INFORMATION TECHNOLOGY SECURITY POLICY FOR INDIAN RAILWAYS: REPORT OF THE INTER-DISCIPLINARY CORE GROUP

Ministry of Railways (Railway Board)

August 2007

Preface

The pace of computerization is increasing at a fast pace in Indian Railways. Several large, mission-critical IT applications have been implemented in the recent past. IT Security has therefore assumed great importance for Indian Railways to avoid unauthorized access to information, its unauthorized manipulation, unauthorized deletion or damage, and denial of service to authorized users.

The approach paper for the 11th 5–year plan estimates an overall capital outlay of Rs. 3100 crore for IT projects during the plan period. Out of this amount, an estimated Rs. 200 crore should be spent on IT security alone during this period.

While individual IT applications in Indian Railways have been designed to be secure, organization-wide IT Security has not been put on a formal footing. In view of the above, Railway Board had set up an Inter-disciplinary Core Group vide its Order no ERB-I/2006/23/37 dated 13/10/2006, to formalize the IT Security systems and processes in Indian Railways.

The Core Group met on several occasions, and the experience of the members was pooled; consultations were also held with technical experts. In addition, the literature was surveyed and relevant material consulted to draft a common Baseline IT Security Policy to draw up a minimum set of security requirements for all IT systems.

The Recommendations of the Core Group read along with the Baseline IT Security Policy mandate the security parameters that all IT systems in Indian Railways must follow.

The Recommendations and the Baseline IT Security Policy are herewith put up to Board for approval.

(Samar Jha) **SDGM** **Western Railway**	**(Harsh Kumar)** **EDF(X)-II** **Railway Board**	**(Sunil Kumar)** **CPM – IT / FOIS** **Northern Railway**
(Raman Bansal) **CSM – Telecom** **CRIS**	**(Chhatrasal Singh)** **Director (C&IS)** **Railway Board**	**(S. S. Mathur)** **GM – IT** **CRIS**

Executive Summary

As is well known and accepted the Security of IT Systems has assumed great importance in Indian Railways in recent times because of Criticality[1], Extent[2] of applications and Threats[3] to them.

In view of this a multi-disciplinary Core Group was set up by Board to draw up a policy and recommend procedures and mechanisms for ensuring effective IT Security in Indian Railways.

The Core Group has developed a 'Baseline IT Security Policy' and based on this policy recommended an IT Security set-up to develop detailed procedures and instructions and to maintain an appropriate level of security for the Railways' IT assets.

Main recommendations of the Core Group are:

- Baseline IT Security Policy to form the basis for detailed IT security procedures in all Railway units.
- Setting up of **CERT-RAIL** organization in Board to coordinate.
- Setting up of IT Security organizations in all Zonal Railways and Units.
- IT Security Group of CRIS to provide technical support to Railways' IT security organization.
- Provision of IT Security training to all IT Security managers and staff of Indian Railways.
- Third-party IT Security Audit of all major IT applications and assets.

[1] Substantial presence of IT systems in critical areas of Railway working.
[2] Nation wide network to support these applications at different stations/locations.
[3] Higher threats perception and damage that can be caused to the system.

Table of Contents

Background	5
Definitions	6
Approach	8
Information assets in Indian Railways	9
Classification	11
Coverage	14
Identity Management	16
Equipment Procurement	17
Recommendations	17
IT Governance	20
Further Action	21
Appendix A: IT Security Organization	22
Appendix B: IT Security Standards	23
Appendix C: Cobit Framework	26
Appendix D: Terms of Reference	28
Appendix E: Bibliography	29

1. Background

1.1. In recent years, Indian Railways have implemented several large computerised Information Systems that are mission-critical in nature. In the meantime, incidents of unauthorized access to information, its unauthorized manipulation, unauthorized deletion, and denial of service to users, have increased tremendously all over the world.

1.2. As a result, IT Security has assumed great importance for Indian Railways. Traditionally, each individual IT application being used in Indian Railways has been designed to be fairly secure. However, organization-wide IT Security has not been put on a formal footing.

1.3. Recently, in view of the increasing importance of electronic information in Government work, the Ministry of Home Affairs, Government of India, has also mandated an IT Security system for all Government bodies.

1.4. The pace of computerization is also increasing very fast in Indian Railways. The approach paper for the 11^{th} 5 – year plan estimates an overall capital outlay of Rs. 3100 crore for IT projects during the plan period. An estimated Rs. 200 crore will be spent on IT security alone.

1.5. In view of the above, Railway Board set up an Inter-disciplinary Core Group vide its Order no ERB-I/2006/23/37 dated 13/10/2006 to formalize the IT Security processes in Indian Railways so that an appropriate level of IT Security could be mandated for all IT applications.

1.6. The Inter-disciplinary Core Group as originally cast consisted of the following members:

Executive Director/(C&IS), Railway Board	Convener
CPM/FOIS/Northern Railway	Member
Executive Director/F(X)II Railway Board	Member
SDGM/Western Railway	Member
GM/IT/CRIS	Member

1.7. Vide Railway Board's Order no ERB-I/2006/23/37 dated 19/12/2006, CSM/Tele/CRIS was co-opted as Technical Member.

1.8. Vide Railway Board's Order no ERB-I/2006/23/37 dated 07/02/2007, CPM-IT/FOIS was nominated the Convener in place of Executive Director (C&IS), and Director (C&IS) was nominated as a Member.

1.9. The present composition of the Core Group is:

CPM-IT / FOIS / Northern Railway	Convener
SDGM / Western Railway	Member
Executive Director / F(X)II / Railway Board	Member
Director / C&IS / Railway Board	Member
GM-IT / CRIS	Member
CSM / Telecom / CRIS	Technical Member

1.10. The **terms of reference** of the Core Group are

1.10.1. To formulate the policy / mechanism for ensuring adequate measures in the main areas of computer security, such as

- Access control
- Confidentiality – denial of access to unauthorized person, pen / flash drives etc
- Data loss / theft
- Integrity – protection against unauthorized changes
- Authentication – establishing the identity of actual user

1.10.2. To lay down well defined procedures for safeguarding computer hardware / software and data / information stored and transacted, in stand-alone computers or computer networks.

