Chapter 2
Other computerised applications in Indian Railways

2.1 IT Security on Western Railway

2.1.1 Highlights

Even 20 years after implementation of computerised applications in Western Railway, IT security policy was not laid down. Both the physical and logical access controls were inadequate exposing the systems to unauthorised access and malicious software. Western Railway Administration did not conduct any threat based risk assessment for systems and data. An independent vulnerability assessment by Audit using the tool NS Auditor revealed as many as 274 vulnerabilities, out of which 197 were of high risk.

(Para Nos. 2.1.6.1 and 2.1.6.3)

Network security was inadequate as open ports were found in personal computers in Western Railway rendering the systems vulnerable to viruses and worms and intrusion by hackers. There was no mechanism to monitor and control internet usage of users.

(Para No.2.1.6.2)

Physical and information assets in Western Railway were not classified and there was no mechanism to designate ownership of critical information raising questions on safeguarding of assets and classified information. Training in IT security was inadequate and internal audit of IT assets, application and its security were not conducted.

(Para Nos.2.1.6.4, 2.1.6.6 and 2.1.6.7)

2.1.2 Recommendations

- Western Railway Administration should develop a proper IT security policy and assess the risks and vulnerabilities on priority basis.
- Western Railway Administration should continuously monitor the network traffic and system usage and institute adequate security controls- both physical and logical to safeguard IT assets, systems and data from external and internal threats.
- Internal audit of IT systems should be conducted. IS security training should be adequately imparted. Physical and information assets should be classified based on their sensitivity.

2.1.3 Introduction

IT Security encompasses understanding and management of risks involved, managing the network traffic and security, safeguarding IT assets, data, applications, infrastructure and personnel, selecting and implementing effective controls to ensure confidentiality, integrity and availability of the information and communication systems that store, process and transmit data. Dramatic increase in reported computer security incidents, ease of obtaining and using hacking tools, steady advance in sophistication and effectiveness of attack technology and the dire warnings of new and more destructive cyber attacks etc., could affect the Railway's computer system.

2.1.4 Audit objective

The audit of IT security of the computerised applications in Western Railway was carried out with a view to assessing whether adequate and effective information security controls were implemented to protect confidentiality, integrity and availability of the systems and data.

2.1.5 Audit scope, criteria and methodology

IT Security audit was confined to assessing the security program management, which provides a framework for understanding the associated risks and instituting effective controls for mitigating the risks, network security management, access and change management controls.

Standard Information Security practices were used as audit criteria to evaluate the IT Security in Western Railway.

Relevant records, reports and documents relating to IT assets were analysed. Network security was analysed using network security scanner. A questionnaire was used to obtain information with regard to IS Security policy and other aspects apart from discussion with the users.

2.1.6 Audit findings

The IT Security audit of computerised applications in Western Railway disclosed inadequacies in IT Security, network security and traffic management, lack of risk assessment, non-classification of IT assets and information, inadequate change management and training, absence of internal audit of IT systems and inadequate management of business continuity process as brought out below:

2.1.6.1 Inadequate IT Security

A proper policy framework for IT security embodies adherence to strict norms and procedures in the system for ensuring confidentiality, integrity and availability of reliable and authentic information. Moreover, critical or sensitive business information processing facilities should be housed in secured areas, protected by defined perimeter security with appropriate security barriers and entry controls. Precautions are also required to prevent and detect malicious software since both the software and information processing facilities are vulnerable to introduction of malicious software, such as computer viruses, network worms, Trojan horses and logic bombs. Audit observed that:

- Even after 20 years of implementation of computerised applications in Western Railway, IT security policy was not laid down by the Railway Administration. Absence of laid down security policy result in ineffective segregation of responsibility, absence of established performance centres and demarcated areas of operation.

