भारतीय मानक

सूचना सुरक्षा प्रबन्ध प्रणाली — अपेक्षाएं

Indian Standard

INFORMATION SECURITY MANAGEMENT SYSTEM — REQUIREMENTS

ICS 35.040

BUREAU OF INDIAN STANDARDS
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI 110002

October 2002

Price Group 5

FOREWORD

This Indian Standard was adopted by the Bureau of Indian Standards, after the draft finalized by the Information System Security Sectional Committee had been approved by the Electronics and Telecommunication Division Council.

The central theme of an Information Security Management System (ISMS) is to enable the implementing organization to enhance trust and confidence among its trading partners as well as within its own organization on its ability to protect the information and information processing assets.

Business needs of an organization can be broadly categorized into two types, one as 'strategic needs' and the other as 'imperative needs'. It is recognized that the risks to a business in relation to imperative needs are significantly high as compared to strategic needs. The adoption of an Information Security Management System (ISMS) is an imperative need of an organization's business.

The design and implementation of an organization's Information Security Management System is influenced by the prevailing threat scenario, risks to its information and information processing assets, their effect on business processes, need for business continuity and the size and structure of the organization.

It is not the intent of this standard to imply uniformity in the structure of Information Security Management Systems or uniformity of documentation. This standard can be used by internal and external parties, including certification bodies, to assess the organization's ability to meet stake holder's, customer's, regulatory and the organization's own requirements.

This standard promotes the adoption of a 'risk based approach' when developing, implementing and improving the effectiveness of the Information Security Management System, to enhance trust and confidence between the organization and its customers, trading partners and other external agencies as well as within the organization.

For an organization to carry out its business in a safe and secure manner, it has to identify all critical information assets and manage numerous risks, threats and vulnerabilities associated with the information and information processing facilities and mitigate the risks.

The risk based approach enables the organization to systematically assess the risks, threats and vulnerabilities associated with the critical information assets and related information processing facilities.

When used within the Information Security Management System, such an approach emphasizes the importance of:

a) awareness and understanding of risks, threats and vulnerabilities;
b) selection and implementation of appropriate security controls;
c) monitoring and reviewing the performance and effectiveness of the ISMS;
d) keeping the security mechanism up-to-date; and
e) continual improvement of the ISMS.

The model of a risk-based Information Security Management System is shown in Fig. 1.

(Continued on third cover)

Indian Standard

INFORMATION SECURITY MANAGEMENT SYSTEM — REQUIREMENTS

1 SCOPE

1.1 General

This standard specifies requirements for an Information Security Management System where an organization:

a) needs to demonstrate its ability to reasonably protect all business critical information and related information processing assets from loss, damage or abuse,

b) aims to enhance the trust and confidence between customers, trading partners and external agencies as well as within the organization, and

c) needs to assure conformity to applicable contractual and regulatory requirements.

1.2 Application

All requirements of this standard are generic and are intended to be applicable to all organizations, regardless of the type and size of business. Where any requirement(s) of this standard cannot be applied due to the nature of an organization and its business critical information, this can be considered for exclusion.

Where exclusions are made, claims of conformity to this standard are not acceptable unless these exclusions are limited to selection of controls (*see* **7.2.1**) and such exclusions do not affect the organization's ability, or responsibility, to protect all business critical information and related information processing facilities, and to assure conformity to applicable regulatory requirements.

2 REFERENCES

The following Indian Standards contain provisions which through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below:

IS No.	*Title*
14357 : 2002	Code of practice for Information Security management system (*first revision*)
14990 (Part 3) : 2001	Information technology — Security techniques — Evaluation criteria of IT security: Part 3 Security assurance requirements

3 TERMINOLOGY

For the purpose of this standard, the terms and definitions given below and those given in IS 14357 shall apply.

3.1 Critical Information — Information which, in the absence of assurance in terms of availability, integrity and confidentiality, is likely to have an impact on the way business is intended to be carried out.

4 INFORMATION SECURITY MANAGEMENT SYSTEM

4.1 General Requirements

The organization shall establish, document, implement and maintain an Information Security Management System and continually improve its effectiveness in accordance with the requirements of this standard.