1.10.3. To suggest a mechanism for drawing up a plan for third party security audit.

1.10.4. To evolve a mechanism for coordinating with other central agency / agencies involved in computer security.

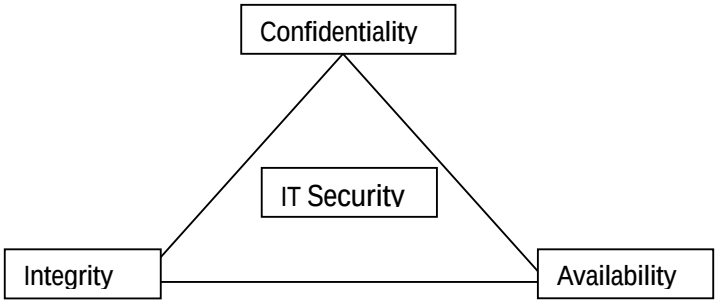
1.10.5. To suggest measures for obtaining International Security Standard Certifications such as ISO 27001 for the major applications of IR.

1.11. The Core Group met on several occasions, and the experience of the members was pooled; consultations were held with technical experts from, amongst others, CRIS, Konkan Railway Corporation Ltd., and ICICI Bank Ltd. In addition, the literature was surveyed and relevant material consulted.

1.12. The Core Group has not restricted itself solely to the terms of reference as enunciated by Board. It has looked at the entire scope of IT Security as understood today. Each of the terms of reference has, however, been addressed by the recommendations as given in Appendix D.

2. Definition of IT Security and IT Security Management System

2.1. IT Security is concerned with ensuring an appropriate level of ***confidentiality, integrity, and availability*** of the information contained in an IT system.



2.2. An Information Security Management System (ISMS) defines all aspects of IT Security in an organizational unit. It also lays down the procedures to manage it, based on a set of IT security policies. The basic elements of an ISMS are laid down below:

2.2.1. ***Scope of the ISMS and identification of information assets:*** Information assets are the hardware, programs, and data that constitute the information systems of an organization. The scope of the ISMS determines the information assets as well as the business processes and staff covered within its ambit. A clear definition of the scope is important where an information system is interfaced with an external information system.

2.2.2. ***Threat perception and vulnerability assessment:*** Each information asset varies in value to the organization. The threats and vulnerabilities of each asset also vary. Accordingly, a clear idea of the threats faced by each information asset as well as an assessment of its vulnerability to these threats is an important part of an ISMS.

2.2.3. ***Preventive measures:*** These measures are taken to prevent the occurrence of security breaches and to maintain an appropriate level of IT security of each information asset. *Surveillance measures* form an important part of preventive measures, to ensure that threat perceptions and vulnerabilities of each information asset are continuously updated and kept current.

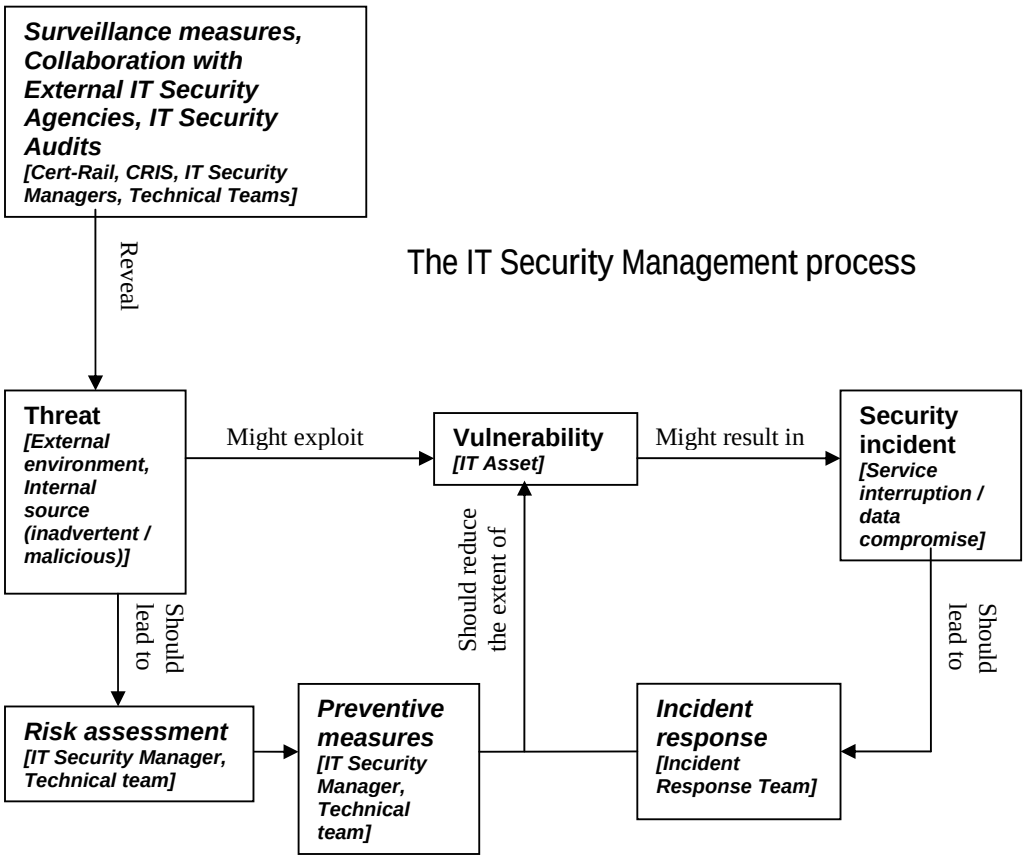
2.2.4. ***Monitoring:*** Monitoring of operations to identify any security breach is vital to ensure that timely action can be taken.

2.2.5. ***Incident response*** to mitigate the effect of any security breach or potential breach.

2.2.6. ***An IT Security organization*** to assume the responsibility for the above policies and procedures, consisting of suitably trained IT managers with the requisite authority.

2.3. The conventional definition of security, that is, prevention of theft, is not valid in the case of IT security, since no physical movement of any object needs to take place – information can be simply copied, leaving the original unchanged. Therefore the conventional Railway security apparatus and organization has at best a marginal role to play in the area of IT Security.

2.4. On the other hand, theft of computer equipment is similar to the theft of any valuable equipment. Physical security of computer equipment from theft, vandalism, etc. is therefore a general law enforcement problem, and is not given great importance while discussing the technical aspects of IT Security. Valuable IT equipment and assets need to be physically protected with as much care as other valuable plant and equipment.



3. Core Group's approach

3.1. The Core Group has kept in view the following guiding principles in drawing up its recommendations:

3.1.1. All information is not similar in value to the organization. Highly valuable information needs to be protected more stringently than less valuable information: a balanced approach is therefore advocated. The guiding principle followed is that the ***minimum level of security required*** should be provided to each information asset.