- Physical security control weaknesses such as inadequate physical barriers and ineffective screening of visitors contributed to weakening the perimeter security at several facilities of the department exposing sensitive computer resources and data to unauthorised access.
- There was no mechanism to guard against internal threats (an action or event initiated by an employee or staff having valid access to information as part of performing his or her duties) to information security. In response to an audit questionnaire one (EDP centre) out of the seven departments stated that there was no loss caused by insider threats. A test check, however, disclosed that a temporary employee had misused the Passenger Reservation System (PRS) facility by issuing reserved tickets to passengers against seats already allotted to other passengers, which was discovered in the train when there were ten passengers for five seats.
- Inadequate logical access controls reduced the reliability of department's computerised data and increased the risk of unauthorised disclosure and modification. It was seen that IP addresses were misused by staff to access the internet network. A test check further disclosed that five out of twelve PC's connected to Railnet could be opened using the administrator's account without a password.
- Personal computers installed in various departments did not have the latest antivirus definition files nor were the staff aware of antivirus definition files to be downloaded through the internet. Railway Administration accepted that personal computers connected to Railnet were affected by virus.
- There was no filtering mechanism to restrict users from downloading malicious content on computers. This coupled with poor physical controls exposed the system to malicious software and rendered the system vulnerable to frequent break downs.

2.1.6.2 Inadequate network management

Network management includes management of network security and traffic. Network security management encompasses deployment, maintenance and monitoring of the effectiveness of network security controls to safeguard information and information systems and protect supporting network infrastructure. Effective network security management practices also require established and documented procedures that provide instructions for the system to restart and recover in the event of system failure in a short time. Further, to manage network traffic effectively network devices have to be configured correctly. Audit observed inadequacies in the network security and traffic management as brought out below:

- In a test check conducted on 12 January 2007 using GFI LANGUARD Network security scanner and on 08 June 2007 using Network Security Auditor (NS Auditor), it was noticed that ten ports were open in the personal computers connected to Railnet, exposing the users of the system to risks as mentioned below apart from penetration of viruses and worms in servers and personal computers and other intrusion by hackers.

Type of risk	Impact
Denial of Service on Port 135	The usage of Central Processing Unit (CPU) could be raised up to 100% by telneting to port 135 and irrelevant data/characters could be input.
OOB denial of Service	An attacker can send a custom packet causing the system to stop responding.
Teardrop denial of service	An attacker can send a custom UDP packet causing the system to stop responding.
Land denial of service	An attacker can send a custom packet causing the system to stop responding. The source code written in 'C' language is also available on the internet.

- Railway administration did not have a mechanism (either by installation of hardware or software) to monitor and control internet usage of users. On scrutiny of files, Audit noticed that some users of Railnet in Western Railway had downloaded and uploaded voluminous data (of 5.3 GB and 3.3 GB respectively) resulting in wastage of time besides denial of Internet service to other genuine users.

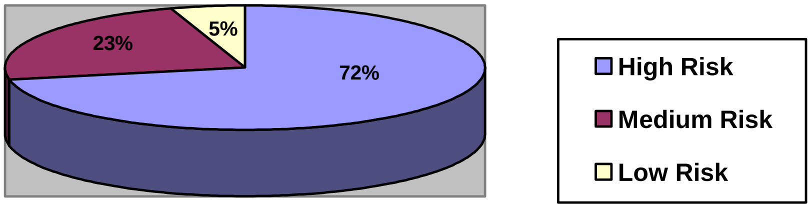
Railway Administration stated that there was no system to monitor the pattern of usage by individual users and as a result cyber slacking[1] could go uncontrolled.

2.1.6.3 Lack of risk assessment

Risk assessment is essential for risk management and overall security programme. This assists in identification of security risks and institution of effective controls. Audit observed that:

- Railway Administration has not performed any threat based risk assessment for systems and data. An independent vulnerability assessment by Audit in 3com switch (Host IP 10.3.3.103) using the tool NS Auditor revealed as many as 274 vulnerabilities, out of which 197 were of high risk (for e.g. Cross-site scripting, Avenger's News system command Execution, Directory transversal vulnerability, Remote command execution, Web_store and cgi etc) 63 were of medium risk and 14 were of low risk. Railway Administration accepted that automated tools were not identified to scan and monitor the network and host devices.