The organization shall:

a) identify all business critical information and classify them according to their business value,

b) carry out a risk assessment on a continuous basis to determine the threats and vulnerabilities associated with the information and information processing assets,

c) select and implement appropriate security controls to mitigate the risks,

d) ensure the availability of resources necessary to implement these controls,

e) monitor and review the implementation of these controls, and

f) continually improve the effectiveness of overall ISMS.

These steps shall be managed by the organization in accordance with the requirements of this standard.

4.2 Documentation Requirements

4.2.1 *General*

The Information Security Management System documentation shall include:

a) documented statements of an information security policy,
b) information security manual,
c) documented procedures required by this standard,
d) documents needed by the organization to ensure the effective implementation of ISMS, and
e) information security records required by this standard (*see* **4.2.4**).

NOTES

1 Where the term 'documented procedure' appears within this standard, this means that the procedure is established, documented, implemented and maintained.

2 The extent of the Information Security Management System documentation can differ from one organization to another due to:

a) the size of organization,
b) the complexity of selected controls, and
c) the competence of personnel.

3 The documentation can be in any form or type of medium.

4.2.2 *Information Security Manual*

The organization shall establish and maintain an Information Security Manual that includes:

a) the scope of the Information Security Management System, including details of and justification for any exclusions (*see* **1.2**), and
b) the documented procedures established for the Information Security Management System, or reference to them.

4.2.3 *Control of Documents*

Documents required by the Information Security Management System shall be controlled. Information Security records are a special type of documents and shall be controlled according to the requirements given in **4.2.4**.

The organization shall establish the controls needed:

a) to approve documents for adequacy prior to issue,
b) to review and update as necessary and reapprove documents,
c) to ensure that changes and the current revision status of documents are identified,
d) to ensure that relevant versions of applicable documents are available at points of use,
e) to ensure that documents remain legible and readily identifiable,
f) to ensure that documents of external origin are identified and their distribution controlled, and
g) to prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose.

4.2.4 *Control of Information Security Records*

Information Security records shall be established and maintained to provide evidence of conformity to requirements and of the effective operation of the Information Security Management System. Information security records shall remain legible, readily identifiable and retrievable. Controls established shall provide for the identification, storage, protection, retrieval, retention time and disposition of information security records.

5 MANAGEMENT RESPONSIBILITY

5.1 Management Commitment

Top management shall provide evidence of its commitment to the development and implementation of the Information Security Management System and continually improving its effectiveness by:

a) establishing the information security policy,
b) conducting periodic reviews, and
c) ensuring the availability of resources.

5.2 Trust and Confidence

Top management shall ensure that the information security requirements are determined on a continuous basis and fulfilled with the aim of enhancing the trust and confidence between the organization and its customers, trading partners and external agencies as well as within the organization (*see* **7.2.1** and **8.2.1**).

5.3 Information Security Policy

Top management shall ensure that the information security policy:

a) is appropriate to the business environment of the organization,
b) includes a commitment to comply with security requirements and continually improve the effectiveness of the Information Security Management System,
c) is communicated and understood within the organization, and
d) is reviewed for continuing suitability.

5.4 Responsibility, Authority and Communication

5.4.1 *Responsibility and Authority*

Top management shall ensure that the responsibilities, authorities and their interrelations for information security are defined and communicated within the organization.

5.4.2 *Management Representative*

Top management shall appoint a member of management who, irrespective of other responsibilities, shall have responsibility and authority that includes:

a) ensuring that steps needed for implementation of the Information Security Management System are established and maintained,
b) reporting to the top management on the performance of the Information Security Management System and any need for improvement, and
c) liaison with external parties on matters relating to the Information Security Management System.

5.4.3 *Internal Communication*

Top management shall ensure that appropriate communication processes are established within the organization and that communication takes place regarding the effectiveness of the Information Security Management System.

5.5 Provision of Resources

The top management shall provide the resources needed to implement and maintain the Information Security Management System and continually improve its effectiveness.

5.6 Management Review

5.6.1 *General*

Top management shall review the organization's Information Security Management System, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the Information Security Management System, including the Information Security policy. Records from management reviews shall be maintained (*see* **4.2.4**).