3.1.2. **IT Security standards** have been laid down internationally: **ISO:17799** defines elements of an Information Security Management System and **ISO:27001** defines the security auditing process. ***The definition of IT security has been adopted from these standards***. It is the intention that ***all the critical IT assets*** (applications, databases, networks) ultimately be brought up to the level of the ISO:17799 and ISO:27001 standards, and maintained at that level through regular security audits. A gist of the provisions of these standards appears at Appendix B of these recommendations.

3.1.3. The IT Security standards follow a **3-tier** structure: **guidelines and baseline policies** provide the basis for **procedures and work instructions** applicable to individual units, and finally result in

records of the working procedures. ***The Core Group has proposed to follow the above 3-tier structure for Indian Railways as well.*** However, it is of the view that detailed procedures and work instructions are needed only for information assets that are of extremely high value. For other information assets, a common sense approach based on the Baseline IT Security Policy (described in section 3.2.1 below) is advocated.

3.2. The approach followed by the Core Group is modeled on the practices recommended for large organizations:

3.2.1. An **enabling IT Security policy**, called the "**Baseline IT Security Policy for Indian Railways**", has been formulated as an overarching policy within which detailed procedures for individual units are to be drawn up. The Baseline IT Security Policy is annexed to this document. It is applicable to all the units of Indian Railways.

3.2.2. The concept of empowering nominated ***IT Security Managers*** of each unit, to lay down the detailed procedures and instructions for their respective units and for the information assets under their control has been advocated. The provisions enshrined in the Baseline IT Security Policy will guide the IT Security Managers for this purpose.

3.2.3. Creation of separate posts for IT Security management has not been advocated as a general rule, and the approach centres on training and empowering existing IT managers to take on the additional responsibility for IT security.

3.2.4. A phased approach to IT Security audit and certification is advocated, since it is not practical to take up all the information systems of Indian Railways for audit / certification at one time.

4. IT applications and information assets in Indian Railways

4.1. Information Technology has evolved in Indian Railways over a period of 40 years.

4.1.1. The first computers were installed in the 1960s and 1970s, primarily to execute high-volume batch jobs such as payroll preparation. Inventory control, revenue reconciliation, and other similar processes were also run as batch jobs. For this purpose, EDP centres were set up in Railway Board and all the Zonal Railways and Units of Indian Railways.

4.1.2. By the mid-1980s, technology had evolved to the extent that on-line transaction processing applications were within the realms of possibility. Therefore, standardized transactions such as reservation and ticketing could be taken up under on-line transaction processing applications. These applications could be accessed through terminals distributed across the country.

4.1.3. At the same time, small EDP centres were conceived for Divisional headquarters, workshops, etc. These centres were provided with mini-computers (today's small servers).

4.1.4. Later, as general purpose IT equipment became cheaper, PCs and small servers were gradually installed in all the offices of the Railways.

4.1.5. In the late 1990s, SDT and MIS applications were conceived as decentralized applications running on smaller independent servers placed in Zonal and Divisional headquarters.

4.2. As a result of the above evolution, the IT assets of Indian Railways are being managed in the following basic ways:

4.2.1. Large ***centrally administered applications*** such as PRS, FOIS, UTS have common hardware and software, with the core equipment placed either in one location (FOIS) or a few locations (PRS – 5, UTS – 7). This pattern is observed in up-coming applications such as COIS / ICMS, Crew Management System, etc. The administration is done by C&IS Directorate of Railway Board and CRIS.

4.2.2. ***Batch-type applications*** such as Payroll are being managed by the respective EDP centres, whether in Zonal headquarters, Divisional headquarters, PUs, or Workshops. These fall under the control of the CCA Directorate of Board.

4.2.3. ***Zone based applications*** such as PRIME, AFRES, MMIS are being managed by the respective Zonal EDP centres. These also fall under the control of CCA Directorate of Board.

4.2.4. ***PCs, small servers, and other equipment***, used for general information processing or running small home-made applications are being managed by the respective departments. These are not being directly managed by any Directorate of Board.

4.3. The Core Group has therefore kept the different types of IT applications and assets in view while formulating its views.

4.4. The IT applications and systems available today in Railways are:

4.4.1. *Ticketing and passenger service applications:* the passenger reservation system PRS and the unreserved ticketing system UTS fall in this category. These applications cater to ticketing, reservation, and information needed by passengers to plan and execute the journey.

4.4.2. *Freight and operations related applications:* the freight operations information system FOIS, COIS, control office application, crew management system, etc falls in this category.

4.4.3. *MIS applications* such as asset management applications for all technical departments.

4.4.4. *Finance and related applications* such as AFRES / PRIME, MMIS, personnel management system, operating statistics system, PAS, FAS, etc.

4.4.5. *Small independent systems*, developed in various units of the Railways.

4.5. These applications are provided with the following architectures:

4.5.1. *Essentially centralized:* FOIS, COIS, and the like are based on a single set of servers placed in a central location, with a central database, whereas PRS and UTS are based on 5 and 9 server clusters respectively, located in large Zonal Headquarters. These applications are managed by CRIS or dedicated organizations operating under CCM/PMs.

4.5.2. *Zonal applications:* Applications such as MMIS, and the Personnel Management system are centralized in the Zonal headquarters. These are managed by the EDP centres.

4.5.3. *Production Unit systems:* All Production Units are based in one location only. All their systems are therefore managed by their local EDP / IT centres. These applications are local to each Production Unit.

4.5.4. *Distributed systems:* Systems such as the MIS applications, Control Office application, Workshop systems, are distributed: the servers are placed in the individual units, while the application logic is centrally developed and managed.

4.6. The information assets of the Indian Railways comprise all the individual elements of the above systems. These are:

4.6.1. *Hardware:* Servers, PCs, printers, data storage devices, routers, switches, other network devices.

4.6.2. *System software:* Operating Systems, Database Management Systems, software application servers and web servers of different types, Office suites, email software, software development environments, compilers, etc.

4.6.3. *Application software:* Program codes (source code and object code) of applications written specially for Railways, whether in-house or outsourced. Program modules and components, program libraries, software classes and objects, customized interfaces and services, all form part of application software.

4.6.4. *Data / information:* The data / information residing in the system, including transactions, logs, unstructured data, non-text data, emails, all are information assets. Data backed up or archived, along with the concerned logs and snapshots is also included.

4.6.5. *Documentation:* System specifications, design documents, user manuals, policies of various kinds, records, printouts; both in paper form as well as on electronic media. Removable media containing system software and application software are also considered documentation for this purpose.

