 users had privilege to modify data of one or more modules of ICMS. Review of User Master Data revealed that nine users did not have registration code which included active users and superannuated users.

4.2.16 In 147 cases,[15] users log-in time to various ICMS modules was 3 days to 523 days old and users had not logged out from ICMS. It was further noticed that data in ICMS was being populated by users who had logged in but had not logged out from ICMS for a long period of time and their password had also expired. Though it was observed that ICMS forced a user to automatically log-out after a specific period of inactivity, as per ICMS database, these users were not automatically logged out even after logged-into ICMS for a period of 3 to 523 days.

Analysis of data[16] pertaining to users' session details as well as last login details revealed instances where user logout time preceded user login time. (NR, NER, WCR, SCR)

4.2.17 There was no record of login/logout of 407 active users[17] in the table containing user's Last Login details.

4.2.18 In response to audit query, CRIS provided designation wise duties and responsibilities of CRIS ICMS team rather than details of duties and responsibilities of individual official. Thus, it could not be ascertained whether

[10] Meerut, Panipat, Patiala, Alambagh (NR) and six locations of SECR, three locations of WCR
[11] Jagadhari Workshop, Jammu Tawi, Hussainpur (NR), three locations of SECR, one location of WCR
[12] Anand Vihar, Ambala (CPRC and CTLC), Delhi Control (Coaching stock and CTLC), Jagadhari Workhops, Jammu Tawi, Delhi Sarai Rohilla
[13] Ms.Sushma
[14] A user having special privileges including privilege to create/manage new/existing users
[15] NR-84, WCR-15, SCR-48
[16] DT_Session and DT_Last_Login_Info
[17] SCR-80, SECR-5, NR-207, NER-115

duties and responsibilities of each official was segregated/separately defined.

4.3 Change Procedure/Management

As per IT Security Policy, all the IT Groups were required to develop procedures for effecting changes in the application software. However, ICMS group had not developed/formulated procedures for effecting changes in the ICMS software. As per the test check of CRIS records relating to changes made in the ICMS, no system/procedure for getting appropriate approvals before releasing the changes made in the ICMS in the online environment was found in place.

4.4 ICMS Documentation

As per the information made available by CRIS, CRIS has a User Manual on ICMS, Software Requirements Specifications (SRS) on COIS and System Design and Development (SDD) on COIS. CRIS did not provide any documentation on User Requirement Specification for PAM and COIS. CRIS also did not provide SRS for PAM. Even the SDD on COIS did not contain complete details of all the tables in use in COIS module including their table structure, linkage between various tables, description of various fields of ICMS tables, description of values used for various fields. User Manual was updated till December 2014 and was not found complete as it did not have details of the various reports generated by ICMS including their format, details of codes used in various reports, period for which various reports make ICMS data available to users etc. (NR, ECR)

4.5 Business Continuity Plan

4.5.1 Business Continuity Plan at CRIS Centralized Data Centre

ICMS is a Centralized Application and all the servers (Database server, Application Server, Web servers etc.) were installed at CRIS Headquarters office at Chanakyapuri, New Delhi. In order to ensure continuity of ICMS operations, CRIS started the process of implementing the Business Continuity Plan during 2011-12. In November 2015, CRIS submitted an Abstract Estimate for Disaster Recovery (DR) setup of ICMS application at a cost of ₹ 12.04 crore to Railway Board. As on 31 March 2016, the process for DR Setup was still going on.

In response to Audit query, CRIS stated (February 2016) that ICMS Data Backup Security Policy for new system, installed in October 2015 was under progress and review. It was further noticed that though daily back up was being taken up by ICMS team but no off line/remote site backup of ICMS was being maintained by CRIS ICMS group.

4.5.2 Business Continuity Plan at Zonal Level

No documented Business Continuity Plan was available in SWR, NCR, SCR, ECR, ECOR, ER, WR, NER, SER, NWR & SR. CRIS had procured new ICMS servers in February 2015. Though the server was made online in October 2015 the installation process was yet to be completed (March 2016). The following deficiencies were observed in the ICMS locations checked in audit:

(i) Personal computers/desktops were used in ICMS locations of WR, SR, NR and NER instead of thin clients. At NCR and ECR, thin clients were

provided initially but these were subsequently replaced by desktop computers, making the system vulnerable to security risks and virus attacks, in the absence of anti-virus.