5.6.2 *Review Input*

The input to management review shall include, as a minimum, the following:

a) results of audits,
b) status of preventive and corrective actions,
c) follow-up actions from previous management reviews,
d) changes that could affect the Information Security Management System, and
e) recommendations for improvement.

5.6.3 *Review Output*

The output from the management review shall include any decisions and actions related to:

a) improvement of the effectiveness of the Information Security Management System, and
b) resource needs.

6 RESOURCE MANAGEMENT

6.1 Human Resources

6.1.1 *General*

Personnel performing work connected with information security shall be competent on the basis of appropriate education, training, skills and experience.

6.1.2 *Competence, Awareness and Training*

The organization shall :

a) determine the necessary competence for personnel performing work connected with information security,
b) provide training or take other actions to satisfy these needs,
c) evaluate the effectiveness of the actions taken,
d) ensure that its personnel are aware of the relevance and importance of their activities, and
e) maintain appropriate records of education, training, skills and experience (*see* **4.2.4**).

6.1.3 *Security in Job Definition and Resourcing*

6.1.3.1 *Security in job responsibilities*

Security roles and responsibilities for implementing and maintaining the security policy as well as any specific responsibilities for the protection of critical information and information processing assets shall be documented.

6.1.3.2 *Personnel screening*

The organization shall establish necessary verification checks at the time of recruitment.

6.1.3.3 *Terms and conditions and confidentiality agreements*

The terms and conditions of employment shall state the responsibility for information security. Where necessary, appropriate confidentiality or non-disclosure agreements shall be included.

6.2 Infrastructure

6.2.1 *General*

The organization shall determine, provide and maintain the infrastructure needed to achieve conformity to information security requirements. Infrastructure includes but is not limited to the following:

a) buildings, workspace and associated utilities,
b) information processing assets, both hardware and software, and
c) supporting services such as network communication.

6.2.2 *Information Security Infrastructure*

6.2.2.1 *Information security forum and coordination*

The organization shall establish a management framework to initiate and control the implementation of information security controls within the organization. Where necessary, the organization shall set up cross-functional team(s) to coordinate the implementation of security controls.

6.2.2.2 *Allocation of security responsibilities*

Responsibilities for the protection of all critical information and information processing assets including business continuity planning shall be defined.

6.2.2.3 *Authorization process for information processing facilities*

A management authorization process for new information processing facilities shall be established. The use of personal information processing facility for processing business information, which may cause new vulnerabilities, shall also be authorized.

6.2.2.4 *Specialist information security advice*

The organization shall nominate an individual to coordinate knowledge and experience, in-house as well as outside, to ensure consistency and provide help in security decision making.

6.2.2.5 *Cooperation between organizations*

Appropriate contacts with agencies such as law enforcement, regulatory bodies, information service providers, telecommunication operators shall be maintained to ensure that appropriate action can be quickly taken and advice obtained in the event of a security incident.

6.3 Work Environment

The organization shall determine and manage the work environment needed to achieve conformity to information security requirements.

7 PLANNING AND IMPLEMENTATION

7.1 Planning

7.1.1 *Information Security Management System Planning*

The organization shall ensure that:

a) the planning of the Information Security Management System is carried out in order to meet the requirements given in **4.1**, and
b) the integrity of the Information Security Management System is maintained when changes to the Information Security Management system are planned and implemented.

7.1.2 *Asset Classification and Control*

7.1.2.1 *Inventory and classification of assets*

All critical information assets and related information processing assets, including hardware, software and internal services, shall be identified and classified to indicate the need, priorities, impact and degree of protection required. Each of these assets shall have a nominated owner.

7.1.2.2 *Information labelling and handling*

Organization shall establish procedures for handling of critical information assets, including information assets in physical and electronic forms, according to their classification. All critical information assets that are classified as sensitive shall be suitably labelled.

7.1.3 *Risk Assessment*

An appropriate risk assessment shall be undertaken. The risk assessment shall identify the threat and vulnerabilities associated with the critical information and related information processing assets and shall determine the extent of risks commensurate with the degree of information security assurance required. For degree of information security assurance levels (Evaluation Assurance Levels-EALs) [*see* IS 14990 (Part 3)].