5. Classification of Information Systems by security needs

5.1. Security needs of different applications vary. The primary risk to IT Security of the individual information bases can be:

5.1.1. *Unauthorized reading or copying of information (data / program code):* loss of **confidentiality** – this mode of security breach is

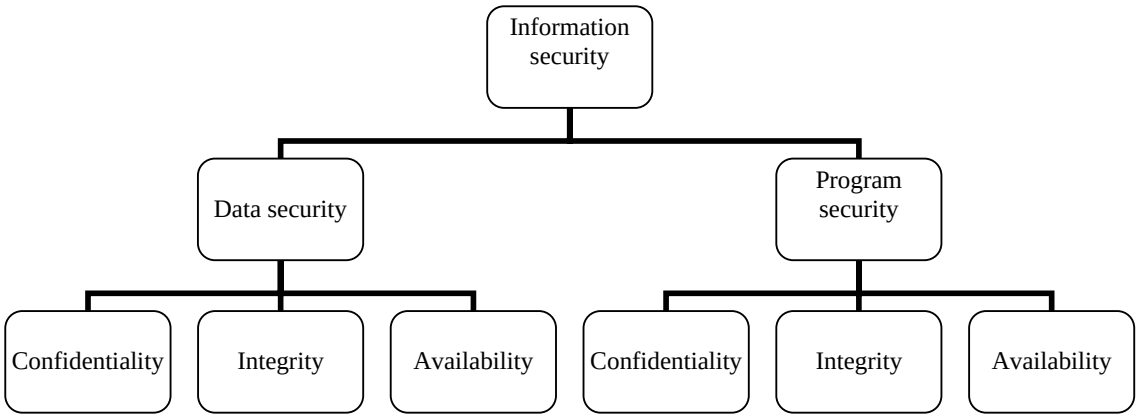
important for applications such as MMIS, from which confidential information regarding tenders could be noted

5.1.2. *Unauthorized manipulation of information (data / program code):* loss of **integrity**

5.1.3. *Unauthorized deletion of information (data / program code) or causing denial of service:* loss of **availability**

5.2. In general, loss of confidentiality is much less a problem in the context of Indian Railways than loss of information integrity. In some applications, availability of the information is of prime importance.

5.3. The IT Security needs for program code differ from those for data. Program code needs to be protected primarily for reasons of copyright. Data security requirements are more complex, and are described below.



5.4. Classification of applications based on the **data security** needs is given below:

5.4.1. IT applications in which the prevention of the loss of data confidentiality is of prime importance

5.4.1.1. E-tendering systems need protection of the confidentiality of the bids received electronic form.

5.4.1.2. Some employee records, for example, disciplinary proceedings etc need to be kept confidential in the personnel management information systems. Similarly, in the health management information system, employee records need to be kept confidential for privacy reasons.

5.4.1.3. All applications relating to vigilance aspects need to keep data confidential.

5.4.1.4. Other browser-based systems such as the IR collaborative portal might also need to keep data confidential.

5.4.2. IT applications in which data integrity is of prime importance

5.4.2.1. In all applications, data integrity is very important. However, it becomes vital for the Passenger Reservation System in which it is vital to ensure that existing data is not tampered with.

Similarly in freight booking in the FOIS, unauthorized tampering with data can have large financial implications.

5.4.2.2. All financial applications need to keep their data safe from any unauthorized change.

5.4.3. IT applications in which information availability is of prime importance

5.4.3.1. All applications involving a public interface are highly susceptible to disruptions and availability. High availability is vital for the Unreserved Ticketing System (required uptime over 99.95% at each counter), and to a slightly lesser extent, the Passenger Reservation System.

5.4.3.2. Operational applications such as the Control Charting System also require extremely high uptime of 99.95%.

5.4.3.3. Adequate availability of applications includes an appropriate performance level as well.

5.5. In the case of **security of program code**, the considerations are different from those for data.

5.5.1. Confidentiality

5.5.1.1. In the case of program code, confidentiality has two aspects: firstly, code should be kept confidential to ensure that intellectual property is protected; secondly, code of those applications needs to be kept confidential in which it is desirable to keep certain program logic from becoming publicly available (for example, encryption algorithms etc.)

5.5.1.2. For Indian Railways' applications, program code confidentiality is of moderate importance.

5.5.1.3. Program code needs to be kept confidential for reasons of copyright and IPR. "Freeware" can be distributed freely, hence needs no confidentiality. In-house distributed software code might be freely distributed within the organization, or even designated as freeware. However, most software code is protected by IPR measures, hence needs to be kept confidential.

5.5.2. Integrity

5.5.2.1. For program code, integrity is vital. A loss of integrity of the programs can literally create havoc. Inadvertent changes in program logic can cause programmes to fail. On the other hand, deliberate and possibly malicious changes in program logic in an unauthorized manner can lead to large scale fraud.

5.5.2.2. **Configuration control** of program code, including system software, is of utmost importance to maintain integrity.

5.5.2.3. Regular structured code walkthroughs are also essential to monitor the integrity of program codes.

5.5.3. Availability

5.5.3.1. For program code, availability is generally restricted to ensuring that previous versions of the program are available to manage configuration control.

5.5.3.2. Working copies must be maintained of the media on which source code is stored, and appropriate storage conditions should be ensured.

5.5.4. In general, therefore, program code of all but designated freeware should be kept confidential and secure; **configuration control** of all program code should be mandatory; and the media on which source codes or other program codes are stored should be provided appropriate conditions.

5.5.5. **Licensing requirements** are legal in nature. All software must be installed in such a way that licensing requirements are met. When not in use, licensed software media must be kept in a secure place to protect it from theft.

5.6. Since the basic requirements for security vary from application to application, it is recommended that each large application be assessed on these three parameters, namely, **confidentiality, integrity,** and **availability**, for both the **data** and the **program code**, and accordingly an **appropriate security strategy be devised** by the concerned IT Security Manager.

6. Units and information assets to be covered

6.1. It is recommended that IT Security Management Systems should be established in all units of Indian Railways that have significant IT assets. Such units are:

6.1.1. **CRIS:** CRIS manages most of the large centralized applications of Indian Railways. There are two aspects of the security system required in CRIS: firstly, the data of the important centralized applications such as Freight Operations Information System, Crew Management System, etc and the Passenger Reservation System, Unreserved Ticketing System, National Train Enquiry System etc residing in data centres managed by CRIS; secondly, the program code under development and maintenance for all these applications, which is maintained in the development centre in CRIS.

6.1.2. **CRIS**' role in IT management is projected to become increasingly important for IR. Therefore, CRIS must adopt the most rigorous IT Security processes.

6.1.3. **Zonal EDP centres:** EDP centres in zonal railways manage payroll applications, financial applications, and other applications such as Material Management Information System etc. In some cases, applications developed under the MIS project are also deployed in the EDP centres. For such applications, program code is also managed by the EDP centres.

6.1.4. **EDP centres in production units:** EDP centres/I. T. Centres in production units run payroll applications, material management systems, shop floor production systems, financial applications, and personnel management systems. Programme codes are maintained by individual centres.

6.1.5. **EDP centres in divisions:** divisional EDP centres run payroll systems as well as some small divisional applications, for which data and programmes are maintained by each centre. In some cases, applications developed under the MIS project are hosted in these EDP centres. The MIS application programme codes are centrally managed by the mis coordinator.

6.1.6. **EDP centres in workshops/other units:** units such as workshops, maintenance facilities etc also possesses EDP centres in which payroll and a few other applications are managed.

6.1.7. **EDP centres in training institutes:** EDP centres in the Central Training Institutes such as Railway Staff College are fairly large and offer library management systems, payroll systems etc apart from providing computing facilities to the trainees.

6.2. Special IT Security procedures should be drawn up for large centrally administered applications such as PRS, UTS, FOIS, etc. by CRIS. All the information assets forming part of these systems will be covered under the procedures drawn up by CRIS specifically addressing these applications.

6.3. In recent years IT assets have become distributed across Indian Railways as well. Examples are:

6.3.1. In all offices of Indian Railways, PCs and other office automation equipment is available in large numbers. It is estimated that over 25,000 PCs and related equipment are in operation across Indian Railways. This number is increasing by an estimated 8% to 12% per annum. In general, individual departments and groups manage and maintain these systems.

6.3.2. In over 1500 stations and PRS locations, dumb terminals, printers and communication equipment are placed to provide it ticketing services. This equipment is managed by the concerned CCM/PMs.

6.3.3. In major yards and interchange points, FOIS terminals are placed. Similarly, in all control offices, terminals of FOIS, NTES, COIS punctuality model, and Control Office Automation are placed.

6.4. The IT assets distributed in these small units will generally be covered under application level IT Security procedures. However, where PCs etc. being used for general purposes are installed in large numbers, one of the managers must be designated as the IT Security Manager, and maintain IT security in accordance with the “Baseline IT Security Policy for Indian Railways”.

	IT Asset type	***Examples***	***IT Security procedures to be managed by***

	IT Asset type	***Examples***	***IT Security procedures to be managed by***
1	Centrally Administered Applications	PRS, FOIS, UTS	CRIS / C&IS Dte of Railway Board
2	Zone Based Applications	PRIME, AFRES, MMIS	CCA Dte of Railway Board / Zonal EDP Centres
3	Distributed Applications	MIS applications	MIS Dte of Railway Board
4	Production Unit Applications	Systems in RCF, ICF, DLW	CM-IT of the PU
5	Batch type applications	Payroll	EDP centres
6	General purpose IT equipment	PCs, servers, placed in all offices	Concerned departments

7. Identity Management

7.1. In a large organization such as Railways, identity management is an important part of IT security. Therefore it has been separately treated by the core group.

7.2. Identity management refers to ***identification, authentication,*** and ***authorization*** of persons who access any information system or data.

7.3. ***Identification:*** Identity Management Systems ensure that *identification information* (login ids, passwords, biometric signatures) is *available* and *cannot be bypassed* while accessing an IT asset or entering an IT application, that is, appropriate access control mechanisms are followed. Identity management systems ensure that identity information is stored in a suitably encrypted form.

7.4. ***Authentication:*** The identity passed to the application is *authenticated* by “two-factor” or similar authentication mechanisms (“what you have + what you know”). Identity management systems ensure that *identity information is transferred in suitably encrypted form* to prevent “man-in-the-middle” attacks.

7.5. ***Authorization:*** Identity Management Systems also ensure that the right *authorization matrix* is maintained so that only authorized persons are allowed to access the different parts of an information system and the various IT assets. Authorizations are *granted* and *revoked* as the role of each user changes, through the Identity Management System.

7.6. Identity Management systems consist of a combination of Public Key Infrastructure and other encryption methods, directory and discovery methods, and physical identification systems such as biometrics. Therefore the core group is of the view that a separate exercise should be undertaken by CRIS to set up Identity Management systems for the different applications and IT assets of Indian Railways. A report on

comprehensive Identity Management should be put up to the C&IS Directorate of Railway Board, for further policy decisions.

8. Procurement of equipment required for IT Security

8.1. In the past, hardware and software required for effective IT security such as operating systems, firewalls, intrusion detection systems, access control systems, etc., have themselves suffered from design defects, making them susceptible to electronic attacks. They have been rendered ineffective at the very time that they were needed.

8.2. To combat this problem, a set of Common Criteria for IT security have been drawn up by an association of Government and industry bodies known as the Common Criteria Project (in India, STQC IT Services of the Ministry of IT is a member).

8.3. Software and hardware products are certified against the defined criteria by the authorized members of the Common Criteria Project. Certified products (Targets of Evaluation or TOEs) are assessed at one of 7 Evaluation Assurance Levels (EALs).

8.4. The EAL at which a particular piece of equipment is assessed, is juxtaposed against a pre-defined Protection Profile (PP) required by a particular IT asset to meet a particular security objective.

8.5. It is therefore recommended that future procurement of critical IT equipment should specify the minimum EAL expected to meet its IT security objectives.

Assessment level	**Security characteristic**
EAL-1	Functionally tested
EAL-2	Structurally tested
EAL-3	Methodically tested and checked
EAL-4	Methodically designed, tested and reviewed
EAL-5	Semi-formally designed and tested
EAL-6	Design semi-formally verified, and tested
EAL-7	Design formally verified, and tested

8.6. Normally, a level of EAL-4 is adequate for most equipment. However, the required level varies from application to application.

9. Recommendations of the committee

9.1. In accordance with the above approach, principles, and assessment, therefore, the Core Group makes the recommendations given below.

9.2. Baseline IT Security Policy

9.2.1. A Baseline IT Security Policy has been drawn up, which conforms to the latest ISO standards on IT Security. It is recommended that this Baseline policy should form the basis for subsidiary procedures and instructions, to be drawn up by each Unit as defined in section 6.1 above.