[1] practice of emloyees using the Internet or other employer-provided resources for leisure during work hours, contributing to inefficiency



2.1.6.4 Absence of classification of IT assets and information

Physical and information assets should be classified to indicate the need, priorities and to provide proper degree of protection. Information and physical assets have varying degrees of sensitivity and criticality. As per the IT Security standards, the information may be classified as unclassified, operational use only, private, restricted and confidential. Audit observed that:

- There is no centralised inventory of critical information and systems maintained by the Railway administration. Test check of the Stores & Signal &Telecommunication department revealed that inventory database was also not maintained department wise. In these circumstances, the Railway administration may not be in a position to do proper asset classification of the system based on the importance and sensitivity of the system/data in use, indicating lack of effective control.
- In spite of incurring expenditure of the order of Rs.32.06 crore during the last three years on acquisition of IT assets, the assets were neither classified nor was there a mechanism to designate ownership of critical information raising questions on safeguarding of assets and classified information.

2.1.6.5 Inadequate change management

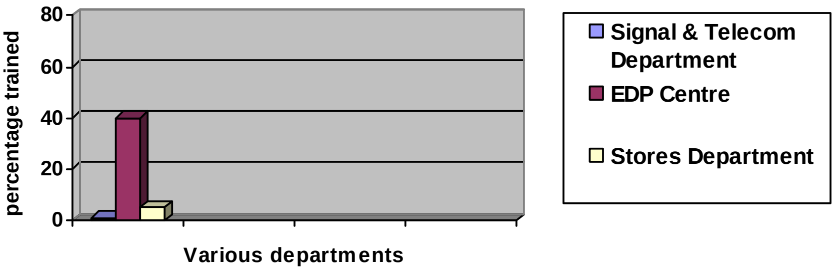
Established change management practices/ procedures are required to ensure that unauthorised changes are not carried out to the system. This should ensure only approved changes are incorporated in the programme and in time. Audit observed that:

- Changes in the system necessitated due to change in introduction of rules were not carried out in a timely fashion resulting in inconvenience to the traveling public as well as increasing the risk of loss of revenue to the Railways. For instance pursuant to Government of India notification of March 2006 regarding introduction of service tax on catering services on board the trains of Indian Railways, service tax for catering service on Rajdhani/ Shatabdi trains was not updated immediately in the fare structure resulting in short recovery of Rs.0.42 crore for the period from 1 April 2006 to 31 May 2006. Railway Administration stated that this has since (June 2006) been introduced after obtaining necessary instructions from Railway Board.
- No records were maintained to indicate the requests for change and the changes carried out in the system.

2.1.6.6 Inadequate training

An effective security awareness program is the means through which the organisation communicates the importance of security policies, procedures and responsibilities to its employees. Audit observed that:

- Out of three departments (Signal &Telecommunication, EDP centre and Stores), training in IT security awareness was imparted only in the EDP centre. Even in the EDP Centre, only 10 out of 25 employees were trained in security awareness. In the other two departments only basic training (use of Login & password) was imparted, which was inadequate.



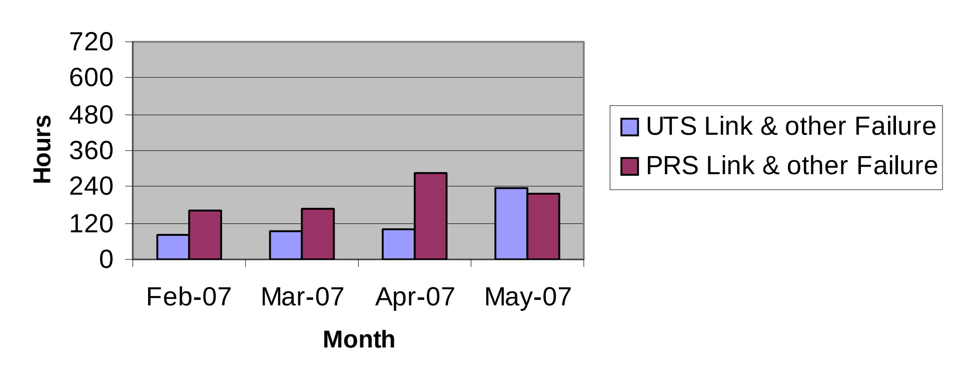
2.1.6.7 Absence of internal audit of IT systems

Internal audit assists in providing an assurance that safeguards are adequate and in alerting the administration to potential problems and threats. Audit noticed that Railway Administration has not covered internal audit of IT assets, application and its security in the annual inspection programme and hence internal audit of IT assets, application and its security has not been done so far.