7.1.4 *Risk Management*

Following risk assessment, the organization shall identify and manage the areas of risks, based on the organization's information security policy and the degree of information security assurance required. For degrees of information security assurance levels (Evaluation Assurance Levels-EALs) [*see* IS 14990 (Part 3)].

7.2 Implementation

7.2.1 The organization shall select and implement all applicable security controls from the list given in Table 1, with due consideration to the requirements arising out of risk assessment and legal and contractual obligation. Any exclusions shall be suitably justified and documented. Requirement for any additional controls shall also be considered.

7.2.2 The organization shall determine the need for procedures for its ISMS and effectively implement the selected security controls. Monitoring and verification arrangements necessary to establish conformance to the security requirements shall be established and appropriate records maintained.

Table 1 Applicable Security Controls

(*Clause* 7.2.1)

Ref No.	Information Security Controls
1	**Physical and environmental security**
1.1	Secure Areas
1.1.1	*Physical security perimeter* — Organizations shall use security perimeters to protect areas which contain information processing facilities.
1.1.2	*Physical entry control* — Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
1.1.3	*Securing offices, rooms and facilities* — Secure areas shall be created in order to protect offices, rooms and facilities with special security requirements.
1.1.4	*Working in secure areas* — Additional controls and guidelines for working in secure areas shall be used to enhance the security provided by the physical controls protecting the secure areas.
1.1.5	*Isolated delivery and loading areas* — Delivery and loading areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
1.2	Equipment Security
1.2.1	*Equipment siting and protection* — Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
1.2.2	*Power supplies* — Equipment shall be protected from power failures and other electrical anomalies.
1.2.3	*Cabling security* — Power and telecommunication cabling carrying data or supporting information services shall be protected form interception or damage.
1.2.4	*Equipment maintenance* — Equipment shall be maintained in accordance with manufacturer's instruction and/or documented procedures to ensure its continued availability and integrity.
1.2.5	*Security of equipment off-premises* — Security procedures and controls shall be used to secure equipment used outside organization's premises.
1.2.6	*Secure disposal or re-use of equipment* — Information shall be erased from equipment prior to disposal or re-use.
1.3	General Controls
1.3.1	*Clear desk and clear screen policy* — Organizations shall have and implement a clear desk and a clear screen policy in order to reduce the risks of unauthorized access, loss of, and damage to information.
1.3.2	*Removal of property* — Equipment, information or software belonging to the organization shall not be removed without authorization.
2	**Communications and operations management**
2.1	Operational Procedures and Responsibilities
2.1.1	*Documented operating procedures* — The operating procedures identified in the security policy shall be documented and maintained.
2.1.2	*Operational change control* — Changes to information processing facilities and systems shall be controlled.
2.1.3	*Segregation of duties* — Duties and areas of responsibility shall be segregated in order to reduce opportunities for unauthorized modification or misuse of information or services.
2.1.4	*Separation of development and operational facilities* — Development and testing facilities shall be separated from operational facilities.
2.1.5	*External facilities management* — Prior to using external facilities management services, the risks shall be identified and appropriate controls agreed with the contractor, and incorporated into the contract.
2.2	System Planning and Acceptance
2.2.1	*Capacity planning* — Capacity demands shall be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.
2.2.2	*System acceptance* — Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to acceptance.
2.3	Protection Against Malicious Software
2.3.1	*Controls against malicious software* — Detection and prevention controls to protect against malicious software and appropriate user awareness procedures shall be implemented.
2.4	Housekeeping
2.4.1	*Information back-up* — Back-up copies of essential business information and software shall be taken regularly.
2.4.2	*Operator logs* — Operational staff shall maintain a log of their activities.
2.4.3	*Fault logging* — Faults shall be reported and corrective action taken.
2.5	Network Management
2.5.1	*Network controls* — A range of controls shall be implemented to achieve and maintain security in networks
2.6	Media Handling and Security
2.6.1	*Management of removable computer media* — The management of removable computer media, such as tapes, disks, cassettes and printed reports shall be controlled.
2.6.2	*Disposal of media* — Media shall be disposed off securely and safely when no longer required.
2.6.3	*Information handling procedures* — Procedures for the handling and storage of information shall be established in order to protect such information from unauthorized disclosure or misuse.

Table 1 (*Continued*)

Ref No.	Information Security Controls
2.6.4	*Security of system documentation* — System documentation shall be protected from unauthorized access.
2.7	Exchanges of Information and Software
2.7.1	*Information and software exchange agreements* — Agreements, some of which may be formal, shall be established for the electronic or manual exchange of information and software between organization.
2.7.2	*Security of media in transit* — Media being transported shall be protected from unauthorized access, misuse or corruption.
2.7.3	*Electronic commerce security* — Electronic commerce shall be protected against fraudulent activity, contract dispute and disclosure or modification of information.
2.7.4	*Security of electronic mail* — A policy for the use of electronic mail shall be developed and controls out in place to reduce security risks created by electronic mail.
2.7.5	*Security of electronic office systems* — Policies and guidelines shall be prepared and implemented to control the business and security risks associated with electronic office systems.
2.7.6	*Publicaly available systems* — There shall be a formal authorization process before information is made publicly available and the integrity of such information shall be protected to prevent unauthorized modification.
2.7.7	*Other forms of information exchange* — Procedures and controls shall be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities, mobile phones, satellite phones, wap devices, etc.
3	**Access Control**
3.1	Business Requirements for Access Control
3.1.1	*Access control policy* — Business requirements for access control shall be defined and documented, and access shall be restricted to what is defined in the access control policy.
3.2	User Access Management
3.2.1	*User registration* — There shall be a formal user registration and the de-registration procedure for granting access to all multi-user information systems and services.
3.2.2	*Privilege management* — The allocation and use of privileges shall be restricted and controlled.
3.2.3	*User password management* — The allocation of passwords shall be controlled through a formal management process.
3.2.4	*Review of user access rights* — a formal process shall be conducted at regular intervals to review users' access rights.
3.3	User Responsibilities
3.3.1	*Password use* — Users shall be required to follow good security practices in the selection and use of passwords.
3.3.2	*Unattended user equipment* — Users shall be required to ensure that unattended equipment has appropriate protection.
3.4	Network Access Control
3.4.1	*Policy on use of network services* — Users shall only have direct access to the services that they have been specifically authorized to use.
3.4.2	*Enforced path* — The path from the user terminal to the computer service shall be controlled.
3.4.3	*User authentication for external connections* — Access by remote users shall be subject to authentication.
3.4.4	*Node authentication* — Connections to remote computer systems shall be authenticated.
3.4.5	*Remote diagnostic port protection* — Access to diagnostic ports shall be securely controlled.
3.4.6	*Segregation in networks* — Controls shall be introduced in networks to segregate groups of information services, users and information systems.
3.4.7	*Network connection control* — The connection capability of users shall be restricted in shared networks, in accordance with the access control policy.
3.4.8	*Network routing control* — Shared networks shall have routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications.
3.4.9	*Security of network services* — A clear description of the security attributes of all network services used by the organization shall be provided.
3.5	Operating System Access Control
3.5.1	*Automatic terminal identification* — Automatic terminal identifications shall be used to authenticate connections to specific locations and to portable equipment.
3.5.2	*Terminal log-on procedures* — Access to information services shall use a secure log-on process.
3.5.3	*User identification and authentication* — All users shall have a unique identifier (user id) for their personal and sole use so that activities can be traced to the responsible individual.
3.5.4	*Password management system* — A password management system shall be in place to provide an effective, interactive facility which ensures quality passwords.
3.5.5	*Use of system utilities* — Use of system utility programmes shall be restricted and tightly controlled.
3.5.6	*Duress alarm to safeguard users* — Duress alarms shall be provided for users who might be the target of coercion.
3.5.7	*Terminal time-out* — Inactive terminals in high risk locations or serving high risk systems shall shut down after a defined period of inactivity to prevent access by unauthorized persons.
3.5.8	*Limitation of connection time* — Restrictions on connection times shall be used to provide additional security for high-risk applications.
3.6	Application Access Control
3.6.1	*Information access restriction* — Access to information and application system functions shall be restricted in accordance with the access control policy.
3.6.2	*Sensitive system isolation* — Sensitive systems shall have a dedicated (isolated) computing environment.

Table 1 (*Concluded*)

Ref No.	Information Security Controls
3.7	Monitoring System Access and Use
3.7.1	*Event logging* — Audit logs recording exceptions and other security-relevant events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
3.7.2	*Monitoring system use* — Procedures for monitoring use of information processing facilities shall be established and the result of the monitoring activities reviewed regularly.
3.7.3	*Clock synchronization* — Computer clocks shall be synchronized for accurate recording.
3.8	Mobile Computing and Teleworking
3.8.1	*Mobile computing* — A formal policy shall be in place and appropriate controls shall be adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments.
3.8.2	*Teleworking* — Policies and procedures shall be developed to authorize and control teleworking activities.
3.9	Security of Third Party access
3.9.1	*Identification of risks from third party access* — The risks associated with access to organizational information processing facilities by third parties shall be assessed and appropriate security controls implemented.
3.9.2	*Security requirements in third party contracts* — Arrangements involving third party access to organizational information processing facilities shall be based on a formal contract containing all necessary security requirements.
3.10	Outsourcing
3.10.1	*Security requirements in outsourcing contracts* — The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks and/or desk top environments shall be addressed in a contract agreed between the parties.
4	**Systems Development and Maintenance**
4.1	Control of Implementation of Software and Operational System
4.1.1	*Security requirements analysis and specification* — Business requirements for new systems, or enhancements to existing systems shall specify the requirements for controls.
4.2	Security in Application Systems
4.2.1	*Input data validation* — Data input to application systems shall be validated to ensure that it is correct and appropriate.
4.2.2	*Control of internal processing* — Validation checks shall be incorporated into systems to detect corruption of the data processed.
4.2.3	*Message authentication* — Message authentication shall be used for applications where there is a security requirement to protect the integrity of the message content.
4.2.4	*Output data validation* — Data output from an application system shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
4.3	Cryptographic Controls
4.3.1	*Policy on the use of cryptographic controls* — A policy on the use of cryptographic controls for the protection of information shall be developed and followed.
4.3.2	Encryption — Encryption shall be applied to protect the confidentiality of sensitive or critical information.
4.3.3	*Digital signatures* — Digital signatures shall be applied to protect the authenticity and integrity of electronic information.
4.3.4	*Non-repudiation services* — Non-repudiation services shall be used to resolve disputes about occurrence or non-occurrence of an event or action.
4.3.5	*Key management* — A key management system based on an agreed set of standards, procedures and methods shall be used to support the use of cryptographic techniques.
4.4	Security of System Files
4.4.1	*Control of operational software* — Control shall be applied to the implementation of software on operational systems.
4.4.2	*Protection of system test data* — Test data shall be protected and controlled.
4.4.3	*Access control to program source library* — Strict control shall be maintained over access to program source libraries.
4.5	Security in Development and Support Processes
4.5.1	*Change control procedures* — The implementation of changes shall be strictly controlled by the use of formal change control procedures to minimize the corruption of information systems.
4.5.2	*Technical review of operating system changes* — Application systems shall be reviewed and tested when changes occur.
4.5.3	*Restrictions on changes to software packages* — Modifications to software packages shall be discouraged and essential changes shall be made through control procedures.
4.5.4	*Covert channels and trojan code* — The purchase, use and modification of software shall be controlled and checked to protect against possible covert channels and trojan code.
4.5.5	*Outsourced software development* — Controls shall be applied to secure outsourced software development.

7.3 Business Continuity Management

A business continuity management process shall be implemented to reduce the disruption caused by disasters and security failures to an acceptable level through a combination of preventive and recovery controls. This process shall include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure timely resumption of essential operations.

The consequences of disasters, security failures and loss of service shall be suitably analyzed. Contingency plans, as necessary, shall be developed and implemented to ensure that the business operations can be restored within the required time scale. Such plans shall be maintained, practiced and kept up-to-date to ensure their continuing effectiveness.

7.4 Compliance with Legal Requirements

Organization shall identify all the applicable statutory, regulatory and contractual requirements concerning the design, operation, use and management of information systems, which may include the following:

a) Intellectual property rights (IPR),
b) Safeguarding of organizational records,
c) Data protection and privacy of personal information,
d) Prevention of misuse of information processing facilities,
e) Collection of evidence for legal action, and
f) Regulation of cryptographic controls.

8 MONITORING, REVIEW AND IMPROVEMENT

8.1 General

The organization shall plan and implement the monitoring, review and improvement steps needed:

a) to ensure conformity of the Information Security Management System to security requirements, and
b) to continually improve the effectiveness of the Information Security Management System.

8.2 Monitoring

8.2.1 *Internal Audit of ISMS*

The organization shall conduct internal audits of the ISMS at planned intervals to determine its:

a) conformance to the requirements of this standard and to the Information Security Management System requirements established by the organization, and
b) effective implementation and maintenance.

An audit programme shall be planned taking into consideration the importance of the selected controls, result of risk assessment as well as the results of previous audits. The audit criteria, scope, frequency and methods shall be defined.

Selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process.

Auditors shall not audit their own work.

The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (*see* **4.2.4**) shall be documented.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

8.2.2 *Technical Compliance Checking*

The organization shall apply suitable methods for monitoring the technical compliance of the information processing facilities and operational systems. These methods shall demonstrate the ability of the information processing facilities and operational systems to perform as desired. When planned results are not achieved, correction and corrective action shall be taken, as appropriate. Audit requirements and activities involving checks on information processing facilities and operational systems shall be carefully planned to minimize risk of disruptions to normal business. Access to operational system audit tools shall be restricted to protect any possible misuse or compromise.

8.2.3 *Incident Handling*

Security incidents and malfunctions shall be monitored and appropriate action initiated. Incidents affecting the security shall be reported through appropriate management channels as quickly as possible. All personnel concerned shall be made aware of the procedures for reporting the different types of incidents (security breach, threat, weakness or malfunction) that might have an impact on the information security.

The organization shall establish a formal disciplinary process for dealing with personnel who commit security breaches.

8.3 Analysis of Data

The organization shall determine, collect and analyze appropriate data to demonstrate the suitability and effectiveness of the Information Security Management System and to evaluate where continual improvement of the Information Security Management System can

be made. This shall include data generated as a result of monitoring and review and from other relevant sources.

The analysis of data shall provide information relating to:

a) conformance to security requirements; and
b) trends such as user behaviour, capacity utilization, network traffic to determine opportunities for preventive action.

8.4 Improvement

8.4.1 *Continual Improvement*

The organization shall continually improve the effectiveness of the Information Security Management System through the use of the information security policy, audit results, analysis of data, corrective and preventive actions and management review.

8.4.2 *Corrective Action*

The organization shall take action to eliminate the cause of security incidents in order to prevent recurrence. Corrective actions shall be appropriate to the effects of the security incidents encountered.

A documented procedure shall be established to define requirements for:

a) reviewing security incidents,
b) determining the causes of security incidents,
c) evaluating the need for action to ensure that security incidents do not recur,
d) determining and implementing action needed,
e) records of the results of action taken (*see* **4.2.4**), and
f) reviewing corrective action taken.

8.4.3 *Preventive Action*

The organization shall determine action to eliminate the causes of potential security incidents in order to prevent their occurrence. Preventive actions shall be appropriate to the effects of the potential problems.

A documented procedure shall be established to define requirements for:

a) determining potential security incidents and their causes,
b) evaluating the need for action to prevent occurrence of security incidents,
c) determining and implementing action needed,
d) records of results of action taken (*see* **4.2.4**), and
e) reviewing preventive action taken.

(*Continued from second cover*)

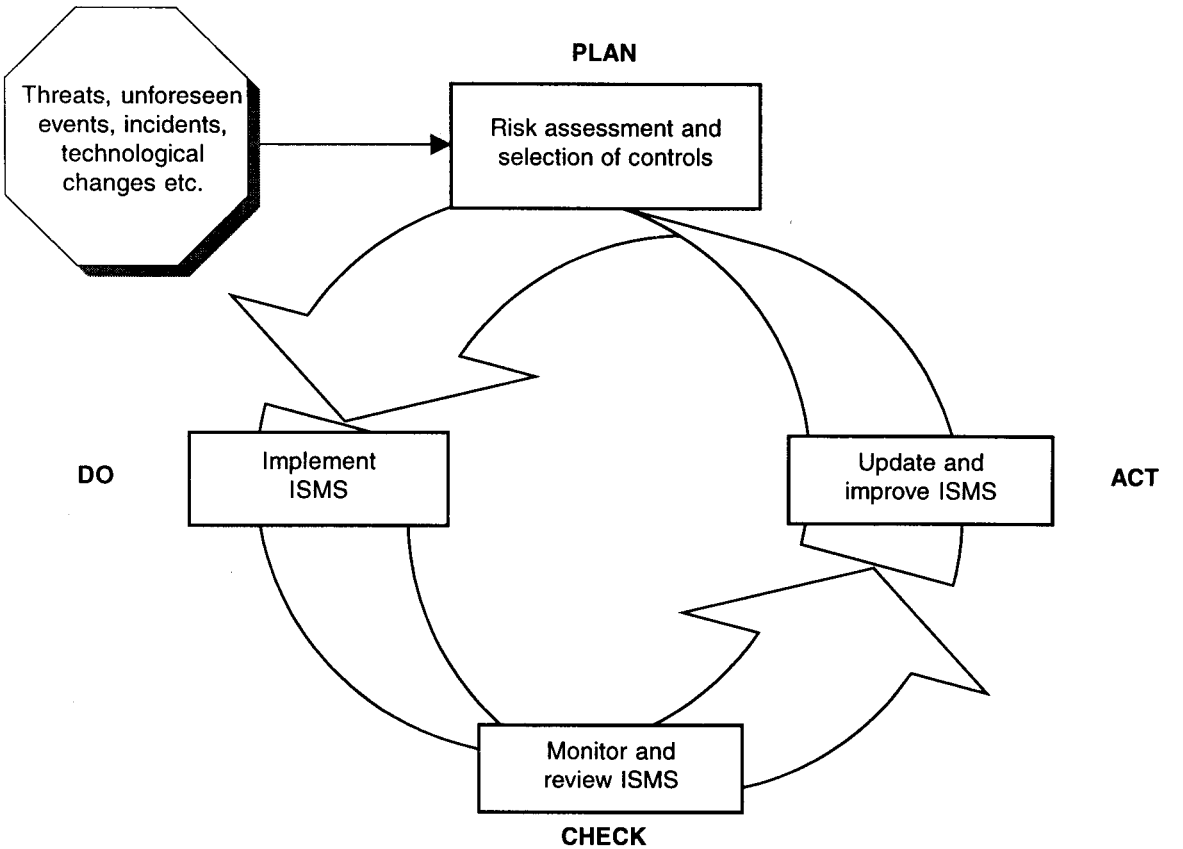

FIG. 1 MODEL OF A RISK-BASED INFORMATION SECURITY MANAGEMENT SYSTEM

While preparing this standard, assistance has been taken from BS 7799 (Part 2) : 1999 issued by the British Standards Institution. Extracts from BS 7799 (Part 2) : 1999 are included and reproduced with the permission of the British Standards Institution under licence number 2002SK/0122. Hard copies of British Standards are available from BSI Customer Services, 389 Chiswick High Road, London W4 4AL, United Kingdom.

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 1986 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc: No. LTD 38 (1973).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 323 01 31, 323 3375, 323 94 02

Telegrams: Manaksanstha
(Common to all offices)

Regional Offices:		Telephone
Central	: Manak Bhavan, 9 Bahadur Shah Zafar Marg NEW DELHI 110002	323 76 17, 323 38 41
Eastern	: 1/14 C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi KOLKATA 700054	337 84 99, 337 85 61 337 86 26, 337 91 20
Northern	: SCO 335-336, Sector 34-A, CHANDIGARH 160022	60 38 43 60 20 25
Southern	: C.I.T. Campus, IV Cross Road, CHENNAI 600113	254 12 16, 254 14 42 254 25 19, 254 13 15
Western	: Manakalaya, E9 MIDC, Marol, Andheri (East) MUMBAI 400093	832 92 95, 832 78 58 832 78 91, 832 78 92
Branches	: AHMEDABAD. BANGALORE. BHOPAL. BHUBANESHWAR. COIMBATORE. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. KANPUR. LUCKNOW. NAGPUR. NALAGARH. PATNA. PUNE. RAJKOT. THIRUVANANTHAPURAM. VISAKHAPATNAM.	

Printed at Simco Printing Press, Delhi