(ii) Antivirus software was not in use over NER and NR[18] at most of the ICMS locations visited by Audit team and antivirus software was not found updated in CR.

(iii) ICMS systems were not covered under Annual Maintenance Contract over SCR, SR, NR[19]. At ECR, warranty period of six PCs (out of 17) had already expired on 31st March 2016 and AMC for these six PCs with any of the agency was not found to be executed till date of audit. Codal life of three Thin Clients had expired on 31 March 2016 and process for replacement of these thin clients was yet to be started.

(iv) Smoke detectors, fire extinguishers were not found at ICMS locations in NCR (5)[20], SR[21], ER[22], SCR[23], NR[24] and NER[25].

(v) Dust/waste bins (fire hazards) were found to be placed inside the premises housing systems on which ICMS was installed and running. In the event of fire breaking out due to short circuit, sharp energy variations etc. there were no extinguishers available to douse the fire so as to save the information system assets (SR).

(vi) As per Railway Board orders/instructions, media and route diversity is to be provided in all the FOIS projects to ensure continuous and smooth operations. Over NR, at almost all the locations visited by Audit, ICMS connectivity was provided by FOIS network but at none of the locations, standby/redundancy lines were made available. Users reported [26] connectivity problems. Records for Link/Connectivity Failure/Problems was not maintained over NR[27] and CR[28]. In SR though failure report register was being maintained in the ICMS locations test checked and the register contained information about network failure, system failure etc. details regarding rectification of failures, actual down time of the system were not available in the register.

(vii) No UPS were provided at four ICMS terminals[29]. UPS provided at five locations [30] were not in working condition/had no power backup. Adequate and proper furniture was not provided[31].

[18] Except at Ambala (CTLC) where an free version of anti-virus was in use.
[19] Ambala (CPRC), Delhi(CTLC), Jagadhari Workshops, Jammu Tawi and Amritsar
[20] While Smoke Detectors were not available on all the locations, fire extinguishers were found at all the locations
[21] Smoke Detector and Fire Extinguisher not available at all locations visited.
[22] Smoke Detector was not available at all locations visited and fire extinguisher was not available at HWH/TNC
[23] Fire Alarm/Smoke Detector was available at 2 locations and fire extinguisher were available at all locations
[24] Except UMB Control office
[25] Smoke Detector were not found at all locations visited by Audit
[26] At New Delhi, Delhi Control office (CPRC), Anand Vihar, Ambala Control office (CPRC), Delhi Sarai Rohilla, Jammu Tawi
[27] At Mumbai CST and Mazgaon of CR and at locations visited by NR Audit team except at Train Branch at Delhi and Anand Vihar
[28] Mumbai CST and Mazgaon
[29] At Delhi Control office, Train Branch of Anand Vihar, Jammu Tawi, Amritsar
[30] At Train Branch of Delhi Sarai Rohilla, New Delhi, Delhi, Ambala and Mazgaon
[31] At Control office of Ambala, Delhi (Coaching section), Train Branch of Anand Vihar, Ambala, Jammu Tawi, Delhi, Delhi Sarai Rohilla, Amritsar, Mazgaon Yard

(viii) Over NR, SCR and CR, dust free environment was not available at 12 locations[32] and air conditioners were not available at 11[33] locations.

(ix) Water seepage problem was noticed at Train Branch at New Delhi, Delhi Main and Amritsar locations of NR and Guntakal of SCR which could adversely affect smooth ICMS operations.

Thus, the IT Security was deficient and physical and logical access controls needed strengthening. Change Management was not documented as per IT best practices and Business Continuity Plan was yet to be fully implemented.

During Exit Conference (October 2016), Railways agreed that access control is a weak area and they needed to work on strengthening the same. Railway Board also agreed to the audit observations. As regards audit recommendations, Railway Board stated that audit recommendations are useful and Railways would act upon them to improve the system.

[32] At Train Branch of Anand Vihar, Delhi Sarai Rohilla, Delhi, Ambala, Jagadhari Workshop, Secunderabad, Vijayawada, Guntakal, Guntur, Mumbai CST, Dadar Terminus, Mazgaon

[33] Anand Vihar, Delhi Sarai Rohilla, Delhi, Ambala, Jagadhari Workshop, Jammu Tawi, Amritsar, Mumbai CST, Dadar Terminus, Lokmanya Tilak Terminus, Mazgaon