9.2.2. To begin with, CRIS should draw up detailed IT Security procedures for its major applications based on the Baseline IT Security Policy for Indian Railways, and circulate them to all Railway units. The units should refer to CRIS' procedures to draw up their own IT Security procedures.

9.3. CERT-Rail, a central body to manage overall IT security

9.3.1. The overall IT Security environment in Indian Railways will be monitored by the Cert-Rail organization, to be set up under Executive Director / C&IS in the Railway Board.

9.3.1.1. Cert-Rail will monitor the progress of IT Security adoption measures in all units of Railways.

9.3.1.2. Cert-Rail will also provide overall guidance to CRIS' IT Security group, which will provide necessary technical support.

9.3.1.3. Cert-Rail will ensure that the Baseline Security Policy is kept updated with the latest knowledge and disseminated to the individual units.

9.3.1.4. Cert-Rail will interact with Ministry of IT, Cert-In, and other IT Security related forums set up by Government of India and industry.

9.3.2. Cert-Rail will co-opt experts from industry and academia as and when required, to obtain specialized skills through them. Representatives of major IT vendors would also be so co-opted as and when required.

9.4. IT Security organization in Zonal Railways and units

9.4.1. The Core Group recommends that General Managers of Zonal Railways / Production Units, and CAOs / DGs / Directors of other units, nominate one person at officer level in each Unit (defined in section 6.1 above) as the IT Security Manager.

9.4.2. GMs may delegate this power to AGMs, or the PHODs of departments with major IT applications and assets under their control, that is, FA&CAO, CCM, COM, CSTE (for Railnet), or other PHODs as IT applications related to their departments are put into operation.

9.4.3. Care should be taken to select persons with an IT background as IT Security Managers.

9.4.4. The recommended IT Security Manager is:

	Unit	Recommended IT Security Manager
1	Zonal Headquarters	Sr EDPM: coordinating manager SAG / JAG officer from each department with significant information assets under its control SAG / JAG officer from S&T department to be responsible for network security
2	Divisions	Sr EDPM / EDPM / JAG officer from any discipline
3	Workshops / maintenance sheds	JAG / SS officer
4	Production Unit	CM – IT / Sr EDPM (JAG)
5	RDSO, CORE, COFMOW	SAG / JAG officer
6	Central Training Institutes	SAG / JAG officer

9.4.5. The nominated IT Security Manager must ensure that adequate staff is deployed for monitoring and incident response as detailed in the "Baseline IT Security Policy for Indian Railways".

9.5. IT Security Group in CRIS

9.5.1. CRIS should set up a dedicated IT Security Group with adequate strength to ensure that all the applications managed by it are adequately secured.

9.5.2. CRIS' IT Security group should provide technical support to Cert-Rail. Technical staff for Cert-Rail might also be drawn from CRIS.

9.5.3. CRIS' IT Security group should also provide technical consultancy to Zonal Railways to set up and maintain their IT Security systems. This should also include coordination of the training of IT Security Managers and staff on request from the Zonal Railways / units.

9.5.4. CRIS' IT Security group should also set out norms for procurement of sensitive IT equipment; for example, recommending which equipment should not be bought without Common Criteria certification, and at what level it should be assessed.

9.6. Training in IT Security

9.6.1. As mentioned above, CRIS' IT Security group should coordinate IT Security related training for all the nominated IT Security Managers

and their staff. The training should be imparted through a certified agency such as STQC of the Ministry of IT.

9.6.2. The nominated IT Security Managers should be given training on ISMS formulation and IT Security audit, leading to certification, in a phased manner.

9.6.3. All staff nominated for the various IT Security related work such as incident response teams should be adequately trained.

9.6.4. GMs of Zonal Railways and Units must ensure that adequate funds are made available for comprehensive training on IT security. All relevant personnel must go through one training rotation as recommended by CRIS within a period of 1 year.

9.7. IT Security Audit policy

9.7.1. All major IT applications and assets, such as PRS, FOIS, UTS, Railnet, etc. should be audited by a certified third party IT Security auditing agency. The shortlist prepared by Cert-In of the Ministry of IT should be followed for this purpose.

9.7.2. A list of the applications and assets to be considered for audit should be drawn up by Cert-Rail and updated periodically.

9.7.3. The IT Security Manager of the concerned unit will be responsible for ensuring that all the important IT applications / assets under his control are covered by a plan for IT Security audit.

9.7.4. IT Security audits can be carried out in a phased manner, with the most important applications being taken up first.

9.7.5. Getting the IT Security audit conducted will be the responsibility of the designated agency / IT Security Manager for each such application.

9.8. ***Identity Management Systems*** should be further explored by CRIS' IT Security Technical Group, and the best options for enforcing appropriate Identity Management decided upon for the different categories of IT assets and applications.

9.9. The recommended IT Security organization is depicted in Appendix A.

10. IT Security and IT Governance

10.1. In general, IT Security Management is a sub-set of Information Technology Governance. If IT Governance is lacking, IT Security can never be put on a sound footing.

10.2. Implementation of IT security policy is almost impossible without a Steering Committee function exercised by Board, and without clear accountability for IT security measures.

10.3. The Core Group therefore strongly recommends that a formal approach to IT Governance is needed in Indian Railways. This can be modeled on a well-regarded IT Governance framework such as COBIT 4.1 of the Information Systems Audit and Control Association (ISACA) of the USA. This aspect can be taken up separately by Board.

10.4. A short write-up on COBIT 4.1 is placed at Appendix C.

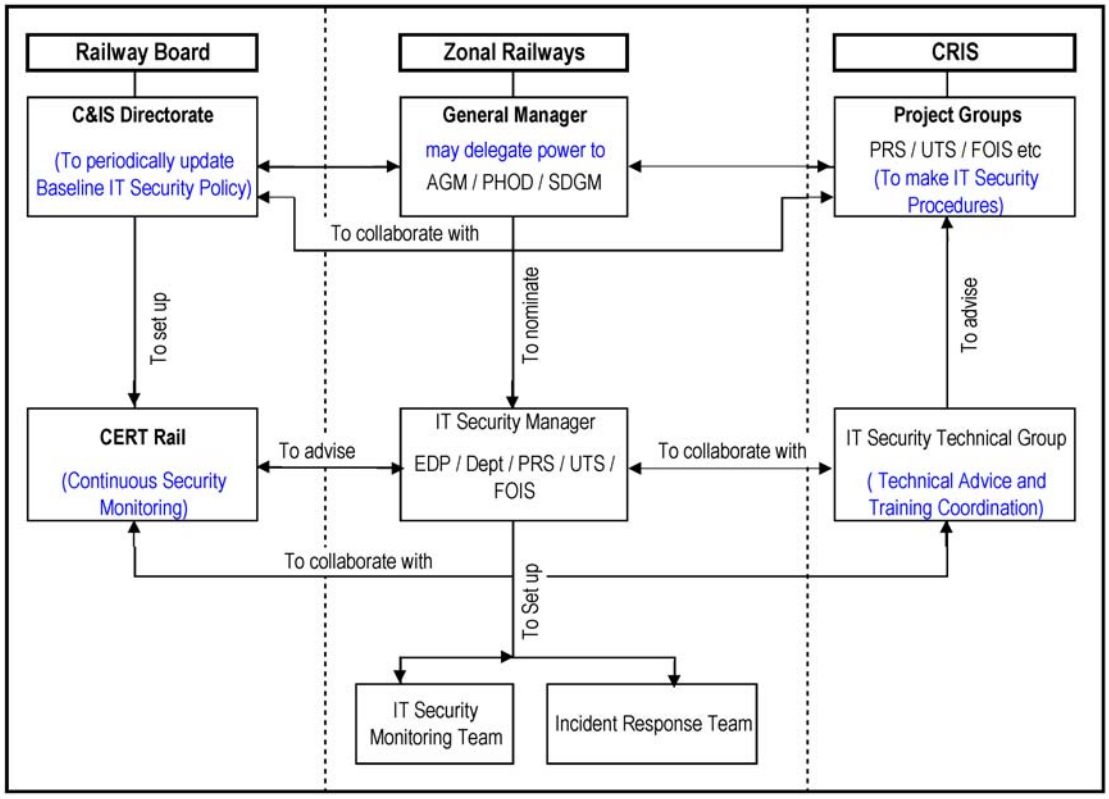
11. Further action

11.1. Since this is the first attempt at setting down the IT Security Policy for Indian Railways, this document and the Baseline Security Policy will need to be reviewed and improved in future.

11.2. The Core Group recommends that Railway Board review the progress in this area after a period of twelve months, and also set up a committee / core group to review these recommendations and the Baseline Security Policy at periodic intervals.

Appendix A

Recommended IT Security Organisation For Indian Railways



Appendix B

Major provisions of the IT Security standards ISO:17799:2005 and ISO 27001:2005.

ISO/IEC:17799:2005 is the international standard for **"Information technology — Security techniques — Code of practice for information security management"**. It establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization.

The standard lays down that IT security requirements can be established by

- carrying out a risk assessment, that is, identifying threats to IT assets, and evaluating the vulnerability to these threats and likelihood of their occurrence, and estimating potential impact
- studying the legal, statutory, regulatory, and contractual environment of the organization
- studying the principles, objectives and business requirements for information processing developed internally by the organization

It outlines control objectives and controls to enable an organization to meet the commonly accepted goals of information security management.

Controls considered to be essential to an organization from a legislative point of view include, depending on applicable legislation:

- data protection and privacy of personal information
- protection of organizational records
- intellectual property rights

Controls considered to be common practice for information security include:

- information security policy document
- allocation of information security responsibilities
- information security awareness, education, and training
- correct processing in applications
- technical vulnerability management
- business continuity management
- management of information security incidents and improvements

The standard contains 11 security control clauses collectively containing a total of 39 main security categories. The 11 clauses are:

- Security Policy
- Organizing Information Security
- Asset Management
- Human Resources Security

- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

The 39 main security categories are distributed under these 11 clauses. These contain a control objective stating what is to be achieved, and one or more controls that can be applied to achieve the control objective.

Each of the controls is provided with implementation guidelines to support the implementation of the control.

The standard also discusses in detail the area of IT Security risk assessment.

It lays down that risk assessment should include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation). Risk assessments should be performed periodically to address changes in the security requirements and in the risk situation.

The scope of a risk assessment can be either the whole organization, parts of the organization, an individual information system, specific system components, or services where this is practicable.

Risks can be treated by reducing them, accepting them, transferring them, or avoiding them. The cost of treating the risks should be balanced in relation to the possible cost of likely harm in case they occur.

The standard therefore provides a comprehensive view of IT security. By correctly assessing IT Security risks as laid down in the standard, and by setting up the various controls and by following the guidelines for implementation of the controls, IT security can be managed by any organization in a comprehensive manner.

ISO/IEC 27001:2005 – Information technology — Security techniques — Information security management systems — Requirements provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) in an organization.

It follows the Plan-Do-Check-Act (PDCA) model laid down below:

Plan (establish the ISMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.

Check (monitor and review the ISMS)	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

The standard also lays down that the ISMS should be developed after including all the control objects and controls defined in ISO-17799:2005.

ISO-27001:2005 specifies that organizations should also get their ISMS reviewed annually by the Management Representative nominated for the purpose.

The ISMS should also be audited through authorized IT Security auditors at periodic intervals, normally two years.

Appendix C

A brief background note on COBIT 4.1, a framework for IT Governance

IT Governance encompasses all the processes required to manage the IT assets of an organization to the optimum level, in order to obtain the best value from them. COBIT is a framework for IT Governance developed by the IT Governance Institute (ITGI) of the Institute of Information Systems Audit and Control Association (ISACA) based in USA.

According to the ITGI, IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives.

Control Objectives for Information and related Technology (COBIT®) provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts. They are strongly focused more on control, less on execution. These practices will help optimize IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong.

For IT to be successful in delivering against business requirements, management should put an internal control system or framework in place. The COBIT control framework contributes to these needs by:

- Making a link to the business requirements
- Organizing IT activities into a generally accepted process model
- Identifying the major IT resources to be leveraged
- Defining the management control objectives to be considered

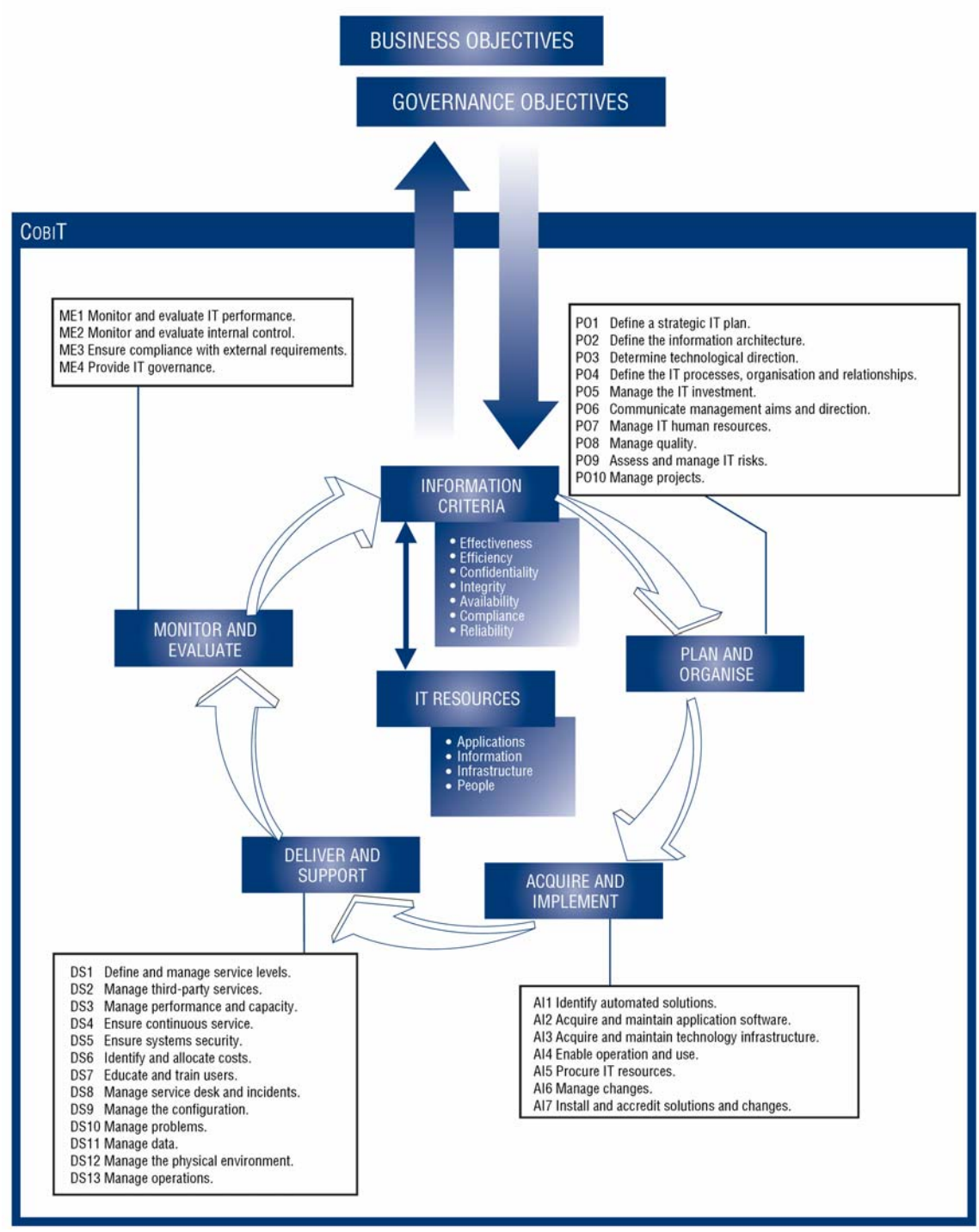
The process focus of COBIT is illustrated by a process model that subdivides IT into four domains and 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT. Enterprise architecture concepts help identify the resources essential for process success, i.e., applications, information, infrastructure and people.

The four domains defined are:

- plan and organize
- acquire and implement
- deliver and support
- monitor and evaluate

Within these four domains, 34 processes have been defined. An outline of the defined processes is given in the figure below. The framework further defines

control objectives and evaluation criteria against each process in order to guide the organization to set up appropriate procedures and instructions in each area.



COBIT Framework

Appendix D

Terms of Reference of the Committee mapped to Recommendations

Term of reference	Recommendation of Core Group
To formulate the policy / mechanism for ensuring adequate measures in the main areas of computer security, such as	
Access control	Section 8 of the Baseline IT Security Policy
Confidentiality – denial of access to unauthorized person, pen / flash drives etc	Section 10.1 of the Baseline IT Security Policy
Data loss / theft	Section 10.2, 10.3 of the Baseline IT Security Policy
Integrity – protection against unauthorized changes	Section 10.2 of the Baseline IT Security Policy
Authentication – establishing the identity of actual user	Section 8.2 of the Baseline IT Security Policy
To lay down well defined procedures for safeguarding computer hardware / software and data / information stored and transacted, in stand-alone computers or computer networks.	All sections of the Baseline IT Security Policy cover this aspect
To suggest a mechanism for drawing up a plan for third party security audit.	Section 13.2 of the Baseline IT Security Policy
To evolve a mechanism for coordinating with other central agency / agencies involved in computer security.	Section 9.3.1.4 of the Recommendations of the Core Group (this document)
To suggest measures for obtaining International Security Standard Certifications such as ISO 27001 for the major	Section 9.7 of the Recommendations of the Core Group (this document)

applications of IR.	

Appendix E

Bibliography

1. ISO/IEC 17799, Second edition, 2005-06-15: "Information technology — Security techniques — Code of practice for information security management", International Organization for Standardization, 2005.

2. ISO/IEC 27001, First edition, 2005-10-15: "Information technology — Security techniques — Information security management systems — Requirements" International Organization for Standardization, 2005.

3. "The Information Technology Act 2000", Government of India, 2000.

4. "The Information Technology (Amendment) Bill, 2006", Government of India, 2006.

5. "Common Criteria: an Introduction", a brochure produced by Syntegra on behalf of the Common Criteria Project Sponsoring Organizations, 2006.

6. "Report of the Sub-Group on Research & Development and Information Technology including Related Telecom / Networking Issues for the 11th 5-year Plan", Ministry of Railways, 2006.

7. "Computer Security, Data Safety, and IT Business Continuity on Indian Railways: Need for Policy and Systems", a paper by Shri Samar Jha, SDGM and CVO, Western Railway (with inputs by Shri V. K. Devnath, CM(IT), KRCL), 2005.

8. "Baseline IT Security Policy, Version: 3.0", Office of the Government Chief Information Officer, Government of the Hong Kong Special Administrative Region, 2006.

9. "Vision 2025: Technology for Information", a paper presented during the Seminar on Indian Railways – Vision 2025, C&IS Directorate, Ministry of Railways, 2002.

10. "Approach Paper on IT for the 10th Five Year Plan", C&IS Directorate, Ministry of Railways, 2001.