2.1.6.8 Inadequate management of business continuity process

A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures to an acceptable level through a combination of preventive and recovery controls. The business continuity plan should be tested regularly to ensure that they are updated and periodically reviewed for their continuing effectiveness. Audit observed that:

- There was no managed process for developing and maintaining business continuity throughout the organization, regular testing and updating of the plan, formulating and documenting a business continuity strategy etc.
- Link failures in UTS and PRS were not addressed on time resulting in disruption of service. A test check in audit of link failure for a period of four months at major locations revealed that link failures ranged from 10 minutes to 54 hours (minimum at Vapi station and maximum at Vasai station) in UTS and from 10 minutes to 20 hours and 30 minutes (minimum at Malad station and maximum at Okha station) in PRS respectively. The link showed an increasing trend, reflecting that there was no appropriate contingency plan to minimise the impact of this failure.



2.1.7 Conclusion

The IT security of the computerised applications in Western Railway was grossly inadequate. Neither a comprehensive IT security policy was developed nor were the risks and vulnerabilities assessed. The network security and network traffic was not effectively monitored, information security and access controls were inadequate to protect the confidentiality, integrity and availability of the systems and data thereby exposing the IT systems to both external and internal threats.

2.2 Provident Fund Accounting System in Izatnagar Division of North Eastern Railway

2.2.1 Highlights

Business rules relating to accounting of Provident Fund transactions were not fully incorporated in the Provident Fund Accounting System in Izatnagar Division of North Eastern Railway leading to incorrect processing of transactions.

(Para No.2.2.6.1)

The Provident Fund Accounting System was not functioning concurrently with the Pay Roll System and therefore up to date balances of subscribers' PF accounts were not available.

(Para No.2.2.6.2)

Validation controls were deficient, which adversely affected the reliability of data. IT Security policy was not framed and weak access control mechanisms coupled with absence of audit trail rendered the Provident Fund Accounting System vulnerable to manipulation.

(Para Nos.2.2.6.3 and 2.2.6.4)

2.2.2 Recommendations

- North Eastern Railway Administration should modify the Provident Fund Accounting System to incorporate all the business rules relating to PF accounting. The system should also be integrated to function concurrently with the Pay Roll System.
- The deficiencies in validation pointed out should be rectified on priority. North Eastern Railway Administration should strengthen Information System security by drawing up a comprehensive IT Security policy and by strengthening logical and physical access controls.

2.2.3 Introduction

To facilitate correct and updated maintenance of Provident Fund (PF) accounts of 10,331 employees and payment of miscellaneous bills, North Eastern Railway Administration implemented computerised Provident Fund (PF) Accounting System in August 1998, at Izatnagar Division. The system is operational in the Divisional Accounts Office, Izatnagar under the control of Senior Divisional Financial Manager with 12 nodes connecting with one Pentium server on DOS platform and dbase as application software.

2.2.4 Audit objectives

Audit of the P.F. Accounting System implemented over Izatnagar Division of North Eastern Railway was conducted with a view to assessing whether the:

- System was developed in accordance with extant rules and provisions and data was reliable.
- Information System security was adequate and effective in regulating the IT environment.

2.2.5 Audit scope, criteria and methodology

IT Audit of the PF Accounting System was conducted for a period of four years and records for the period from 2004-05 to 2007-08 were examined. The extant rules and provisions in the railway codes were used as audit criteria to evaluate the system. Apart from examination of relevant records, data analysis was also carried out to arrive at conclusions.

2.2.6 Audit findings

The Information Technology audit of PF Accounting System implemented in Izatnagar Division of North Eastern Railway disclosed that the system was not designed as per business rules. Validation controls and Information System security were deficient, which adversely affected the integrity of data processed as brought out below:

2.2.6.1 Non mapping with business rules

Audit observed that business rules relating to accounting of Provident Fund transactions were not fully incorporated in the system leading to incorrect processing of transactions as shown below:

- Even though the rule provides that recovery of temporary withdrawal from Provident Fund should commence from the month following the month in which it was sanctioned, the provision was not built in the system. Consequently, it was noticed that the system could not commence monthly recovery from December 2004 for temporary withdrawals from Provident Fund sanctioned in November 2004 for 16 employees.
- As per provisions in the code, interest should not be granted to an account after six months of superannuation even if the final settlement on superannuation had not taken place. There was no inbuilt control to restrict the payment of interest up to six months of the date of superannuation.
- The subscription to PF should be rounded off to the nearest rupee, fifty paise and above being counted as the next higher rupee and less than fifty paise being dropped. Due to incorrect logic built in, the system was rounding off fractions of more than fifty paise only to the next higher rupee, which was inconsistent with the rule. It was observed that in the month of March 2005 and February 2006, there were 29 and 32 cases respectively where fifty paise was not rounded off to the next higher rupee. Only more than fifty paise was rounded off to the next higher rupee which resulted in less recovery.
- In PF Module, the length of the amount field of Voluntary Provident Fund (VPF) was fixed at four digits (‘9999’). Though admissible by rules, the system could not capture the actual contribution towards VPF of seven employees in February 2006, whose contributions ran into five figures i.e.; more than Rs.9999.

2.2.6.2 Delayed PF Accounting

The system was not functioning concurrently with the Pay Roll System and was trailing behind by three months. In the absence of simultaneous operation of both the pay roll and PF Accounting systems, up to date balances of subscribers’ PF accounts were not available.

2.2.6.3 Deficient validation checks

Audit observed that validation controls were deficient, which adversely affected the reliability of data as shown below:

- Details of subscription to PF, withdrawal from PF and interest accrued on PF of an employee are maintained through a unique Account number. Analysis of PF data revealed that in 50 cases the same PF number was allotted to more than one employee. Presence of such duplicate PF account numbers rendered the database unreliable with possible incorrect accountal of employees' contributions.

- Analysis of data revealed that opening balance for 293 accounts for 2005-06 and 17 accounts for the period from 2000-01 to 2005-06 were shown as zero and minus respectively.
- The date of birth and date of appointment fields were left blank in 310 and 294 cases (February 2006) respectively. Since PF rules provide that subscription of PF deduction of an employee should commence after completion of one year of service and should be stopped three months prior to the month of superannuation, capturing data in these fields was essential to ensure adherence to rules.
- Rules state that the minimum amount of subscription payable for any month shall be 8.33 per cent of the subscriber's emoluments (Basic Pay + Dearness Pay) and shall not exceed the emoluments. Instances of irregular contribution towards PF were noticed due to inadequate validation controls. In five cases the subscription to PF exceeded the basic pay plus dearness pay drawn for the month. In 85 cases the employees' subscription towards PF (March 2005) was less than the statutory minimum.
- As per New Pension Scheme, 10 per cent of Basic pay, Dearness Pay and Dearness Allowance has to be recovered from all Railway employees who joined after 1 January 2004. This recovery should be effective from the month after the month of joining. It was observed that due to poor validation, subscriptions to New Pension scheme were not effected in 62 cases even after completion of requisite length of service.

2.2.6.4 Information System security

Information System security comprising a well documented security policy is essential to protect data and valuable assets against loss, misuse and damage to the computer system as well as to prevent the unauthorised disclosure of confidential data. There must be a well documented plan for business continuity and data recovery, definite responsibilities in accordance with rules and structures for continuing operations in the event of any intentional or unintentional disaster. Audit observed that PF Accounting system suffered from the following deficiencies:

- ▪ The control procedures were not manualised.
- ▪ Training was not provided to employees regarding operation of system and security awareness.
- ▪ User ids and passwords were shared by the users irrespective of their duties.
- ▪ No audit trail was maintained.
- To maintain data integrity, edition/deletion of data was required to be authorised at higher level. It was observed that data entry was being done

in dbase software where edit/delete facility was available to all users and all users were authorised to access the software as well as data.

- All system changes should be authorised at appropriate levels, tested and documented. It was observed that changes made in the database/system were not documented.

2.2.7 Conclusion

The PF Accounting System in Izatnagar Division of North Eastern Railway was not comprehensively developed as all the relevant business rules were not incorporated and the system suffered from inadequate validation controls. There was no IT security policy and weak access control mechanisms coupled with absence of audit trail rendered the system vulnerable to manipulation.

(N.R. RAYALU)

New Delhi **Deputy Comptroller and Auditor General**

Dated:

Countersigned

(VINOD RAI)

New Delhi **Comptroller and Auditor General of India**

Dated: