NCFM

NSE's CERTIFICATION IN FINANCIAL MARKETS

Information Security Auditors Module
Work Book

NATIONAL STOCK EXCHANGE OF INDIA LIMITED

Exchange Plaza, Bandra Kurla Complex,
Bandra (East), Mumbai 400 051 INDIA

Preface

Information security is gaining importance in today's corporate environment where a vast amount of information is being processed by organisations on a day to day basis. Information Security Audit is an audit of how the confidentiality, availability and integrity of an organization's information are assured. An information security audit is one of the best ways to determine the security of an organization's information without incurring the cost and other associated damages of a future security incident. It provides a fair and measurable tool, to examine how secure a site and processes and systems really are. Even today, it is possible to find a number of organizations where a written security policy does not exist. Security policies are a means of standardizing security practices by having them codified. When security practices are unwritten or informal, they may not be generally understood and practiced by all employees in the organization. Without a well defined audit of the systems and processes, there is a great risk of misuse, negligence, fraud and security incidences which could have large ramifications for the organizations and the market place. A well defined, objective, information security audit should form a part of every organization's policy.

In order to achieve this, a certification program for Information Security Auditors has been introduced under NCFM. Information Security Auditors will provide an independent, objective, and unbiased evaluation of systems, process, controls, in place in an organisation to effectively handle information and data integrity issues. The module would be useful for those who are assigned the task of undertaking information security audits for entities in the financial markets.

The module is being developed with the assistance of iSec Services Pvt. Ltd. (iSec), which is an information security consulting company providing information security compliance, assurance, audit, training etc.

We hope this workbook will guide those who are assigned the task of undertaking information security audits for entities in the financial markets.

Contact details of iSec Services Pvt. Ltd.

Delhi: B 1/1810, Vasant Kunj
New Delhi - 110 070
Telefax: (011) 26123369

Mumbai: B 102, Patliputra CHS
4, Bunglows
Mumbai - 400 053
Telefax: (022) 26300209

Email: contactus@isec.co.in
Website: www.isec.co.in

CONTENTS

Distribution of weights in the Information Security Auditors Module Curriculum

Information Security Auditors Module (Part-1)

Chapter No.	*Title*	*Weights (%)*
1.	Regulatory, Legal and Compliance issues in Information Security for Financial Markets	
	Section A	20
	Section B	25
2.	Business Continuity Planning	25
3.	Access Control	30

Information Security Auditors Module (Part-2)

Chapter No.	*Title*	*Weights (%)*
4.	Application Security	15
5.	Communications and Operations Management	15
6.	Physical and Environmental Security	30
7.	Security Management Practices	40

CHAPTER 1

REGULATORY, LEGAL AND COMPLIANCE ISSUES IN INFORMATION SECURITY FOR FINANCIAL MARKETS

SECTION-A

1.1 INTRODUCTION TO SECURITIES AND EXCHANGE BOARD OF INDIA (SEBI)

The SEBI Act of 1992 vests it with wide ranging powers to regulate the stock exchanges and securities industry to promote their orderly functioning. It can frame or issue rules, regulations, directives, guidelines, and norms in respect of primary markets and secondary markets intermediaries operating in the market and certain financial institutions. The role of SEBI is to create conditions for efficient mobilisation and allocation of resources through the securities markets, stimulating competition and encouraging innovations. SEBI provides a high degree of protection to investors with regard to their rights and interests through adequate, accurate and authentic information and disclosure of such information on a continuous basis. In short the SEBI endeavors to create an effective surveillance mechanism and encourage responsible and accountable autonomy on the part of all players in the market.

Role of SEBI in the Development of Stock and Capital Markets

SEBI and the Primary Market

(i) It is no longer necessary for companies to obtain prior permission for raising of capital from the market.

(ii) SEBI has issued guidelines for all companies for disclosure of information and protection of investor's interest.

(iii) For issues above Rs.100 Crore book building requirement has been introduced.

(iv) Bankers to the Issue and portfolio managers have to be registered with SEBI.

SEBI and the Secondary Market

(i) The governing bodies of Stock Exchange have been recognised, restructured and broad based.
(ii) SEBI has drawn up a comprehensive plan of inspecting all Stock Exchanges to determine the extent of compliance with SEBI guidelines.
(iii) Computerised screen based trading has been introduced on all major stock exchanges.
(iv) All Stock Exchanges (SEs) have been directed to set up a clearing house or cleaning corporation.
(v) SEBI has accepted the Dave Committee recommendations on improving the working of OTCEI.
(vi) The Bombay Stock Exchange (BSE) has been asked to reduce trading period from 14 days to 7 days for B group shares. The BSE has been allowed to introduce a revised Carry Forward System.
(vii) Brokers, sub-brokers have been brought under the regulatory framework of SEBI. Penal action is taken by SEBI against any member for violation of SEBI Act.
(viii) Registers to Issues and Share Transfer Agents have been brought under SEBI.
(ix) Merchant Banking activity has been statutory brought under SEBI.
(x) SEBI has issued guidelines pertaining to buy-back of shares.

SEBI and Investor Protection

SEBI has taken various steps to strengthen investor confidence and interest in the Secondary Market. This includes rationalisation and refinement of margin system such as mark to market margin, volatility margin etc.

SEBI and Mutual Funds

All Mutual Funds have to be registered with the SEBI. UTI has also been brought under SEBI. SEBI has issued guidelines to provide for portfolio disclosure, standardisation of accounting policies, valuation norms for determining net asset value and pricing.
SEBI has been entrusted with a challenging, difficult and complex job.

1.2 SECURITIES CONTRACTS (REGULATION) ACT 1956

An Act to prevent undesirable transactions in securities by regulating the business of dealing therein, by providing for certain other matters connected therewith.

We will take a look at few sections under SCRA.

Section 3: Establishment and Incorporation of Board

(i) With effect from such date as the Central Government may, by notification, appoint, there shall be established, for the purposes of this Act, a Board by the name of the Securities and Exchange Board of India.

(ii) The Board shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract, and shall, by the said name, sue or be sued.

(iii) The head office of the Board shall be at Bombay.

(iv) The Board may establish offices at other places in India.

Section 11: Functions of Board

(1) Subject to the provisions of this Act, it shall be the duty of the Board to protect the interests of investors in securities and to promote the development of, and to regulate the securities market, by such measures as it thinks fit.

(2) Without prejudice to the generality of the foregoing provisions, the measures referred to therein may provide for—

- (i) regulating the business in stock exchanges and any other securities markets;
- (ii) registering and regulating the working of stock brokers, sub-brokers, share transfer agents, bankers to an issue, trustees of trust deeds, registrars to an issue, merchant bankers, underwriters, portfolio managers, investment advisers and such other intermediaries who may be associated with securities markets in any manner;

  (a) registering and regulating the working of the depositories, (participants), custodians of securities, foreign institutional investors, credit rating agencies and such other intermediaries as the Board may, by notification, specify in this behalf;
- (iii) registering and regulating the working of (venture capital funds and collective investment schemes), including mutual funds;
- (iv) promoting and regulating self-regulatory organisations;

(v) prohibiting fraudulent and unfair trade practices relating to securities markets;

(vi) promoting investors' education and training of intermediaries of securities markets;

(vii) prohibiting insider trading in securities;

(viii) regulating substantial acquisition of shares and take over of companies;

(ix) calling for information from, undertaking inspection, conducting inquiries and audits of the (stock exchanges, mutual funds, other persons associated with the securities market), intermediaries and self-regulatory organisations in the securities market;

(a) calling for information and record from any bank or any other authority or board or corporation established or constituted by or under any Central, State or Provincial Act in respect of any transaction in securities which is under investigation or inquiry by the Board;

(x) performing such functions and exercising such powers under the provisions of Securities Contracts (Regulation) Act, 1956 (42 of 1956), as may be delegated to it by the Central Government;

(xi) levying fees or other charges for carrying out the purposes of this section;

(xii) conducting research for the above purposes;

(a) calling from or furnishing to any such agencies, as may be specified by the Board, such information as may be considered necessary by it for the efficient discharge of its functions;

(xiii) performing such other functions as may be prescribed.

(2.1) Without prejudice to the provisions contained in sub-section 2, the Board may take measures to undertake inspection of any book, or register, or other document or record of any listed public company or a public company (not being intermediaries referred to in another section) which intends to get its securities listed on any recognised stock exchange where the Board has reasonable grounds to believe that such company has been indulging in insider trading or fraudulent and unfair trade practices relating to securities market.

(3) Notwithstanding anything contained in any other law for the time being in force while exercising the powers under (clause ix or clause ix(a) of sub-section 2 or sub-section 2.1, the Board shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:—

(i) the discovery and production of books of account and other documents, at such place and such time as may be specified by the Board;

(ii) summoning and enforcing the attendance of persons and examining them on oath;

(iii) inspection of any books, registers and other documents of any person referred to in section 12, at any place;

(iv) inspection of any book, or register, or other document or record of the company referred to in sub-section (2A);

(v) issuing commissions for the examination of witnesses or documents.

(4) Without prejudice to the provisions contained in sub-sections (1), (2), (2A) and (3) and section 11B, the Board may, by an order, for reasons to be recorded in writing, in the interests of investors or securities market, take any of the following measures, either pending investigation or inquiry or on completion of such investigation or inquiry, namely:—

(i) suspend the trading of any security in a recognised stock exchange;

(ii) restrain persons from accessing the securities market and prohibit any person associated with securities market to buy, sell or deal in securities;

(iii) suspend any office-bearer of any stock exchange or self-regulatory organisation from holding such position;

(iv) impound and retain the proceeds or securities in respect of any transaction which is under investigation;

(v) attach, after passing of an order on an application made for approval by the Judicial Magistrate of the first class having jurisdiction, for a period not exceeding one month, one or more bank account or accounts of any intermediary or any person associated with the securities market in any manner involved in violation of any of the provisions of this Act, or the rules or the regulations made thereunder:

Provided that only the bank account or accounts or any transaction entered therein, so far as it relates to the proceeds actually involved in violation of any of the provisions of this Act, or the rules or the regulations made thereunder shall be allowed to be attached;

(vi) direct any intermediary or any person associated with the securities market in any manner not to dispose of or alienate an asset forming part of any transaction which is under investigation:

Provided that the Board may, without prejudice to the provisions contained in sub-section (2) or sub-section (2A), take any of the measures specified in clause (*d*) or clause (*e*) or clause (f), in respect of any listed public company or a public company (not being intermediaries referred to in section 12) which intends to get its securities listed on any recognised stock exchange where the Board has reasonable grounds to believe that such company has been indulging in insider trading or fraudulent and unfair trade practices relating to securities market:

Provided further that the Board shall, either before or after passing such orders, give an opportunity of hearing to such intermediaries or persons concerned

Section 18: Returns and Reports

(1) The Board shall furnish to the Central Government at such time and in such form and manner as may be prescribed or as the Central Government may direct, such returns and statements and such particulars in regard to any proposed or existing programme for the promotion and development of the securities market, as the Central Government may, from time to time, require.

(2) Without prejudice to the provisions of sub-section (1), the Board shall, within (ninety) days after the end of each financial year, submit to the Central Government a report in such form, as may be prescribed, giving a true and full account of its activities, policy and programmes during the previous financial year.

(3) A copy of the report received under sub-section (2) shall be laid, as soon as may be after it is received, before each House of Parliament.

Section 27: Offences by Companies

(1) Where an offence under this Act has been committed by a company, every person who at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to any punishment provided in this Act, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

(2) Notwithstanding anything contained in sub-section (1), where an offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

Explanation: For the purposes of this section,—

(i) “company” means any body corporate and includes a firm or other association of individuals; and

(ii) "director", in relation to a firm, means a partner in the firm.

1.3 SECURITIES AND EXCHANGE BOARD OF INDIA ACT, 1992

An Act to provide for the establishment of a Board to protect the interests of investors in securities and to promote the development of, and to regulate, the securities market and for matters connected therewith or incidental thereto.

We will take a look at few sections under SEBI Act,

Section 10: Transfer of Assets, Liabilities, etc., of existing securities and Exchange Board to the Board

(1) On and from the date of establishment of the Board, -

(i) Any reference to the existing Securities and Exchange Board in any law other than this Act or in any contract or other instrument shall be deemed as a reference to the Board;

(ii) All properties and assets, movable and immovable, of, or belonging to, the existing Securities and Exchange Board, shall vest in the Board;

(iii) All rights and liabilities of the existing Securities and Exchange Board shall be transferred to, and be the rights and liabilities of, the Board;

(iv) Without prejudice to the provisions of clause (c), all debts, obligations and liabilities incurred, all contracts entered into and all matters and things engaged to be done by, with or for the existing Securities and Exchange Board immediately before that date, for or in connection with the purpose of the said existing Board shall be deemed to have been incurred, entered into or engaged to be done by, with or, for, the Board;

(v) All sums of money due to the existing Securities and Exchange Board immediately before that date shall be deemed to be due to the Board;

(vi) All suits and other legal proceedings instituted or which could have been instituted by or against the existing Securities and Exchange Board immediately before that date may be continued or may be instituted by or against the Board; and

(vii) Every employee holding any office under the existing Securities and Exchange Board immediately before that date shall hold his office in the Board by the same tenure and upon the same terms and conditions of service as respects remuneration, leave, provident fund, retirement and other terminal benefits as he would have held such office if the Board had not been established and shall continue to do so as an employee of the Board or until the expiry of the period of six months from that date if such employee opts not to be the employee of the Board within such period.

(2) Notwithstanding anything contained in the Industrial Disputes Act, 1947 (14 of 1947), or in any other law for the time being in force, absorption of any employee by the Board in its regular service under this section shall not entitle such employee to any compensation under that Act or other law and no such claim shall be entertained by any court, tribunal or other authority.

Section 11A: Matters to be disclosed by the companies

Without prejudice to the provisions of the Companies Act, 1956 (1 of 1956), the Board may, for the protection of investors, specify by regulations,

(1) The matters relating to issue of capital, transfer of securities and other matters incidental thereto; and

(2) The manner in which such matters, shall be disclosed by the companies.

Section 12: Registration of Stock-Brokers, Sub-Brokers, Share Transfer Agents, etc.

(1) No stock-broker, sub-broker, share transfer agent, banker to an issue, trustee of trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and such other intermediary who may be associated with securities market shall buy, sell or deal in securities except under, and in accordance with, the conditions of a certificate of registration obtained from the Board in accordance with the regulations made under this Act.

Provided that a person buying or selling securities or otherwise dealing with the securities market as a stock broker, sub-broker, share transfer agent, banker to an issue, trustee of trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and such other intermediary who may be associated with securities market immediately before the establishment of the Board for which no registration certificate was necessary prior to such establishment, may continue to do so for a period of three months from such establishment or, if he has made an application for such registration within the said period of three months, till the disposal of such application.

Provided further that any certificate of registration, obtained immediately before the commencement of the Securities Laws (Amendment) Act, 1995, shall be deemed to have been obtained from the Board in accordance with the regulations providing for such registration.

(i) No depository, participant, custodian of securities, foreign institutional investor, credit rating agency, or any other intermediary associated with the securities market as the Board may by notification in this behalf specify, shall buy or sell or deal in securities except under and in accordance with the conditions of a certificate of registration obtained from the Board in accordance with the regulations made under this Act:

Provided that a person buying or selling securities or otherwise dealing with the securities market as a depository, [participant] custodian of securities, foreign institutional investor or credit rating agency immediately before the commencement of the Securities Laws (Amendment) Act, 1995, for which no certificate of registration was required prior to such commencement, may continue to buy or sell securities or otherwise deal with the securities market until such time regulations are made under clause (d) of sub-section (2) of section 30.

(ii) No person shall sponsor or cause to be sponsored or carry on or caused to be carried on any venture capital funds or collective investment scheme including mutual funds, unless he obtains a certificate of registration from the Board in accordance with the regulations:

Provided that any person sponsoring or causing to be sponsored, carrying or causing to be carried on any venture capital funds or collective investment scheme operating in the securities market immediately before the commencement of the Securities Laws (Amendment) Act, 1995, for which no certificate of registration was required prior to such commencement, may continue to operate till such time regulations are made under clause (d) of sub-section (2) of section 30.

(2) Every application for registration shall be in such manner and on payment of such fees as may be determined by regulations.

(3) The Board may, by order, suspend or cancel a certificate of registration in such manner as may be determined by regulations.

Provided that no order under this sub-section shall be made unless the person concerned has been given a reasonable opportunity of being heard.

Section 12A: Prohibition of Manipulative and Deceptive Devices, Insider Trading and Substantial Acquisition of Securities or Control

No person shall directly or indirectly,

(1) Use or employ, in connection with the issue, purchase or sale of any securities listed or proposed to be listed on a recognised stock exchange, any manipulative or deceptive device or contrivance in contravention of the provisions of this Act or the rules or the regulations made there under.

(2) Employ any device, scheme or artifice to defraud in connection with issue or dealing in securities which are listed or proposed to be listed on a recognised stock exchange.

(3) Engage in any act, practice, course of business which operates or would operate as fraud or deceit upon any person, in connection with the issue, dealing in securities which are listed or proposed to be listed on a recognised stock exchange, in contravention of the provisions of this Act or the rules or the regulations made there under.

(4) Engage in insider trading;

(5) Deal in securities while in possession of material or non-public information or communicate such material or non-public information to any other person, in a manner which is in contravention of the provisions of this Act or the rules or the regulations made there under.

(6) Acquire control of any company or securities more than the percentage of equity share capital of a company whose securities are listed or proposed to be listed on a recognised stock exchange in contravention of the regulations made under this Act.

Section 15: Accounts and Audit

(1) The Board shall maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form as may be prescribed by the Central Government in consultation with the Comptroller and Auditor-General of India.

(2) The accounts of the Board shall be audited by the Comptroller and Auditor-General of India at such intervals as may be specified by him and any expenditure incurred in connection with such audit shall be payable by the Board to the Comptroller and Auditor-General of India.

(3) The Comptroller and Auditor-General of India and any other person appointed by him in connection with the audit of the accounts of the Board shall have the same rights and privileges and authority in connection with such audit as the Comptroller and Auditor-General generally has in connection with the audit of the Government accounts and, in particular, shall have the right to demand the production of

books, accounts, connected vouchers and other documents and papers and to inspect any of the offices of the Board.

(4) The accounts of the Board as certified by the Comptroller and Auditor-General of India or any other person appointed by him in this behalf together with the audit report thereon shall be forwarded annually to the Central Government and that Government shall cause the same to be laid before each House of Parliament.

Section 15A: Penalty for Failure to Furnish Information, Return, etc.

If any person, who is required under this Act or any rules or regulations made there under,

(1) To furnish any document, return or report to the Board, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(2) To file any return or furnish any information, books or other documents within the time specified therefore in the regulations, fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(3) To maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Section 15G: Penalty for Insider Trading

If any insider who,

(1) Either on his own behalf or on behalf of any other person, deals in securities of a body corporate listed on any stock exchange on the basis of any unpublished price-sensitive information; or

(2) Communicates any unpublished price-sensitive information to any person, with or without his request for such information except as required in the ordinary course of business or under any law; or

(3) Counsels, or procures for any other person to deal in any securities of any body corporate on the basis of unpublished price-sensitive information, shall be liable to a penalty (of twenty-five crore rupees or three times the amount of profits made out of insider trading, whichever is higher).

Section H: Penalty for Non-Disclosure of Acquisition of Shares and Takeovers

If any person, who is required under this Act or any rules or regulations made thereunder, fails to,

(1) Disclose the aggregate of his shareholding in the body corporate before he acquires any shares of that body corporate; or

(2) Make a public announcement to acquire shares at a minimum price; or

(3) Make a public offer by sending letter of offer to the shareholders of the concerned company; or

(4) Make payment of consideration to the shareholders who sold their shares pursuant to letter of offer, he shall be liable to a penalty (of twenty-five crore rupees or three times the amount of profits made out of such failure, whichever is higher)

Section 15HA: Penalty for Fraudulent and Unfair Trade Practices

If any person indulges in fraudulent and unfair trade practices relating to securities, he shall be liable to a penalty of twenty-five crore rupees or three times the amount of profits made out of such practices, whichever is higher.

Section 26: Cognizance of Offences by Courts

(1) No court shall take cognizance of any offence punishable under this Act or any rules or regulations made there under, save on a complaint made by the Board.

(2) No court inferior to that of a Metropolitan Magistrate or a Judicial Magistrate of the first class shall try any offence punishable under this Act.

1.4 DEPOSITORIES ACT, 1996

An Act to provide for regulation of depositories in securities and for matters connected therewith or incidental thereto.

Section 2: Definitions

(1) **Depository** means a company formed and registered under the Companies Act, 1956 (1 of 1956), and which has been granted a certificate of registration under sub-section (1A) of section 12 of the Securities and Exchange Board of India Act, 1992 (15 of 1992);

Section 3: Certificate of Commencement of Business by Depositories

(1) No depository shall act as a depository unless it obtains a certificate of commencement of business from the Board.

(2) A certificate granted under sub-section (1) shall be in such form as may be specified by the regulations.

(3) The Board shall not grant a certificate under sub-section (1) unless it is satisfied that the depository has adequate systems and safeguards to prevent manipulation of records and transactions:

Provided that no certificate shall be refused under this section unless the depository concerned has been given a reasonable opportunity of being heard.

Section 4: Agreement between Depository and Participant

(1) A depository shall enter into an agreement with one or more participants as its agent.

(2) Every agreement under sub-section (1) shall be in such form as may be specified by the bye-laws.

Section 5: Services of Depository

Any person, through a participant, may enter into an agreement, in such form as may be specified by the bye-laws, with any depository for availing its services.

Section 6: Surrender of Certificate of Security

(1) Any person who has entered into an agreement under section 5 shall surrender the certificate of security, for which he seeks to avail the services of a depository, to the issuer in such manner as may be specified by the regulations.

(2) The issuer, on receipt of certificate of security under sub-section (1), shall cancel the certificate of security and substitute in its records the name of the depository as a registered owner in respect of that security and inform the depository accordingly.

(3) A depository shall, on receipt of information under sub-section (2), enter the name of the person referred to in sub-section (1) in its records, as the beneficial owner.

Section 13: Furnishing of Information and Records by Depository and Issuer

(1) Every depository shall furnish to the issuer information about the transfer of securities in the name of beneficial owners at such intervals and in such manner as may be specified by the bye-laws.

(2) Every issuer shall make available to the depository copies of the relevant records in respect of securities held by such depository.

Section 14: Option to opt out in Respect of any security

(1) If a beneficial owner seeks to opt out of a depository in respect of any security he shall inform the depository accordingly.

(2) The depository shall on receipt of intimation under sub-section (1) make appropriate entries in its records and shall inform the issuer.

(3) Every issuer shall, within thirty days of the receipt of intimation from the depository and on fulfillment of such conditions and on payment of such fees as may be specified by the regulations, issue the certificate of securities to the beneficial owner or the transferee, as the case may be.

Section 17: Rights and Obligations of Depositories, etc.

(1) Subject to the provisions of this Act, the rights and obligations of the depositories, participants and the issuers whose securities are dealt with by a depository shall be specified by the regulations.

(2) The eligibility criteria for admission of securities into the depository shall be specified by the regulations.

1.5 RULES AND REGULATIONS OF SEBI

Securities and Exchange Board of India (Depositories and Participants) Regulations, 1996.

Section 3: Application for Grant of Certificate of Registration

(1) An application for the grant of a certificate of registration as a depository shall be made to the Board by the sponsor in Form A, shall be accompanied by the fee specified in Part A of the Second Schedule and be paid in the manner specified in Part B thereof.

(2) The application shall be accompanied by draft bye-laws of the depository that is proposed to be set-up.

Section 4: Application to Conform to the Requirements

An application in Form A which is not complete in all respects and does not conform to the instructions specified therein shall be rejected:

Provided that before rejecting any such application, the sponsor shall be given in writing an opportunity to remove, within thirty days of the date of communication in this regard, the objections indicated by the Board:

Provided further that the Board may, on being satisfied that it is necessary to extend the period specified in the first proviso, extend such period by such further time as it thinks necessary in order to enable the applicant to remove the objections indicated by the Board.

Section 5: Furnishing of Information, Clarification and Personal Representation

(1) The Board may require the sponsor to furnish such further information or clarification regarding matters relevant to the activity of the depository for the purpose of consideration of the application.

(2) The sponsor or his authorised representative shall, if so required, appear before the Board for personal representation, in connection with the grant of certificate of registration.

Section 10: Application for grant of Certificate of Commencement of Business

A depository which has been granted a certificate of registration under regulation 7, shall within one year from the date of issue of such certificate make an application to the Board for commencement of business in Form C.

Section 11: Application to Conform to the requirements

Any application in Form C which is not complete in all respects and does not conform to instructions specified therein shall be rejected:

Provided that before rejecting any such application, the applicant shall be given in writing an opportunity to remove within thirty days of the date of communication in this regard, the objections indicated by the Board:

Provided further that the Board may, on being satisfied that it is necessary to extend the period specified in the first proviso, extend such period by such further time as it thinks necessary in order to enable the applicant to remove the objections indicated by the Board.

Section 12: Furnishing of Information, Clarification and Personal Representation

(1) The Board may require the depository to furnish such further information or clarification regarding matters relevant for the grant of certificate of commencement of business.

(2) The depository or its authorised representative, if so required, shall appear before the Board for personal representation in connection with the grant of certificate of commencement of business.

Section 26: Rights and Obligations of Depositories, etc.

The depositories, participants, issuers, and issuers' agents, in addition to the rights and obligations laid down in the Depositories [Act] and the bye-laws shall have the rights and obligations arising from the agreements entered into by them.

Section 27: Depository to declare specific securities eligible

Every depository shall, in its bye-laws, state the specific securities which are eligible for being held in dematerialised form in the depository.

Section 28: Security eligible for dematerialisation

The following securities shall be eligible for being held in dematerialised form in a depository:

(1) shares, scrips, stocks, bonds, debentures, debenture stock or other marketable securities of a like nature in or of any incorporated company or other body corporate;

(2) units of mutual funds, rights under collective investment schemes and venture capital funds, commercial paper, certificates of deposit, securitised debt, money market instruments, (Government securities) and unlisted securities shall also be similarly eligible for being held in dematerialised form in a depository;

(3) any other security as may be specified by the Board from time to time, by way of a notification in the Official Gazette and subject to such conditions as it may deem fit to impose.

Section 29: Agreement between Depository and Issuer

(1) Either on the issuer or on the investor exercising an option to hold his securities with a depository in dematerialised form, the issuer shall enter into an agreement with the depository to enable the investor to dematerialise the securities:

Provided that no agreement shall be required to be entered into where the depository itself is an issuer of securities,

Provided further that no such agreement shall be required to be entered into where the State or the Central Government is the issuer of Government securities.

(2) Where the issuer has appointed a Registrar to the Issue or Share Transfer Agent, who has been granted certificate of registration by the Board under sub-section (1) of section 12 of the Act, the depository shall enter into a tripartite agreement with the issuer and the Registrar to the Issue or Share Transfer Agent, as the case may be, in respect of the securities to be declared by the depository as eligible to be held in dematerialised form.

Section 30: Systems and Procedures

Every depository shall have systems and procedures which will enable it to co-ordinate with the issuer or its agent, and the participants, to reconcile the records of ownership of securities with the issuer or its agent, as the case may be, and with participants, on a daily basis.

Section 31: Connectivity

Every depository shall maintain continuous electronic means of communication with all its participants, issuers or issuers' agents, as the case may be, clearing houses and clearing corporations of the stock exchanges and with other depositories.

Section 32: Transfer to be effected only after payment

The depository shall satisfy the Board that it has a mechanism in place to ensure that the interest of the persons buying and selling securities held in the depository are adequately protected and shall register the transfer of a security in the name of the transferee only after the depository is satisfied that payment for such transfer has been made.

Section 34: Internal Monitoring, Review and Evaluation of Systems and Controls

Every depository shall have adequate mechanisms for the purposes of reviewing, monitoring and evaluating the depository's controls systems, procedures and safeguards.

Section 35: External Monitoring, Review and Evaluation of Systems and Controls

Every depository shall cause an inspection of its controls, systems, procedures and safeguards to be carried out annually and forward a copy of the report to the Board.

Section 36: Insurance against risks

Every depository shall take adequate measures including insurance to protect the interests of the beneficial owners against risks likely to be incurred on account of its activities as a depository.

Section 37: Manner of keeping records

Where records are kept electronically by the depository, it shall ensure that the integrity of the automatic data processing systems is maintained at all times and take all precautions necessary to ensure that the records are not lost, destroyed or tampered with and in the event of loss or destruction, ensure that sufficient back up of records is available at all times at a different place.

Section 38: Records to be maintained

(1) Every depository shall maintain the following records and documents, namely:—

- (i) records of securities dematerialised and rematerialised;
- (ii) the names of the transferor, transferee, and the dates of transfer of securities;
- (iii) a register and an index of beneficial owners;
  - (a) details of the holding of the securities of beneficial owners as at the end of each day;

(iv) records of instructions received from and sent to participants, issuers, issuers' agents and beneficial owners;

(v) records of approval, notice, entry and cancellation of pledge or hypothecation, as the case may be;

(vi) details of participants;

(vii) details of securities declared to be eligible for dematerialisation in the depository; and

(viii) such other records as may be specified by the Board for carrying on the activities as a depository.

(2) Every depository shall intimate the Board the place where the records and documents are maintained.

(3) Subject to the provisions of any other law the depository shall preserve records and documents for a minimum period of five years.

Section 59: Board's Right to inspect

The Board may appoint one or more persons as inspecting officer to undertake inspection of the books of account, records, documents and infrastructure, systems and procedures, or to investigate the affairs of a depository, a participant, a beneficial owner an issuer or its agent for any of the following purposes, namely:

(1) to ensure that the books of account are being maintained by the depository, participant, issuer or its agent in the manner specified in these regulations;

(2) to look into the complaints received from the depositories, participants, issuers, issuers' agents, beneficial owners or any other person;

(3) to ascertain whether the provisions of the Act, the Depositories [Act], the bye-laws, agreements and these regulations are being complied with by the depository, participant, beneficial owner, issuer or its agent;

(4) to ascertain whether the systems, procedures and safeguards being followed by a depository, participant, beneficial owner, issuer or its agent are adequate;

(5) to *suo motu* ensure that the affairs of a depository, participant, beneficial owner, issuer or its agent, are being conducted in a manner which are in the interest of the investors or the securities market.

1.6 RULES, REGULATIONS AND BYELAWS OF NSEIL (NATIONAL STOCK EXCHANGE INDIA LIMITED)

Rules of NSEIL

The rules are divides in four categories:
(1) Board
(2) Executive Committee
(3) Trading Membership
(4) Disciplinary Proceeding, Penalties, Suspension and Expulsion

We will take a look at rules pertaining to Information Security under each category.

(1) Board

Rule 1: The Board of Directors (herein referred to as Board) of National Stock Exchange of India Limited, constituted in accordance with the provisions of the Articles of Association of the Company, may organise, maintain, control, manage, regulate and facilitate the operations of the Exchange and of securities transactions by trading members of the Exchange, subject to the provisions of the Securities Contracts (Regulation) Act, 1956 and Rules thereunder, Securities and Exchange Board of India Act, 1992 and any directives thereunder and the trading regulations which RBI may prescribe from time to time for money market instruments.

Rule 3: Subject to the provisions of the Securities Contracts (Regulation) Act, 1956 and Rules thereunder, the Securities and Exchange Board of India Act, 1992 and any directives thereunder and the trading regulations which RBI may prescribe from time to time for money market instruments, the Board is empowered to make Bye Laws, Rules and Regulations from time to time, for all or any matters relating to the conduct of business of the Exchange, the business and transactions of trading members between trading members inter-se as well as the business and transactions between trading members and persons who are not trading members, and to control, define and regulate all such transactions and dealings and to do such acts and things which are necessary for the purposes of the Exchange.

Rule 5: The Board is empowered to delegate, from time to time, to the Executive Committee(s) or to the Managing Director or to any person, such of the powers vested in it and upon such terms as they may think fit, to manage all or any of the affairs of the Exchange and from time to time, to revoke, withdraw, alter or vary all or any of such powers.

Rule 9: The Members of the Board and of such committees as may be identified by the Ethics Committee shall adhere to the Code of Conduct as may be prescribed by the Board or Ethics Committee from time to time.

Guidelines for Fair Practices/ Code of conduct for Public Representative and SEBI Nominee Directors

Rule 10:
A. Meetings and Minutes

Public Representative / SEBI Nominee Directors shall:

(i) endeavour to attend all the board meetings and shall be liable to vacate his office if he remains absent for three consecutive meetings of the Board of Directors or does not attend 75% of the total meetings of the Board in a calendar year;

(ii) not participate in the discussion of any subject matter in which any conflict of interest exists or arises, whether pecuniary or otherwise, and in such cases the same shall be disclosed and recorded in the minutes of the meeting;

(iii) not encourage the circulation of agenda papers during the meeting, unless circumstances require;

(iv) meet themselves at least once in 6 months separately, if necessary, to exchange views on critical issues;

(v) offer their comments on the draft minutes and ensure that the same are incorporated in the final minutes;

(vi) insist on the minutes of the previous meeting being placed for approval in subsequent meeting;

(vii) endeavour to have the date of next meeting fixed at each Board Meeting in consultation with other members of the Board;

(viii) endeavour that in case where all the items of the agenda of a meeting were not covered for want of time, the next meeting is held within 15 days for considering the remaining items.

Rule 10:
B. Strategic Planning

Public Representative / SEBI Nominee Directors shall:

(i) participate in the formulation and execution of strategies in the best interest of the exchanges and contribute towards pro-active decision making at the Board level;

(ii) give benefit of his experience and expertise to the Exchange and provide assistance in strategic planning and execution of decisions when the Board is in the throes of a raging controversy.

Rule 10:
C. Regulatory Compliances

Public Representative / SEBI Nominee Directors shall:

(i) endeavour to ensure that the Exchange abides by all the provisions of the SEBI Act, Securities Contracts (Regulation) Act, Rules, Regulations framed thereunder and the circulars, directions issued by the Government / SEBI from time to time;

(ii) endeavour compliance at all levels so that the regulatory system does not suffer any breaches;

(iii) endeavour to ensure that the Exchange takes commensurate steps to honour the time limit prescribed by SEBI for corrective action;

(iv) not support any decision in the meeting of the Board which may adversely affect the interest of investors and shall report forthwith any such decision to SEBI;

(v) endeavour that the arbitral award is given within the period stipulated in the Bye Laws, Rules or Regulations of the Exchange and in any case, the award is delivered within 15 days after the final meeting.

Rule 10:
D. General Responsibility

Public Representative / SEBI Nominee Directors shall:

(i) be punctual and participate actively in the proceedings of the Meetings;

(ii) place priority for redressing Investor Grievance, encourage fair trade practice, to become engine for the right growth of the securities industry;

(iii) make use of every reasonable opportunity to enhance and improve his level of knowledge and endeavour to analyse and administer the exchange issues with professional competence, fairness, impartiality, efficiency and effectiveness;

(iv) submit the necessary disclosures/ statement of holdings/dealings in securities as required by the Exchange from time to time as per their Rules or Articles of Association;

(v) unless otherwise required by law, maintain confidentiality and shall not divulge/ disclose any information obtained in the discharge of their duty. Further, no such information shall be used for personal gain;

(vi) maintain the highest standards of personal integrity, truthfulness, honesty and fortitude in discharge of his duties in order to inspire public confidence and shall not engage in acts discreditable to his responsibilities;

(vii) avoid any interest or activity which is in conflict with the conduct of his official duties;

(viii) perform his duties in an independent and objective manner and avoid activities that may impair, or may appear to impair, his independence or objectivity;

(ix) perform his duties with a positive attitude and constructively support open communication, creativity, dedication and compassion;

(x) not engage in any act involving moral turpitude, dishonesty, fraud, deceit or misrepresentation or any other act prejudicial to the administration of the Exchange.

(2) Executive Committee

Powers of Executive Committee

Rule 5: The Executive Committee of each trading segment shall have such responsibilities and powers as may be delegated to it by the Board from time to time which may, inter alia, include the following responsibilities and powers to be discharged in accordance with the provisions of the Bye Laws and Rules:

(i) approving securities for admission to the relevant Official List for NSE securities;

(ii) admitting trading members;

(iii) listing fees payable by the company whose securities are admitted to dealings on the Exchange;

(iv) continuance of listed status of the company whose securities are admitted to dealings on the Exchange;

Government/SEBI Representative

Rule 9: The Government and SEBI shall nominate on the Executive Committee from time to time, not more than one person each to be referred to as "Government Nominee".

Rule 10: Any vacancy caused by resignation, withdrawal of nomination, death or otherwise of such a nominated Government Representative shall be filled in by a similarly nominated person.

(3) Trading Membership

Rule 1: The rights and privileges of a trading member shall be subject to the Bye Laws, Rules and Regulations of the Exchange.

Rule 2: All trading members of the Exchange shall have to register themselves prior to commencing operations on the Exchange, with the Securities and Exchange Board of India.

Rule 3: The following persons shall be eligible to become trading members of the Exchange:

(i) individuals
(ii) registered firms
(iii) bodies corporate
(iv) companies as defined in the Companies Act, 1956 and
(v) such other persons or entities as may be permitted under the Securities Contracts (Regulation) Rules, 1957 as amended from time to time.

Rule 6: No person shall be eligible to be admitted to the trading membership of the Exchange unless the person satisfies:

(i) the requirements prescribed in that behalf under the Securities Contracts (Regulation) Act, 1956, and the Rules framed thereunder and under the Securities and Exchange Board of India Act, 1992, and
(ii) such additional eligibility criteria as the Board or relevant authority may prescribe for the different classes of trading members and trading segments from time to time.

Rule 6:
A. Certification

No person shall be eligible to be admitted to the trading membership of the Exchange unless he has passed the Certification Programme conducted by the Exchange for such Trading segment of the Exchange as it may determine from time to time.

Rule 7: Unless otherwise specified by the relevant authority, membership for any person shall be restricted to only one trading segment.

Rule 8: Trading member of any trading segment may trade in NSE securities applicable to that segment.

(4) Disciplinary Proceedings, Penalties, Suspension and Expulsion

Disciplinary Jurisdiction

Rule 1: The relevant authority may expel or suspend and/or fine under censure and/or warn and/or withdraw any of the membership rights of a trading member if it be guilty of contravention, non-compliance, disobedience, disregard or evasion of any of the Bye Laws, Rules and Regulations of the Exchange or of any resolutions, orders, notices, directions or decisions or rulings of the Exchange or the relevant authority or of any other Committee or officer of the Exchange authorised in that behalf or of any conduct, proceeding or method of business which the relevant authority in its absolute discretion deems dishonourable, disgraceful or unbecoming a trading member of the Exchange or inconsistent with just and equitable principles of trade or detrimental to the interests, good name or welfare of the Exchange or prejudicial or subversive to its objects and purposes.

Penalty for Misconduct, Unbusiness like Conduct and Unprofessional Conduct

Rule 2: In particular and without in any way limiting or prejudicing the generality of the provisions in Rule (1) above, a trading member shall be liable to expulsion or suspension or withdrawal of all or any of its membership rights and/or to payment of a fine and/or to be censured, reprimanded or warned for any misconduct, unbusiness like conduct or unprofessional conduct in the sense of the provision in that behalf contained herein.

Misconduct

Rule 3: A trading member shall be deemed guilty of misconduct for any of the following or similar acts or omissions namely:

(i) **Fraud:** If it is convicted of a criminal offence or commits fraud or a fraudulent act which in the opinion of the relevant authority renders it unfit to be a trading member;

(ii) **Violation:** If it has violated provisions of any statute governing the activities, business and operations of the Exchange, trading members and securities business in general;

(iii) **Improper Conduct:** If in the opinion of the relevant authority it is guilty of dishonourable or disgraceful or disorderly or improper conduct on the Exchange or of willfully obstructing the business of the Exchange;

(iv) **Breach of Rules, Bye Laws and Regulations:** If it shields or assists or omits to report any trading member whom it has known to have committed a breach or evasion of any Rule, Bye-law and Regulation of the Exchange or of any resolution, order, notice or direction thereunder of the relevant authority or of any Committee or officer or the Exchange authorised in that behalf;

(v) **Failure to comply with Resolutions:** If it contravenes or refuses or fails to comply with or abide by any resolution, order, notice, direction, decision or ruling of the relevant authority or of any Committee or officer of the Exchange or other person authorised in that behalf under the Bye Laws, Rules and Regulations of the Exchange;

(vi) **Failure to submit to or abide by Arbitration:** If it neglects or fails or refuses to submit to arbitration or to abide by or carry out any award, decision or order of the relevant authority or the Arbitration Committee or the arbitrators made in connection with a reference under the Bye Laws, Rules and Regulations of the Exchange;

(vii) **Failure to testify or give information:** If it neglects or fails or refuses to submit to the relevant authority or to a Committee or an officer of the Exchange authorised in that behalf, such books, correspondence, documents and papers or any part thereof as may be required to be produced or to appeal and testify before or cause any of its partners, attorneys, agents, authorised representatives or employees to appear and testify before the relevant authority or such Committee or officer of the Exchange or other person authorised in that behalf;

(viii) **Failure to submit Special Returns:** If it neglects or fails or refuses to submit to the relevant authority within the time notified in that behalf special returns in such form as the relevant authority may from time to time prescribe together with such other information as the relevant authority may require whenever circumstances arise which in the opinion of the relevant authority make it desirable that such special returns or information should be furnished by any or all the trading members;

(ix) **Failure to submit Audited Accounts:** If it neglects or fails or refuses to submit its audited accounts to the Exchange within such time as may be prescribed by the relevant authority from time to time.

(x) **Failure to compare or submit accounts with Defaulter:** If it neglects or fails to compare its accounts with the Defaulters' Committee or to submit to it a statement of its accounts with a defaulter or a certificate that it has no such account or if it makes a false or misleading statement therein;

(xi) **False or misleading Returns:** If it neglects or fails or refuses to submit or makes any false or misleading statement in its clearing forms or returns required to be submitted to the Exchange under the Bye Laws, Rules and Regulations;

(xii) **Vexatious complaints:** If it or its agent brings before the relevant authority or a Committee or an officer of the Exchange or other person authorised in that behalf a charge, complaint or suit which in the opinion of the relevant authority is frivolous, vexatious or malicious;

(xiii) **Failure to pay dues and fees:** If it fails to pay its subscription, fees, arbitration charges or any other money which may be due by it or any fine or penalty imposed on it.

Rule 5: A trading member shall be deemed guilty of unprofessional conduct for any of the following or similar acts or omissions namely:

(i) Business in Securities in which dealings not permitted: If it enters into dealings in securities in which dealings are not permitted.

Rule 14: The penalty of suspension, withdrawal of all or any of the membership rights, fine, censure or warning may be inflicted singly or conjointly by the relevant authority. The penalty of expulsion may be inflicted by the relevant authority.

Rule 21: When a trading member ceases to be such under the provisions of these Bye Laws otherwise than by death, default or resignation it shall be as if such trading member has been expelled by the relevant authority and in that event all the provisions relating to expulsion contained in these Rules shall apply to such trading member in all respects.

Rule 22:

(i) The relevant authority shall require a trading member to suspend its business when it fails to maintain or provide further security as prescribed in the Bye Laws and Regulations and the suspension shall continue until it pays the necessary amount by way of security.

(ii) **Penalty for Contravention:** A trading member who is required to suspend its business under clause (a) shall be expelled by the relevant authority if it acts in contravention of the provisions of the Bye Laws.

Rule 24: The Relevant authority for the purpose of this section shall be the Disciplinary Action Committee as may be constituted by the Board of Directors from time to time. At any point of time, not less than sixty percent of the members of the Disciplinary Action Committee shall be from among non-trading members, who shall be nominated by the Exchange with the prior approval of Securities and Exchange Board of India. The Disciplinary Action Committee may delegate any of its powers under this Section to the Managing Director.

Regulations of NSEIL

The Regulations framed hereunder shall be known as National Stock Exchange (Capital Market) Trading Regulations, 1994. These Regulations shall be in addition to the provisions of the Securities Contracts (Regulation) Act, 1956, the Securities Contracts (Regulation) Rules, 1957, Securities and Exchange Board of India Act, 1992 and Rules and Byelaws of National Stock Exchange of India Limited (NSEIL), as may be applicable to Trading Members and Participants.

These Regulations shall be applicable to all Trading Members and Participants to the extent specified herein, in the Capital Market Segment of National Stock Exchange. They shall be subject to jurisdiction of the Courts of Mumbai irrespective of the place of business of Trading Members in India.

Trading System

(1) The Exchange shall provide an Automated Trading facility in all the Securities admitted for dealings on the Capital Market and such a system shall herein after be referred to as **NEAT** (**N**ational **E**xchange for **A**utomated **T**rading) system.

(2) Trading on the Exchange shall be allowed only through approved Workstation(s) located at approved locations for the office(s) of a Trading Member. If an approved workstation of a Trading Member is connected by LAN or any other way to other workstations at any place it shall require an approval of the Exchange.

(3) Each Trading Member/Participant shall have a unique identification number which shall be provided by the Exchange and which shall be used to log on (sign on) to the system.

(4) A Trading Member/Participant shall have a non-exclusive permission to use the Trading system as provided by the Exchange in the ordinary course of business as Trading Member/Participant.

(5) A Trading Member/Participant shall not have any title, rights or interest with respect to Trading System, its facilities, software and the information provided by the NEAT.

(6) The permission to use the Trading System shall be subject to payment of such charges as the Exchange may from time to time prescribe in this regard.

(7) A Trading Member/Participant shall not, permit itself or any other person(s) to:

(i) use the software provided by the Exchange for any purpose other than the purpose as approved and specified by the Exchange.

(ii) use the software provided by the Exchange on any equipment other than the workstation approved by the Exchange.

(iii) copy, alter, modify or make available to any other person the software provided by the Exchange.

(iv) use the software in any manner other than the manner as specified by the Exchange.

(v) attempt directly or indirectly to decompile, dissemble or reverse engineer the same.

(8) A Trading Member/Participant shall not, by itself or through any other persons on his behalf, publish, supply, show or make available to any other person or reprocess, retransmit, store or use the facilities of the Trading System or the information provided by the Trading System except with the explicit approval of the Exchange and in the ordinary course of business to complete the transactions on the Exchange.

Trading Members and Users

(1) Trading Members and participants shall be entitled to appoint, subject to such terms and conditions as may be specified by the Relevant Authority from time to time,

(i) Authorised Persons;

(ii) Approved Users.

(2) Each Trading Member/Participant shall be permitted to appoint such number of Users as may be notified from time to time by the Exchange.

(3) The appointment of Users shall be subject to such terms and conditions as the Exchange may from time to time prescribe.

(4) Each User shall be given an unique identification number through which he shall have access to the system.

(5) A User can access the system through a password and can change such password from time to time.

(6) A Trading Member/Participant or its Users thereof shall maintain complete secrecy of its password.

(7) A User shall be required to change his password at the end of the password expiry period. The password expiry period shall be prescribed by the Exchange from time to time.

(8) (i) Only persons who are registered as Trading Members and Participants in accordance with provisions of the Bye-Laws, Rules and Regulations of the Exchange or are agents of Trading Members for whom an application has been made to the Exchange by the Trading Members in accordance with the format specified by the Managing Director from time to time may be approved as Users.

(ii) No person shall be admitted as a User who is under 21 years of age.

(iii) No person shall be admitted as a User against whom any disciplinary action has been taken by the Exchange or any other Stock Exchange.

(iv) No Trading Member/Participant shall without permission of the Exchange take into his employment a former Trading Member or User of such Trading Member as a User, if such Trading Member or User is one against whom any disciplinary action has been taken by the Exchange or any other Stock Exchange.

(9) The Exchange shall have a right to reject any application made under 8 (i) or at any time withdraw any approval previously granted, or suspend a User temporarily from access to the system. Such suspension may be

conditional and may be revoked on the fulfillment of condition specified, if any, to the satisfaction of the Exchange.

(10) A Trading Member/Participant desiring to change the User Id or cancel the authority given to its User to operate the trading system on its behalf shall intimate the Exchange in writing, in such form and manner as the Exchange may specify, immediately on taking such action and obtain confirmation from the Exchange of having received such intimation, and of the disabling of the particular User by the Exchange. However the Trading Member/Participant will continue to be liable for all the activities reported on the basis of such or previous User Id undertaken upto a period of 24 hours after his obtaining a confirmation as mentioned above from the Exchange. The Trading Member shall cancel all his outstanding orders in respect of such User.

(11) Whenever a User of the Trading Member/Participant ceases to act in such or any capacity with the Trading Member then each such Trading Member shall inform the Exchange, within 24 hours, the name and other particulars of such User.

(12) No application shall be made by any Trading Member/Participant under 8(i), if such a person for whom such an application is made, is already an approved User of any other Trading Member/Participant.

(13) The Exchange shall notify different level of the Users for each workstation provided. These levels shall define the access to the system by the Users and shall include a provision for inquiry only on the terminal, provision for order entry and trading, or such others as may be specified by the Exchange.

(14) The Exchange may change the status of the User of the Trading Member from Trader to Inquiry only where circumstances warrant and intimate to such Trading Member any reasons thereof.

(15) A Trading Member/Participant, shall not access the trading system using a different Trading Member/Participant or User Id other than the one allotted to him.

(16) A User shall not attempt to aid in or access the trading system using the Trading Member code from a location other than the Trading Member's location, unless he has the express prior approval of the Trading Member for whom he is an approved User.

(17) A Trading Member/Participant who wants the Exchange to reset his password, has to make a request in writing signed by the Trading Member/Participant indicating his Broker Id and User Id. A Trading Member/Participant shall not make a request for resetting the password of any other Trading Member/Participant.

Dealings in Securities

(1) Dealings shall be permitted on the Exchange in securities as provided in these Regulations and Byelaws of the Exchange and for such categories of Trading Members/Participants, trade types, market types, settlement

periods and for such trading hours as the Exchange may specify from time to time.

(2) The Exchange may at its discretion at any time suspend trading in particular securities as it deems fit. Such suspension shall take effect, on such conditions and in such time and manner as the Exchange may prescribe in this regard.

(3) The Exchange may also revoke suspension of trading in securities at any time.

(4) Trading Members may trade on the Trading System in securities that are admitted for dealing on the Exchange, either on behalf of their constituents or on their own account unless otherwise specified by the relevant authority and trading shall be subject to such conditions as the Exchange may prescribe from time to time.

(i) When a Trading Member enters an order on behalf of a Mutual Fund or any of its Schemes, Foreign Institutional Investor or any of its sub-account holders, then such a Trading Member shall at the time of entering orders on behalf of such clients, enter the unique code in respect of such Mutual Fund or its Scheme, Foreign Institutional Investor or any of its sub-accounts in such format and with effect from such date as may be notified by the Exchange.

(5) The Exchange may, at any time restrict conditionally or unconditionally a Trading Member/Participant from dealing in a specified security.

(6) The Trading Member/Participant shall continue to be liable for all trades executed on the system for orders entered into the system on his behalf. Trading Member/Participant shall be responsible for all the actions of their authorised persons.

(7) A Trading Member shall be responsible for all the actions including trades originating through or with the use of all following variables - Trading Member Id, User Id, valid User password at that point of time. However if the Trading Member satisfies the Exchange that the action(s) and /or trade(s) took place due to fraud or misrepresentation by any other person other than his authorised person(s) and that the action(s) and/or trades did not originate from any of his approved workstations, the Exchange may issue such directions as it considers just and reasonable. The directions may include referring the matter to arbitration and /or annulment of trade(s) so effected.

(8) **Particulars of Unique Client Code:** When a Trading Member enters an order on behalf of a Constituent, then such a Trading Member shall at the time of entering orders on behalf of such Constituent, enter the unique code in respect of such Constituent in such format and with effect from such date as may be notified by the Exchange. Every Trading Member shall be responsible to furnish particulars of unique client codes of each of his Constituents to the Exchange in such form, manner, at such intervals and within such time as may be specified by the Exchange from time to time.

(9) The Trading Member shall, in respect of all transactions in a scrip, where total quantity of shares bought/sold under proprietary or any single client code is more than 0.5 % of the number of equity shares of the company listed on the Exchange, disclose to the Exchange immediately upon execution of the trade, the name of the scrip, name of the Constituent, quantity of shares bought / sold and the traded price. The Exchange shall disseminate such information on the same day after market hours to the general public. The information is to be furnished to the Exchange in such format and within such time as may be prescribed by the Exchange from time to time.

(10) Every Trading Member and the Sub-broker shall comply with the SEBI (Central Database of Market Participants) Regulations, 2003. The Trading Member shall ensure that his Constituents comply with the SEBI (Central Database of Market Participants) Regulations, 2003.

Trade Operations

(1) Trading Members shall ensure that appropriate confirmed order instructions are obtained from the constituents before placement of an order on the system and shall keep relevant records or documents of the same and of the completion or otherwise of these orders thereof.

(2) The Trading Member shall make available to his constituent the NEAT order number and copies of the order confirmation slip / modification slip be dispatched to the constituent.

(3) However where the Trading Member has accumulated the orders of several constituents to meet the requirement of the Regular lot quantity he may give his own order number referred to as the Reference Number, together with a reference to the NEAT Order Number, to the constituent.

(4) The procedures and conditions for amendment or cancellation of orders would be subject to such conditions and as specified by the Exchange from time to time.

(5) Trading Members shall be solely responsible for the accuracy of details of orders entered into the trading system including orders entered on behalf of his constituents.

(6) A potential trade match shall be subject to validation for turnover limits. A turnover limit refers to the maximum value of trades that a Trading Member/Participant will be permitted to execute on the trading system. Subject to the provisions relating to capital adequacy norms and turnover limits as may be specified by SEBI or other regulatory authorities from time to time, turnover limits shall be prescribed by the Exchange, Trading Member wise, for all transactions done by him on the Exchange. The Exchange may specify from time to time the manner in which all regulations relating to turnover limits shall apply.

(7) Trades generated on the system are irrevocable and 'locked in'. The Exchange may specify from time to time the markets in which trade cancellation can be effected.

(8) Where a trade cancellation is permitted and Trading Member wishes to cancel a trade, it may be done only with the approval of the Exchange and in the following manner:

(i) The Trading Member wishing to cancel the trade shall initiate a cancellation request to the Exchange. The counter Trading Member to the trade too will have to put in his cancellation request separately.

(ii) Where a Trading Member initiates such request the onus shall be on the Trading Member to ensure that he receives a written request from the constituent.

(iii) Where a trade cancellation request(s) comes to Exchange from only one party to trade and is/are pending with the Exchange as a result of it being not confirmed by the counterparty to such trade till such time as may be notified by the Exchange, such request may be cancelled at the discretion of the Exchange.

(iv) The Exchange shall not consider any request for a Trade Cancellation after such period after the market close on a trading day as may be notified from time to time.

(v) The Exchange shall not give the reasons for rejection or approval of any such trade cancellation request.

(vi) The Exchange may cancel a trade suo- motu without any request by either of the parties to the trade at any time without giving any reason thereof which cancellation shall be final and binding upon the parties to the trade. In the event of such cancellation, Trading Member shall be entitled to cancel relative contract(s) with his constituents.

Margin Requirements

(1) Subject to the provisions as contained in the Exchange Bye-laws and such other regulations as may be in force, every Trading Member/Participant shall in respect of trades in which he is a party, deposit a margin with Exchange authorities, in the Exchange. Whenever a margin is payable by a Participant, it shall pay such margins directly to the Exchange, unless otherwise directed by the Exchange including VaR margins on an upfront basis.

(2) The Exchange shall prescribe from time to time the securities, the settlement periods and trade types for which margin would be attracted.

(3) The margin shall be deposited with the Exchange within such time as may be notified by the Exchange from time to time.

Composition of Additional Capital and Margins

(A) The relevant authority may specify the requirements of additional capital and margins for the Trading Members. The minimum cash component of such additional capital and margins shall be 50% and the cash component may be in the form of cash or cash equivalents. Cash equivalents are as follows:

(i) Cash equivalent shall include FDRs, bank guarantees, government securities and units of the schemes of liquid mutual funds or government securities mutual funds (by whatever name called which invest in government securities.

(ii) The margin for government securities shall be such as may be prescribed from time to time by the relevant authority but not less than 10%.

(iii) The margin for units of the schemes of liquid mutual funds or government securities mutual funds (by whatever name called which invest in government securities) shall be such as may be prescribed from time to time by the relevant authority but not less than 10% of Net Asset Value (NAV).

(iv) The bank guarantees shall be considered as cash equivalent only if the guarantees have been provided by the banks whose networth is more than Rs. 500 crores; Provided further

- the relevant authority may lay down the exposure limits either in rupee terms or otherwise subject to limits set by SEBI.
- the exposure as mentioned above would include guarantees provided by the bank for itself or for others as well as debt or equity securities of the bank which have been deposited by members for additional capital or margins.

(B) The relevant authority specifies the following securities, including equity shares, units of mutual funds which could be considered as eligible securities and margin for the purpose of non-cash component of base minimum capital, additional capital and margin.

(i) Equity shares classified in Group I at the Exchange in accordance with the parameters of volatility and liquidity as stipulated by SEBI and specified by relevant authority shall be eligible as security for the non-cash component of the additional capital and margin, subject to margin equivalent to the respective VaR of the equity shares.

(ii) Units of all mutual funds shall also be eligible security for the purpose of non-cash component of additional capital and margin subject to a margin equivalent to the VaR of the unit’s NAV plus any exit load charged by the mutual fund.

(iii) The valuation of the equity shares and units of mutual funds above shall be done on a daily basis.

(iv) The eligible shares for the purpose of the securities portion of the base minimum capital shall only be those which are classified as Group I, in terms of the parameters of volatility and liquidity as stipulated by SEBI and specified by the relevant authority subject to a standard margin of 15%. The valuation for these shares would be done atleast once a week.

(4) The Exchange shall prescribe from time to time such categories of securities that would be eligible for a margin deposit as also the method of valuation and amount of securities that would be required to be so deposited against the margin amount.

(5) The Exchange shall at any time, exempt any Trading Member/Participant or category of Trading Members/Participants from all or any of the margin requirements stipulated or modify the specific requirements for a Trading Member/Participant.

(6) The procedure for refund/adjustment of margins will be such as may be notified by the Exchange from time to time.

(7) The Exchange shall from time to time, impose upon any particular Trading Member/Participant or category of Trading Member/Participant any special or other margin requirement.

Order Management

(1) **Order Type:** The Exchange shall stipulate from time to time, the kinds of orders that a Trading Member can place in the system which may include Normal order, Special Term order, etc. as also the order attributes that he could place thereon.

(2) **Order Attributes:**

(i) The Exchange shall from time to time allow various order attributes subject to restrictions as prescribed in the trading parameters, which will include

- ON STOP
- DISCLOSED QUANTITY
- IMMEDIATE OR CANCEL
- GOOD TILL DAY
- GOOD TILL CANCELED
- GOOD TILL DATE

(ii) The attributes of special term order shall be specified by the Exchange from time to time and shall include

- MINIMUM FILL
- ALL OR NONE

(iii) The Exchange shall specify the order types and order attributes permitted for different market types, trade types, etc.

(3) **Modification and Cancellation of Orders**

(i) A Trading Member shall be permitted to modify or cancel his orders, provided a trade has not already taken place in respect of that order.

(ii) The order can be modified by effecting changes in the order input parameters in the manner and on such condition as specified by the Exchange.

(iii) The modified order shall lose or retain its time priority as per the trading parameter set by the Exchange.

(4) **Order Validation:** Orders entered into the Trading System by Trading Members shall be subject to various validation requirements as prescribed by the Exchange from time to time including trading parameters, turnover limits and/or other restrictions placed on traded securities. Orders that do not meet the validation checks will not be accepted by the Trading System.

(5) **Matching Rules:**

(i) The Exchange shall specify from time to time the kinds of order books that shall be maintained on the system, the order matching algorithms and the matching rules and parameters that shall be followed therein.

(ii) The Exchange may modify or change the matching algorithms relevant to any market or order books any time where it is necessary to do so.

(iii) Where the Exchange feels that it is in the interests of the market to do so, it may at any time make unavailable any particular order books or forms of matching, in the case of a particular security or Trading Member or to the market as a whole.

(iv) Without prejudice to the generality of the above, the order matching rules would include the following:

(a) Orders in the Normal market will be matched on price - time priority basis.

(b) The best buy order shall match with the best sell order. For trading on price, the best buy order would be the one with the highest price and the best sell order would be the one with the lowest price.

(c) The trading system shall store orders for the purpose of matching in different order books including:

- Regular lot book
- Special Term order book
- On Stop order book

Contract Note

(1) Every Trading Member shall issue a contract note to his constituents for trades executed in such format as may be prescribed by the Exchange from time to time with all relevant details as required therein to be filled in and issued in such manner and within such time as prescribed by the Exchange.

(2) A contract note shall be signed by a Trading Member or his Authorised signatory or constituted Attorney.

(3) The Contract Notes shall be numbered with unique running serial number commencing from one which shall be reset only at the beginning of every financial year. In case separate series are maintained in respect of different dealing offices of the trading member, then the dealing office name or code shall be prefixed to the serial number.

(4) Notwithstanding anything contained in Regulation 3.5, a contract note may also be issued by a Trading Member in electronic form in such format as may be prescribed by the Exchange from time to time duly authenticated by means of a digital signature as specified in the Information Technology Act, 2000 and the Rules made thereunder.

Brokerage

(1) All the orders entered on the Trading System shall be at prices exclusive of brokerage.

(2) Trading Members shall charge brokerage at rates not exceeding such scale as the Exchange may from time to time prescribe.

(3) A Trading Member shall charge brokerage separately to their constituents and this shall be indicated separately from the price, in the contract note.

Turnover Limits

The Exchange has a right to impose limits with or without reasons on turnover position of Trading Members.

(1) The Exchange shall set turnover limits for each Trading Member.

(2) The Exchange shall use the total consideration for the trade to maintain this limit.

(3) The turnover figure for each member would include the next possible potential match (i.e. the next trade to be executed)

Interest, Dividend, Rights/Bonus And Calls: The buyer shall be entitled to receive all coupons, dividends, bonus, rights and other privileges which may appertain to securities cum coupon, cum dividend, cum bonus, cum rights, etc. and the seller shall be entitled to receive all coupons, dividends, bonus issues, rights and other privileges which may appertain to securities sold ex coupon, ex dividend, ex bonus, ex rights, etc.

Margin from the constituents: The Trading Members shall have the right to demand from its constituents the Margin Deposit which the member has to provide under these Trading Regulations in respect of the business done by the Members for such constituents. The Trading Members shall buy securities on behalf of the constituent only on the receipt of margin of minimum such percentage as the relevant authority may decide from time to time, on the price of the securities proposed to be purchased, unless the constituent already has an equivalent credit with the broker. The Trading Member may not, if so desire, collect such a margin from Financial Institutions, Mutual funds and Foreign Institutional Investors. The Trading Members shall buy securities on behalf of the constituent only on the receipt of margin of minimum of such percentage as the relevant authority may decide from time to time, on the price of the securities proposed to be sold, unless the Trading Member has received the securities to be sold with valid transfer documents to his satisfaction prior to such sale. The Trading Member may not, if so desire, collect such a margin from Financial Institutions, Mutual funds, and Foreign Institutional Investors. The Trading Member shall obtain a written undertaking from the constituents that the latter shall when called upon to do so forthwith from time to time provide a Margin Deposit and/or furnish additional Margin as required under these Rules and Regulations in respect of the business done for the constituent by and/or as agreed upon by constituent with the Trading Member concerned. The Trading Member may keep the unutilised margin deposits of his client in bank deposits and pay interest on the same at such rate as may be mutually agreed in writing between the Trading Member and his constituent out of the interest accrued on the said deposits.

Collection Of Securities Transaction Tax: Every Trading Member shall remit to the Exchange the Securities Transaction Tax (STT), in respect of the transactions entered into by him on the Exchange either on his own behalf or on behalf of his Constituents in accordance with the procedures prescribed by the Relevant Authority from time to time for the calculation and collection of such tax. Any Trading Member who fails to make the payment in accordance with the procedures prescribed by the Relevant Authority from time to time would be liable for such consequences of nonpayment including but not limited to withdrawal of trading facility, appropriation fro m the monies of the Trading Member, withholding of pay-outs, etc. as may be prescribed from time to time.

Annual Accounts And Audit

(1) Each Trading Member shall prepare annual accounts for each financial year ending on 31st March or such other date as advised to the Exchange.

(2) The Assets and Liabilities of the Trading Member's business shall be brought into account in the balance sheet at such amounts and shall be

classified and described therein in such manner that the balance sheet gives a true and fair view of the state of affairs of such business as at the date to which it is made up.

(3) Each Trading Member shall furnish to the Exchange, its audited financial statement and such report shall be furnished not later than six months after the end of the Trading Member's financial year, provided that when the Exchange is satisfied that circumstances warrant an extension of time is necessary to furnish such report, it may grant an extension of such time as it may deem fit.

BYE LAWS OF NSEIL

Regulations

(1) The Board or relevant authority may prescribe Regulations from time to time for the functioning and operations of the Exchange and to regulate the functioning and operations of the trading members of the Exchange.

(2) Without prejudice to the generality of (1) above, the Board or relevant authority may prescribe regulations from time to time, inter alia, with respect to:

(i) norms, procedures, terms and conditions to be complied with for inclusion of securities in the Official List of NSE securities;

(ii) fees payable by an Issuer for inclusion and continued inclusion in the Official List of NSE Securities;

(iii) norms and procedures for approval of market- makers to act as such;

(iv) forms and conditions of contracts to be entered into, and the time, mode and manner for performance of contracts between trading members inter se or between trading members and their constituents;

(v) determination from time to time, of fees, system usage charges, deposits, margins and other monies payable to the Exchange by trading members, participants and by Issuers whose securities are admitted/to be admitted to dealings on the Exchange and the scale of brokerage chargeable by trading members;

(vi) prescription, from time to time, of capital adequacy and other norms which shall be required to be maintained by trading members;

(vii) supervision of the market and promulgation of such Business Rules and Codes of Conduct as it may deem fit;

(viii) maintenance of records and books of accounts by trading members as it may deem fit and records as required under the Securities Contracts (Regulation) Act and Rules and SEBI Act;

(ix) inspection and audit of records and books of accounts;

(x) prescription, from time to time, and administration of penalties, fines and other consequences, including suspension/expulsion for defaults or violation of any requirements of the Bye Laws and Regulations and the Rules and Codes of Conduct and criteria for readmission, if any, promulgated thereunder;

(xi) disciplinary action/procedures against any trading member;

(xii) settlement of disputes, complaints, claims arising between trading members inter-se as well as between trading members and persons who are not trading members relating to any transaction in securities made on the Exchange including settlement by arbitration;

(xiii) norms and procedures for arbitration;

(xiv) administration, maintenance and investment of the corpus of the Fund(s) set up by the Exchange including Investor Protection Fund;

(xv) norms and procedures for settlement and clearing of deals, including establishment and functioning of clearing house or other arrangements for clearing and settlement;

(xvi) norms, procedures, terms and conditions for registration and continuance of registration of Participants;

(xvii) norms and procedures in respect of, incidental or consequential to closing out of contracts, deals or transactions;

(xviii) dissemination of information, announcements to be placed on the trading system;

(xix) any other matter as may be decided by the Board.

Dealings in Securities

(1) Dealings Allowed: Dealings in securities shall be permitted on the Exchange as provided in these Bye Laws and Regulations and save as so provided, no other dealings are permitted.

(2) Admission of Securities to Dealings:

(i) Dealings are permitted on the Exchange in accordance with the provisions prescribed in these Bye Laws and Regulations in that behalf, in securities which are, from time to time, listed or permitted to trade on the trading segments by the relevant authority.

(ii) Admission of securities to listing on the Exchange shall be in accordance with provisions prescribed in these Bye Laws and Regulations in that behalf.

(iii) The relevant authority may admit from time to time securities which are permitted to trade on the Exchange.

(3) **Government Securities:**

(i) Notwithstanding anything contained in Byelaw (2) above, dealings shall be deemed to have been permitted in Government securities, which term for the purpose of these Rules, Bye Laws and the Regulations made thereunder shall denote securities issued by the Government of India, State Governments, Port Trusts, Municipalities, local authorities, statutory bodies and similar other bodies or authorities and include treasury bills issued by the Government of India.

(ii) Government securities shall be deemed to have been admitted to dealing on such market segment of the Exchange as may be prescribed by the relevant authority as from the date of their inclusion on the Official List(s) of NSE Securities.

(4) **Dealings in Securities Dealt on other Stock Exchanges:** Without prejudice to the generality of Byelaw (2) above, the relevant authority may in its discretion and subject to such conditions as it may deem proper, permit dealings in any securities admitted to dealings on any other Stock Exchange or which are regularly dealt in on such Stock Exchange.

(5) **Application for Admission to Listing:** Applications for admission of securities to listing on the Exchange shall be made to the relevant authority in such form as the relevant authority may from time to time prescribe.

(6) **Conditions and Requirements of Dealings:** The relevant authority may not grant admission to dealings to the securities of an Issuer unless it complies with the conditions and requirements prescribed in these Bye Laws and Regulations and such other conditions and requirements as the relevant authority may from time to time prescribe.

(7) **Refusal of Admission to Listing:** The relevant authority may, in its discretion, approve subject to such terms as it deems proper, or defer, or reject any application for admission of a security to listing on the Exchange.

(8) **Fees:** Issuers whose securities are granted admission to dealings on the Exchange shall pay such listing and such other fees and such other deposits as the relevant authority may from time to time determine.

(9) **Dealings in Provisional Documents:** The relevant authority may, in its discretion, permit dealings in Provisional Documents. Provisional Documents for purposes of these Bye Laws and Regulations denote Coupons, Fractional Certificates, Letters of Renunciation or transferable Letters of Allotment, Acceptance or Application or options or other rights or interests in securities, warrants issued or to be issued by an issuer or

other similar documents in respect of an issuer whose securities are sought to be admitted/admitted to dealings on the Exchange.

(10) **Issuers Registered Outside India** Admission to dealings on the Exchange shall not be granted to securities issued by a body corporate, fund or other entity registered or formed outside India unless:

(i) there is adequate public interest in such securities in India;

(ii) the body corporate, fund or other entity agrees to maintain a register of members or other similar record in India and agrees to abide by such other criteria as prescribed by the relevant authority are satisfied.

(11) **Specific Deals:** The relevant authority may permit specific deals to be made in the case of securities of Issuers not admitted to dealings on the Exchange, which for the time being are prohibited or suspended for dealings.

(12) **Prohibited Dealings:** The relevant authority may prohibit dealings on the Exchange in any security or securities for any cause.

(13) **Suspension of Admission to Dealings on the Exchange:** The relevant authority may suspend at any time the admission to dealings on the Exchange granted to any security for such period as it may determine. At the expiration of the period of suspension the relevant authority may reinstate such security subject to such conditions as it deems fit.

(14) **Withdrawal of Admission to Dealings on Redemption or Conversion:** The relevant authority may, if necessary, withdraw admission to dealings granted to securities which are about to be exchanged or converted into other securities as a result of any scheme of reorganisation or reconstruction or which being redeemable or convertible securities are about to fall due for redemption or conversion.

(15) **Withdrawal of Admission to Dealings on Liquidation or Merger:** If any issuer be placed in final or provisional liquidation or is about to be merged into or amalgamated with another entity, the relevant authority may withdraw the admission to dealings on the Exchange granted to its securities. The relevant authority may accept such evidence as it deems sufficient on such liquidation, merger or amalgamation. Should the merger or amalgamation fail to take place or should an issuer placed in provisional liquidation be reinstated and an application be made for readmission of its securities to dealings on the Exchange. The relevant authority shall have the right of approving, refusing or deferring such application.

(16) **Withdrawal of Admission to Dealings on the Exchange:** The relevant authority may, where deemed necessary, after giving an opportunity to the issuer to explain, withdraw the admission to dealings on the Exchange granted to its securities either for breach of or non-compliance with any of the conditions or requirements of admission to dealings, or for any other reason whatsoever.

(17) **Readmission to Dealings on the Exchange:** The relevant authority in its discretion may readmit to dealings on the Exchange the securities of an issuer whose admission to dealings has been previously withdrawn.

Transactions and Settlements

Delivery of securities

(1) Delivery of all securities, documents and papers and payments in respect of all deals shall be in such manner and such place(s) as may be prescribed by the relevant authority from time to time.

(2) The relevant authority shall specify from time to time, the securities, documents and papers which, when delivered in prescribed manner, shall constitute good delivery. Where circumstances so warrant, the relevant authority may determine, for reasons to be recorded, whether or not a delivery constitutes a good delivery and such finding shall be binding on the parties concerned. Where the relevant authority determines that a delivery does not constitute a good delivery, the delivering party shall be required to substitute good delivery instead within such time period as may be specified.

(3) The norms and procedures for delivery with respect to market lot, odd lot, minimum lot, part delivery, delivery of partly paid securities, etc. shall be as prescribed by the relevant authority from time to time.

(4) The requirements and procedures for determining disputed deliveries or defective deliveries, and measures, procedures and system of resolving the dispute or defect in deliveries or of consequences of such deliveries or the resolution shall, subject to these Bye Laws, be as prescribed by the relevant authority from time to time.

Rights and Liabilities of Members and Constituents

Registration of Securities when in Name of trading member or Nominee

(i) When the time available to the constituents of a trading member is less than thirty days to complete transfers and lodge the securities for registration before the closing of the transfer books and where the security is purchased cum interest, dividend, bonus or rights which the issuer may have announced or declared the trading member may register the securities in its or its nominee's name and recover the transfer fee, stamp duty and other charges from the buying constituent.

(ii) The trading member shall give immediate intimation to the Exchange of the names of such constituents and details of the transactions as may be specified by the relevant authority from time to time. The trading member shall also give immediate intimation thereof to the buying constituent and shall stand indemnified for the consequences of any delay in delivery caused by such action.

(iii) The trading member shall be obliged to retransfer the security in the name of the original constituent as soon as it has become ex interest, dividend, bonus or rights.

Miscellaneous

(1) The relevant authority shall be empowered to impose such restrictions on transactions in one or more Exchange securities as the relevant authority in its judgment deems advisable in the interest of maintaining a fair and orderly market in the securities or if it otherwise deems advisable in the public interest or for the protection of investors. During the effectiveness of such restrictions, no trading member shall, for any account in which it has an interest or for the account of any client, engage in any transaction in contravention of such restrictions.

(2) Any failure to observe or comply with any requirement of this Bye Law, or any Bye Laws, Rules or Regulations, where applicable, may be dealt with by the relevant authority as a violation of such Bye Laws, Rules or Regulations.

(3) Trading members have an obligation as the trading members of the Exchange to inform the relevant authority of the Exchange and the Securities Exchange Board of India about insider trading, information on takeover and other such information/practices as may be construed as being detrimental to the efficient operations of the Exchange and as may be required under SEBI Act and Rules and Regulations.

(4) Save as otherwise specifically provided in the regulations prescribed by the relevant authority regarding clearing and settlement arrangement, in promoting, facilitating, assisting, regulating, managing and operating the Exchange, the Exchange should not be deemed to have incurred any liability, and accordingly no claim or recourse, in respect of, in relation to, any dealing in securities or any matter connected therewith shall lie against the Exchange or any authorized person(s) acting for the Exchange.

(5) No claim, suit, prosecution or other legal proceedings shall lie against the Exchange or any authorised person(s) acting for the Exchange, in respect of anything which is in good faith done or intended to be done in pursuance of any order or other binding directive issued to the Exchange under any law or delegated legislation for the time being in force.

1.7 RULES, REGULATIONS AND BYELAWS OF NSCCL (NATIONAL SECURITIES CLEARING CORPORATION LIMITED)

Rules of NSCCL

The rules are divides in four categories,

(i) Board

(ii) Executive Committee

(iii) Clearing Membership

(iv) Disciplinary Proceeding, Penalties, Suspension and Expulsion

We will take a look at rules pertaining to Information Security under each category.

(1) Board

Rule1: The Board is empowered to organise, maintain, control, manage, regulate and facilitate the operations of the F & O segment of the Clearing Corporation and all activities of the Clearing Members

Rule 2: The Board is empowered to make Rules, Bye Laws and Regulations from time to time, for all or any matters relating to the conduct of business of the F & O segment of the Clearing Corporation, the business and transactions of Clearing Members, between Clearing Members inter-se as well as the business and transactions between Clearing Members and persons who are not Clearing Members, and to control, define and regulate all such transactions and dealings and to do such acts and things which are necessary for the purposes of the F & O segment of the Clearing Corporation.

Rule 3: Without prejudice to the generality of the foregoing, the Board is empowered to make Regulations for all or any of the following matters:

(i) conduct of business of the F & O segment of the Clearing Corporation;

(ii) appointment and dissolution of Committee or Committees for any purpose of the Clearing Corporation;

(iii) manner of operations and interfacing with exchanges, custodians, depository and clearing bank(s);

(iv) norms, procedures, terms and conditions for admission to membership of the F & O segment of the Clearing Corporation;

(v) conditions, levy for admission or subscription for admission or continuance of Clearing Membership of the F & O segment of the Clearing Corporation;

(vi) conduct of Clearing Members with regard to the business of the Clearing Corporation;

(vii) prescription, from time to time, of capital adequacy and other norms which shall be required to be maintained by different categories of Clearing Members;

(viii) charges payable by Clearing Members for business transacted through the F & O segment of the Clearing Corporation as may be laid down from time to time;

(ix) maintenance of records and books of accounts by Clearing Members as may be specified from time to time;

(x) investigation of the financial condition, business conduct and dealings of the Clearing Members;

(xi) prescription from time to time, and administration of penalties, fines and other consequences, including suspension/expulsion of Clearing Members from the F & O segment of the Clearing Corporation for violation of any requirements of the Rules, Bye Laws and Regulations and the codes of conduct;

(xii) disciplinary action/procedures against any Clearing Member;

(xiii) penalties for non compliance with or contravention of the Bye Laws, Rules and Regulations or of general discipline of the F & O segment of the Clearing Corporation, including expulsion or suspension of the Clearing Members;

(xiv) declaration of any Clearing Member as a defaulter or suspension or resignation or expulsion from Clearing Membership and consequences thereof;

(xv) such other matters in relation to the Clearing Corporation as may be specified under the provisions of the Articles of Association, Bye Laws or these Rules or as may be necessary or expedient for the organisation, maintenance, control, management, regulation and facilitation of the operations of the Clearing Corporation.

Rule 7: The Board is empowered to vary, amend, repeal or add to Bye Laws and Rules framed by it with prior approval of SEBI, if any.

Rule 8: The Board is authorised to vary, amend, repeal or add to Regulations framed by it. Such changes shall be intimated to SEBI within 24 hours.

Rule 9: The Members of the Board and of such committees as may be identified by the Board shall adhere to the Code of Ethics as specified by SEBI.

(2) Executive Committee

Rule 1: Constitution

One or more Executive Committee(s) may be appointed by the Board for the purposes of managing the day to day affairs of the different clearing sub-segment(s) of the F & O segment of the Clearing Corporation. The Board may decide on the constitution, duration and powers of the Executive Committee(s), nomination and vacation of the nominees from the Executive Committee(s) and appointment of office bearers and rules and procedures for the functioning of the Executive Committee(s).

Rule 2: Powers of Executive Committee

(i) The Board may delegate from time to time to the Executive Committee(s) such of the powers vested in it and upon such terms as it may think fit, to manage all or any of the affairs of the F & O segment of the Clearing Corporation and from time to time, to revoke, withdraw, alter or vary all or any of such powers.

(ii) The Executive Committee(s) shall be bound and obliged to carry out and implement any directives issued by the Board from time to time and shall be bound to comply with all conditions of delegation and limitations on the powers of the Executive Committee(s) as may be specified.

(3) Clearing Membership

Rule 1: Multiple Category

The rights, privileges duties and responsibilities of a Clearing Member shall be subject to and in accordance with the Rules, Bye Laws and Regulations. The relevant authority may define and admit more than one category of Clearing Members for the same clearing sub-segment or for different clearing sub-segments and may specify different norms including eligibility, admission and cessation of membership for different sub-segments.

(4) Disciplinary Proceedings, Penalties, Suspension and Expulsion

Rule 1: Disciplinary Jurisdiction

The relevant authority may expel or suspend and/or fine and/or penalise under censure and/or warn and/or withdraw all or any of the membership rights of a Clearing Member if he is guilty of contravention, non-compliance, disobedience, disregard or evasion of any of the Bye Laws, Rules and Regulations or of any resolutions, orders, notices, directions or decisions or rulings of the F & O segment of the Clearing Corporation or the relevant authority or of any other Committee or officer of the Clearing Corporation authorised in that behalf or of any conduct, proceeding or method of business which the relevant authority in its absolute discretion deems dishonourable, disgraceful or unbecoming a Clearing Member or inconsistent with just and equitable principles or detrimental to the interests, good name or welfare of the Clearing Corporation or prejudicial or subversive to its objects and purposes.

Rule 2: Penalty for Breach of Rules, Bye-Laws and Regulations

Every Clearing Member shall be liable to suspension, expulsion or withdrawal of all or any of his Clearing Membership rights and/or to payment of fine and/or to be censured, reprimanded or warned for contravening, disobeying, disregarding or willfully evading of any of these Rules, Bye- laws and Regulations or any resolutions, orders, notices, directions, decisions or rulings thereunder of the F & O segment of the Clearing Corporation, Securities Contracts (Regulation) Act, 1956 and/or Rules thereunder, Securities and Exchange Board of India Act, 1992 and/or Rules thereunder, the Board of Directors, Executive Committee, Managing Director or any officer of the Clearing Corporation or for any disreputable or fraudulent transactions or dealings or method of business which the Board of Directors in its absolute discretion deems unbecoming a Clearing Member of the Clearing Corporation or inconsistent with just and equitable principles.

Rule 19: Notice of Penalty and Suspension of Business

(i) Notice shall be given to the Clearing Member concerned and to the Clearing Members in general by such mode as may be decided by the relevant authority from time to time of the expulsion or suspension or default of or of the suspension of business by a Clearing Member or of any other penalty imposed on it or on its partners or other employees. The relevant authority may in its absolute discretion and in such manner as it thinks fit notify or cause to be notified to the Clearing Members or to the public that any person who is named in such notification has been expelled, suspended, penalised or declared a defaulter or has suspended his business or ceased to be a Clearing Member. No action or other proceedings shall in any circumstances be maintainable by such person against the Clearing Corporation or the relevant authority or any officer or employee of the Clearing Corporation for the publication or circulation of such notification. The application for Clearing Membership or the application for registration as the constituted attorney or authorised representative or by the person concerned shall operate as license and these Bye Laws and Rules shall operate as leave to print, publish or circulate such advertisement or notification and be pleadable accordingly.

(ii) Notwithstanding anything contained in these provisions, if in the opinion of the relevant authority it is necessary to do so, he may, for reasons to be recorded in writing, temporarily suspend forthwith the Clearing Member, pending completion of appropriate proceedings for suspension under this chapter by the relevant authority, and no notice of hearing shall be required for such temporary suspension and such temporary suspension shall have the same consequences of suspension under this chapter, provided that appropriate proceedings provided in this chapter shall be commenced by issue of a notice to show cause to the Clearing

Member within 10 days of such temporary suspension. Any such temporary suspension may be revoked at the discretion of the relevant authority, for reasons to be recorded in writing, if the relevant authority is satisfied that the circumstances leading to the formation of opinion of the relevant authority to suspend, has ceased to exist or are satisfactorily resolved.

Regulations of NSCCL

Futures & Options

The Regulations framed hereunder shall be known as National Securities Clearing Corporation (Futures & Options Segment) Regulations, 2000. These Regulations shall be applicable to all clearing members dealing in Futures & Options Segment (F&O Segment) of the Clearing Corporation.

A) F&O SEGMENT

(1) Specified Exchange

The relevant authority may from time to time admit transactions executed in specified exchanges after obtaining prior approval of SEBI. For the purpose of these regulations, the following exchange is specified: Futures and Options segment of National Stock Exchange, which exchange is hereinafter referred to as NSE for the purposes of these Regulations.

(2) F&O Clearing Members

'F&O Clearing Member' means a member of the Clearing Corporation and includes all categories of clearing members as may be admitted as such by the Clearing Corporation to the F&O Segment.

(3) Collection of Securities Transaction Tax

The Clearing Corporation shall, on behalf of the Exchange, collect the Securities Transaction Tax. Every Clearing Member shall remit to the Clearing Corporation the Securities Transaction Tax payable by the Trading Member of the Exchange in respect of the transactions entered into by him on the Exchange either on his own behalf or on behalf of his Constituents and cleared and settled through such Clearing Member in accordance with the procedures prescribed by the Relevant Authority form time to time for the calculation and collection of such tax. Any Clearing Member who fails to make the payment in accordance with the procedures, prescribed by the Relevant Authority from time to time, would be liable for such consequences of non-payment including but not limited to withdrawal of clearing facility, appropriation form the monies of the Clearing Member, withholding of pay-outs, etc. as may be prescribed from time to time.

Provisions Regarding Clearing & Settlement of Derivatives Contract

Adjustment of positions in derivatives contracts on account of corporate actions in underlying security

(1) The Relevant Authority may from time to time specify the provisions, relating to adjustments, including non-adjustment, in open positions, discontinuing any or all futures contracts and/or settlement methods and procedures for the relevant derivatives contracts, arising out of or incidental to corporate actions in the underlying security.

(2) **Adjustment**: Adjustment shall mean and include modification in open positions and/or contract specifications in the relevant derivatives contracts, arising out of or incidental to corporate actions in the underlying security, in accordance with the Rules, Bye-laws and Regulations in force from time to time.

Annual Accounts and Audit

(1) Each F&O Clearing Member shall prepare annual accounts for each financial year ending on 31st March or such other date as advised to the Clearing Corporation.

(2) The Assets and Liabilities of the F&O Clearing Member's business shall be brought into account in the balance sheet at such amounts and shall be classified and described therein in such manner that the balance sheet gives a true and fair view of the state of affairs of such business as at the date to which it is made up.

(3) Each F&O Clearing Member shall furnish to the Clearing Corporation, its audited financial statement and such report shall be furnished not later than six months after the end of the clearing member's financial year, provided that when the Clearing Corporation is satisfied that circumstances warrant an extension of time is necessary to furnish such report, it may grant an extension of such time as it may deem fit.

(B) Capital Market Segment

CM Clearing Segment

Collection of Securities Transaction Tax

The Clearing Corporation shall, on behalf of the Exchange, collect the Securities Transaction Tax. Every Clearing Member shall remit to the Clearing Corporation the Securities Transaction Tax payable by the Trading Member of the Exchange in respect of the transactions entered into by him on the Exchange either on his own behalf or on behalf of his Constituents and cleared and settled through such Clearing Member in accordance with the procedures prescribed by the Relevant Authority from time to time for the calculation and collection of such Tax. Any Clearing Member who fails to make the payment in accordance with the procedures, prescribed by the Relevant Authority from time to time, would be liable for such consequences of non-payment including but not limited to withdrawal of clearing facility, appropriation from the monies of the Clearing Member, withholding of pay-outs, etc. as may be prescribed from time to time.

Deals

Deals in Provisional Documents and Provisional Securities

Deals in Provisional Documents and Provisional Securities shall be made and settled as determined in each case by the relevant authority.

Procedure for Settlement of Cleared Deals

Delivery of Securities

(1) Non Depository Deals

On the respective pay-in day, CM clearing members shall deliver securities to the Clearing House as per Delivery Statement in respect of non depository deals. Each delivery shall be accompanied by the corresponding Delivery Slip. Delivery shall be in such delivery units as the relevant authority may notify from time to time together with the necessary transfer forms, duly filled in and showing on the reverse the code and name of the clearing member delivering the securities and such other details as may be required by the Clearing Corporation.

(2) Depository Deals

On the respective pay-in day, CM clearing members shall affect depository delivery in the Depository Clearing System as per Delivery Statement in respect of depository deals. Delivery shall be in such delivery units the relevant authority may notify from time to time.

Receipt of Securities

(1) Non Depository Deals

Securities which are to be received by a CM clearing member shall be delivered to him by the Clearing House in respect of non depository deals on the respective pay-out day as per instructions of the Clearing Corporation. All securities due to a CM Clearing member shall be normally delivered to him unless (a) the CM clearing member has not delivered securities on pay in day as per Final Settlement Obligations or (b) the full extent of funds obligation of the CM Clearing member was not available with the NSCC Clearing account for funds pay-in or (c) it is otherwise ordered by the relevant authority. CM clearing members who are taking delivery of securities from the Clearing House shall sign a receipt thereof in the form attached to the Clearing House Receipt Statement.

(2) Depository Deals

Securities which are to be received by a CM clearing member shall be delivered to him in the Depository Clearing System in respect of depository deals on the respective pay-out day as per instructions of the Clearing Corporation.

Notice of Delivery and Payment outside Clearing House In Respect Of Cleared Securities for Non Depository Deals

Whenever the relevant authority orders delivery and payment to be made outside the Clearing House in respect of cleared non depository deals, a notice to that effect shall normally be sent to the CM clearing members at least a day before the pay-in day.

Notice of Delivery and Payment outside Depository Clearing System in respect of Cleared Securities for Depository Deals

Whenever the relevant authority orders delivery and payment to be made outside the Depository Clearing System in respect of Cleared depository deals directly between CM Clearing Members in the Depository System, a notice to that effect shall normally be sent to the CM clearing members at least a day before the paying day.

Non-Delivery and Non-Payment

Securities on Hold or Selling-Out On Failure to Pay

If a CM clearing member fails to pay on pay-in day for the securities to be received by him, the Clearing Corporation shall be, without further notice or intimation to the member, entitled to withhold the securities due to the member or sell-out any/all of such securities in accordance with the Bye Laws and Regulations relating to closing-out.

Withholding of Securities and Funds

Notwithstanding anything contained in these Regulations, irrespective of whether the deals are depository deals or non-depository deals, the relevant authority may withhold, for such period(s) as the relevant authority may decide from time to time, pay-out of any securities and any funds including securities and funds constituting margins, if (a) the CM clearing member has not delivered the required securities on pay-in day or (b) there are no adequate funds in the NSCC Clearing Account of the clearing member to meet the funds pay-in obligation on the pay-in day or (c) the CM clearing member fails to satisfy the margin Requirements or (d) the CM clearing member fails to fulfill any other obligation or (e) the relevant authority, otherwise, deems fit.

With-holding of securities for shortages

The relevant authority may with-hold the securities pay-out due to the Clearing Member and/or withdraw his clearing facility in case of any pay-in shortages by the Clearing Member for such amount as the relevant authority may deem fit. The relevant authority may, on recovery of such shortages as it may deem fit, release the pay-out and/or restore the clearing facility and permit the clearing member to clear and settle subject to such terms and conditions as the relevant authority may impose.

Withheld Securities and Funds - How Dealt With

The securities and funds withheld pursuant to Regulation above shall be dealt with the relevant authority at such times and in such manner as it may deem fit, which may include appropriating the withheld funds for the purpose of fulfilling the obligations of the clearing member, closing out of the withheld securities or registering the withheld securities in the name of the Clearing Corporation or any other entity as decided by the Clearing Corporation. The funds received out of closing out of withheld or registered securities may be dealt with by the Clearing Corporation at such time and in such manner as it may deem fit.

Annual Accounts and Audit

(1) Each CM clearing member shall prepare annual accounts for each financial year ending on 31st March or such other date as advised to the Clearing Corporation.

(2) The Assets and Liabilities of the CM clearing member's business shall be brought into account in the balance sheet at such amounts and shall be classified and described therein in such manner that the balance sheet gives a true and fair view of the state of affairs of such business as at the date to which it is made up.

(3) Each CM clearing member shall furnish to the Clearing Corporation, its audited financial statement and such report shall be furnished not later than six months after the end of the clearing member's financial year; provided that when the Clearing Corporation is satisfied that circumstances warrant an extension of time is necessary to furnish such report, it may grant an extension of such time as it may deem fit.

Byelaws of NSCCL

Futures & Options Segment

Clearing Sub-Segments of F&O Segment

The Clearing Corporation may establish more than one clearing sub-segment or division in the F & O Segment as may be specified by the relevant authority from time to time. Deals which may be admitted to the different clearing sub-segments or divisions of F & O Segment for the purpose of clearing and settlement will be specified by the relevant authority from time to time.

Executive Committee

(1) Executive Committee(s) may be appointed by the Board for the purposes of managing the day to day affairs of the F & O Segment of the Clearing Corporation in such manner as laid down in the Rules.

(2) The Executive Committee of F & O Segment shall have such responsibilities and powers as may be delegated to it by the Board.

(3) The Executive Committee for F & O Segment shall not have any representation from the Clearing Members and Trading Members. The composition of such Executive Committee shall be subject to the prior approval of Securities and Exchange Board of India (SEBI).

Regulations

(1) The Board may prescribe Regulations from time to time for the functioning and operations of the F & O Segment and to regulate the functioning and operations of the clearing members of the F & O Segment.

(2) Without prejudice to the generality of the above, the Board may prescribe regulations from time to time, inter alia, with respect to:

(i) norms, procedures, terms and conditions for admission of Exchanges;

(ii) norms, procedures, terms and conditions to be complied with for admission of deals for clearing and settlement in the F & O Segment by the Clearing Corporation;

(iii) norms, procedures, terms and conditions for clearing and settlement of deals in the F & O Segment;

(iv) forms and conditions of deals to be entered into, and the time, mode and manner for performance of deals between clearing members inter se or between clearing members and their constituents;

(v) norms, procedures, terms and conditions for guaranteed settlement by the F&O Segment;

(vi) prescription, from time to time, and administration of penalties, fines and other consequences, including suspension/expulsion of clearing members from the F & O Segment for defaults;

(vii) norms, procedures, terms and conditions for imposition and administration of different types of margins and other charges and restrictions that may be imposed by the F & O Segment from time to time.

(viii) determination from time to time, of fees, system usage charges, deposits, margins and other monies payable to the Clearing Corporation by clearing members of the F & O Segment and the scale of clearing and other charges that may be collected by such clearing members;

(ix) supervision of the clearing operations and promulgation of such Business Rules and Codes of Conduct as it may deem fit;

(x) inspection and audit of records and books of accounts;

(xi) settlement of disputes, complaints, claims arising between clearing members inter-se as well as between clearing members and persons who are not clearing members relating to any deal in securities cleared and settled through the F & O Segment including settlement by arbitration;

(xii) norms, procedures, terms and conditions for arbitration;

(xiii) administration, maintenance and investment of the corpus of the Fund(s) set up by the F & O Segment including Settlement Fund(s);

(xiv) establishment, norms, terms and conditions, functioning and procedures of clearing house, clearing through depository or other arrangements including custodial services for clearing and settlement;

(xv) norms, procedures, terms and conditions in respect of, incidental to or consequential to closing out of deals;

(xvi) dissemination of information and announcements;

(xii) any other matter as may be decided by the Board.

Clearing and Settlement of Deals

Delivery of Securities

(1) Delivery and settlement of all securities, documents and papers and payment in respect of all deals in the F & O Segment shall be in such manner and such place(s) as may be specified by the relevant authority from time to time.

(2) The relevant authority shall specify from time to time, the securities, documents and papers which, when delivered in specified manner, shall constitute good delivery. Where circumstances so warrant, the relevant authority may determine, for reasons to be recorded, whether or not a delivery constitutes a good delivery, and such findings shall be binding on parties concerned. Where the relevant authority determines that a delivery does not constitute a good delivery, the delivering party shall be required to substitute good delivery instead within such time as may be specified.

(3) The norms and procedures for delivery with respect to market lot, odd lot, minimum lot, part delivery, delivery of partly paid securities etc., shall be as specified by the relevant authority from time to time.

(4) The requirements and procedures for determining disputed deliveries or defective deliveries, and measures, procedures and system of resolving the dispute or defect in deliveries or of consequences of such deliveries or their resolution shall, subject to these Bye Laws, be as specified by the relevant authority from time to time.

Rights and Liabilities of Clearing Members and Constituents

Registration of Securities When in the name of Clearing Member or Nominee

(1) When the time available to the constituents of a clearing member is not sufficient for them to complete transfers and lodge the securities for registration before the closing of the transfer books and where the security is purchased cum interest, dividend, bonus or rights which the company may have announced or declared, the clearing member may register the securities in its or its nominee's name and recover the transfer fee, stamp duty and other charges from the buying constituent.

(2) The clearing member shall give immediate intimation to the F & O Segment the names of such constituents and details of the deals as may be specified by the relevant authority from time to time. The clearing member shall also give immediate intimation thereof to the buying constituent and shall stand indemnified for the consequences of any delay in delivery caused by such action.

(3) The clearing member shall be obliged to re-transfer the security in the name of the original constituent as soon as it has become ex interest, dividend, bonus or rights.

Miscellaneous

(1) Save as otherwise specifically provided in the Bye Laws and Regulations specified by the relevant authority regarding clearing and settlement arrangement, in promoting, facilitating, assisting, regulating, managing and operating the F & O Segment, the F & O Segment of the Clearing Corporation should not be deemed to have incurred any liability, and accordingly no claim or recourse in respect of or in relation to any dealing in securities or any matter connected therewith shall lie against the F & O Segment or any authorised person(s) acting for the F & O Segment of the Clearing Corporation.

(2) No claim, suit, prosecution or other legal proceeding shall lie against the F & O Segment or any authorised person(s) acting for the F & O Segment in respect of anything which is in good faith done or intended to be done in pursuance of any order or other binding directive issued to the F & O Segment under any law or delegated legislation for the time being in force.

Clearing Members

Clearing Segments

The Clearing Corporation may establish more than one clearing segment as may be specified by the relevant authority from time to time. Deals which may be admitted to the different clearing segments for the purpose of clearing and settlement will be specified by the relevant authority from time to time.

Executive Committee

(1) Executive Committee(s) may be appointed by the Board for the purposes of managing the day to day affairs of the different segment(s) of the Clearing Corporation in such manner as laid down in the Rules.

(2) The Executive Committee of each clearing segment shall have such responsibilities and powers as may be delegated to it by the Board.

Regulations

(1) The Board may prescribe Regulations from time to time for the functioning and operations of the Clearing Corporation and to regulate the functioning and operations of the clearing members of the Clearing Corporation.

(2) Without prejudice to the generality of the above, the Board may prescribe regulations from time to time, inter alia, with respect to:

(i) norms, procedures, terms and conditions for admission of Exchanges;

(ii) norms, procedures, terms and conditions to be complied with for admission of deals for clearing and settlement by the Clearing Corporation;

(iii) norms, procedures, terms and conditions for clearing and settlement of deals for different clearing segments and different securities and instruments;

(iv) forms and conditions of deals to be entered into, and the time, mode and manner for performance of deals between clearing members inter se or between clearing members and their constituents;

(v) norms, procedures, terms and conditions for guaranteed settlement by the Clearing Corporation;

(vi) prescription, from time to time, and administration of penalties, fines and other consequences, including suspension/expulsion of clearing members from the Clearing Corporation for defaults;

(vii) norms, procedures, terms and conditions for imposition and administration of different types of margins and other charges and restrictions that may be imposed by the Clearing Corporation from time to time.

(viii) determination from time to time, of fees, system usage charges, deposits, margins and other monies payable to the Clearing Corporation by clearing members and the scale of clearing and other charges that may be collected by clearing members;

(ix) supervision of the clearing operations and promulgation of such Business Rules and Codes of Conduct as it may deem fit;

(x) inspection and audit of records and books of accounts;

(xi) settlement of disputes, complaints, claims arising between clearing members inter-se as well as between clearing members and persons who are not clearing members relating to any deal in securities cleared and settled through the Clearing Corporation including settlement by arbitration;

(xii) norms, procedures, terms and conditions for arbitration;

(xiii) administration, maintenance and investment of the corpus of the Fund(s) set up by the Clearing Corporation including Settlement Fund(s);

(xiv) establishment, norms, terms and conditions, functioning and procedures of clearing house, clearing through depository or other arrangements including custodial services for clearing and settlement;

(xv) norms, procedures, terms and conditions in respect of, incidental to or consequential to closing out of deals;

(xvi) dissemination of information and announcements;

(xvii) any other matter as may be decided by the Board.

Clearing and Settlement of Deals

Delivery of Securities

(1) Delivery and settlement of all securities, documents and papers and payment in respect of all deals shall be in such manner and such place(s) as may be prescribed by the relevant authority from time to time.

(2) The relevant authority shall specify from time to time, the securities, documents and papers which, when delivered in prescribed manner, shall constitute good delivery. Where circumstances so warrant, the relevant authority may determine, for reasons to be recorded, whether or not a delivery constitutes a good delivery, and such findings shall be binding on parties concerned. Where the relevant authority determines that a delivery does not constitute a good delivery, the delivering party shall be required to substitute good delivery instead within such time as may be specified.

(3) The norms and procedures for delivery with respect to market lot, odd lot, minimum lot, part delivery, delivery of partly paid securities etc., shall be as prescribed by the relevant authority from time to time.

(4) The requirements and procedures for determining disputed deliveries or defective deliveries, and measures, procedures and system of resolving the dispute or defect in deliveries or of consequences of such deliveries or their resolution shall, subject to these Bye Laws, be as prescribed by the relevant authority from time to time.

Borrowing of Securities

Notwithstanding anything contained in Byelaw 16 hereinabove, in the event of failure of the Delivering Member to complete delivery of specified securities on the due date, the Clearing Corporation may borrow the securities specified by it on behalf of such Delivering Member in such manner, within such time frame and subject to such conditions and procedures as the relevant authority may prescribe from time to time, and deliver them to the Receiving Member(s) and / to complete the delivery. Such Delivering Member shall return the specified securities within the time stipulated by the relevant authority together with such fees and charges as may be prescribed by the relevant authority. In the event of failure of the Delivering Member to return the securities borrowed by the Clearing Corporation on its behalf within the stipulated time, the Clearing Corporation shall buy the securities on behalf of the member in the manner and method prescribed by the relevant authority and may recover the amount thereof from such member together with such other fees and charges as may be prescribed by the relevant authority. In the event the Clearing Corporation fails to buy-in the securities to be returned on behalf of such borrowing Delivering Member, the Clearing Corporation may effect close out in respect of the securities, to the extent that it could not be bought in, in the manner prescribed by the relevant authority and recover the amount of such close out and fees from such member.

Rights and Liabilities of Clearing Members and Constituents

Registration of Securities when in the name Of Clearing Member or Nominee

(1) When the time available to the constituents of a clearing member is not sufficient for them to complete transfers and lodge the securities for registration before the closing of the transfer books and where the security is purchased cum interest, dividend, bonus or rights which the company may have announced or declared, the clearing member may register the securities in its or its nominee's name and recover the transfer fee, stamp duty and other charges from the buying constituent.

(2) The clearing member shall give immediate intimation to the Clearing Corporation of the names of such constituents and details of the deals as may be specified by the relevant authority from time to time. The clearing member shall also give immediate intimation thereof to the buying constituent and shall stand indemnified for the consequences of any delay in delivery caused by such action.

(3) The clearing member shall be obliged to re-transfer the security in the name of the original constituent as soon as it has become ex interest, dividend, bonus or rights.

Miscellaneous

(1) Save as otherwise specifically provided in the Bye Laws and Regulations prescribed by the relevant authority regarding clearing and settlement arrangement, in promoting, facilitating, assisting, regulating, managing and operating the Clearing Corporation, the Clearing Corporation should not be deemed to have incurred any liability, and accordingly no claim or recourse in respect of or in relation to any dealing in securities or any matter connected therewith shall lie against the Clearing Corporation or any authorised person(s) acting for the Clearing Corporation.

(2) No claim, suit, prosecution or other legal proceeding shall lie against the Clearing Corporation or any authorised person(s) acting for the Clearing Corporation in respect of anything which is in good faith done or intended to be done in pursuance of any order or other binding directive issued to the Clearing Corporation under any law or delegated legislation for the time being in force.

SECTION-B

1.8 THE INFORMATION TECHNOLOGY ACT, 2000

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.
Whereas the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. And whereas the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information. And whereas it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

We will take a look at few important sections pertaining to IT Act.

Section 3: Authentication of Electronic Records

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Section 4: Legal Recognition of Electronic Records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is,

(i) rendered or made available in an electronic form; and

(ii) accessible so as to be usable for a subsequent reference.

Section 5: Legal Recognition of Digital Signatures

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (hence, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation*:* For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

Section 6: Use of Electronic Records and Digital Signatures in Government and Its Agencies

(1) Where any law provides for,

(i) the filing of any form. application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(ii) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

(iii) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe,

(i) the manner and format in which such electronic records shall be filed, created or issued;
(ii) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (i).

Section 10: Power to make rules by Central Government in respect of Digital Signature

(1) The Central Government may, for the purposes of this Act, by rules, prescribe—
the type of digital signature;
(2) the manner and format in which the digital signature shall be affixed;
(3) the manner or procedure which facilitates identification of the person affixing the digital signature;
(4) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
(5) any other matter which is necessary to give legal effect to digital signatures.

Section 14: Secure Electronic Record

Where any security procedure has been applied to an electronic record at a specific point of time. Then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Section 15: Secure Digital Signature

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was,
(1) unique to the subscriber affixing it;
(2) capable of identifying such subscriber;
(3) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

Section 16: Security Procedure

The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including,
(1) the nature of the transaction;

(2) the level of sophistication of the parties with reference to their technological capacity;

(3) the volume of similar transactions engaged in by other parties;

(4) the availability of alternatives offered to but rejected by any party;

(5) the cost of alternative procedures; and

(6) the procedures in general use for similar types of transactions or communications.

Section 29: Access to computers and data

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person incharge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

Section 34: Disclosure

(1) Every Certifying Authority shall disclose in the manner specified by regulations—

- (i) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;
- (ii) any certification practice statement relevant thereto;
- (iii) notice of the revocation or suspension of its Certifying Authority certificate, if any; and
- (iv) any other fact that materially and adversely affects either the reliability of
- (v) a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall,

- (i) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(ii) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

Section 35: Certifying Authority to issue Digital Signature Certificate

(1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government

(2) Every such application shall be accompanied by such fee not exceeding twenty five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority: Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under subsection and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application: Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that,

(i) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(ii) the applicant holds a private key, which is capable of creating a digital signature;

(iii) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant:

Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

Section 38: Revocation of Digital Signature Certificate

(1) A Certifying Authority may revoke a Digital Signature Certificate issued by it,

(i) where the subscriber or any other person authorised by him makes a request to that effect; or

(ii) upon the death of the subscriber, or

(iii) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that,

(i) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(ii) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(iii) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(iv) the subscriber has been declared insolvent **or** dead or where a subscriber is a firm or a company, which has been dissolved, wound-up **or** otherwise ceased to exist

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

Section 41: Acceptance of Digital Signature Certificate

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate,

(i) to one or more persons;

(ii) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that,

(i) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(ii) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(iii) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

Section 65: Tampering with Computer Source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation: For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Section 66: Hacking with Computer System

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack:

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

Section 69: Directions of Controller to a Subscriber to extend facilities to decrypt information

(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person incharge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

Section 72: Penalty for Breach of Confidentiality and Privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 80: Power of Police Officer and other Officers to enter, Search, etc.

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act.

Explanation: For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

1.9 INDIAN COPYRIGHT ACT 1957

The Copyright Act, 1957 came into effect from January 1958. This Act has been amended five times since then, i.e., in 1983, 1984, 1992, 1994 and 1999, with the amendment of 1994 being the most substantial. Prior to the Act of 1957, the Law of Copyrights in the country was governed by the Copyright Act of 1914. This Act was essentially the extension of the British Copyright Act, 1911 to India. Even the Copyright Act, 1957 borrowed extensively from the new Copyright Act of the United Kingdom of 1956. The Copyright Act, 1957 continues with the common law traditions. Developments elsewhere have brought about certain degree of convergence in copyright regimes in the developed world.

The Indian Copyright Act today is compliant with most international conventions and treaties in the field of copyrights. India is a member of the Berne Convention of 1886 (as modified at Paris in 1971), the Universal Copyright Convention of 1951 and the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) Agreement of 1995. Though India is not a member of the Rome Convention of 1961, the Copyright Act, 1957 is fully compliant with the Rome Convention provisions.

Two new treaties, collectively termed as Internet Treaties, were negotiated in 1996 under the auspices of the **World Intellectual Property Organization (WIPO)**. These treaties are called the **'WIPO Copyrights Treaty (WCT)'** and the **'WIPO Performances and Phonograms Treaty (WPPT)'.** These treaties were negotiated essentially to provide for protection of the rights of copyright holders, performers and producers of phonograms in the Internet and digital era. India is not a member of these treaties as yet.

The Section 9 of the Copyright Act requires for establishment of an office to be called the Copyright Office for the purpose of the Act. The Copyright Office is to be under the immediate control of a Registrar of Copyrights to be appointed by the Central Government, who would act under the superintendence and directions of the Central Government.

The Copyright Office is currently located at the following address:

B-2/W-3, Curzon Road Barracks
Kasturba Gandhi Marg
New Delhi – 110001

Section 11 of the Copyright Act requires the Central Government to constitute a Copyright Board headed by a Chairman with not less than two and not more than 14 other members. Registrar of Copyrights is to be Secretary of the Copyright Board. Section 12 of the Copyright Act also lays down the powers of the Copyright Board and deems it to be a civil court for the purposes of Sections 345 and 346 of the Code of Criminal Procedure, 1973 and also that all the proceedings of the Board would be deemed to be judicial proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code.

We will take a look at few important sections pertaining to Indian Copyright Act.

Section 3: Meaning of Publication

For the purposes of this Act, "publication" means,

(1) in the case of a literary, dramatic, musical or artistic work, the issue of copies of the work to the public in sufficient quantities;

(2) in the case of a cinematograph film, the sale or hire or offer for sale or hire of the film or copies thereof to the public;

(3) in the case of a record, the issue of records to the public in sufficient quantities; but does not, except as otherwise expressly provided in this Act, includes,

(i) in the case of a literary, dramatic or musical work, the issue of any recording such work;

(ii) in the case of a work of sculpture or an architectural work of art, the issue of photographs and engravings of such work.

Section 4: When work not deemed to be published or performed in public

Except in relation to infringement of copyright, a work shall not be deemed to be published or performed in public, if published, or performed in public, without the licence of the owner of the copyright.

Section 5: When work deemed to be first published in India

For the purposes of this Act, a work published in India shall be deemed to be first published in India, notwithstanding that it has been published simultaneously in some other country, unless such other country provides a shorter term of copyright for such work; and a work shall be deemed to be published simultaneously in India and in another country if the time between the publication in India and the publication in such other country does not exceed thirty days or such other period as the Central Government may, in relation to any specified country, determine.

Section 6: Certain disputes to be decided by Copyright Board

If any question arises,

(1) Whether for the purposes of section 3, copies of any literary, dramatic, musical or artistic work, or records are issued to the public in sufficient quantities; or

(2) Whether for the purposes of section 5, the term of copyright for any work is shorter in any other country than that provided in respect of that work under this Act; it shall be referred to the Copyright Board constituted under section 11 whose decision thereon shall be final.

Section 7: Nationality of Author where the making of unpublished work is extended over considerable period

Where, in the case of an unpublished work, the making of the work is extended over a considerable period, the author of the work shall, for the purposes of this Act, be deemed to be a citizen of, or domiciled in, that country of which he was a citizen or wherein he was domiciled during any substantial part of that period.

Section 8: Domicile of corporations

For the purposes of this Act, a body corporate shall be deemed to be domiciled in India if it is incorporated under any law in force in India.

Section 9: Copyright Office

(1) There shall be established for the purposes of this Act an office to be called the Copyright Office.

(2) The Copyright Office shall be under the immediate control of 639 M. of Law-7 the Registrar of Copyrights who shall act under the superintendance and direction of the Central Government.

(3) There shall be a seal for the Copyright Office.

Section 10: Registrar and Deputy Registrars of Copyrights

(1) The Central Government shall appoint a Registrar of Copyrights and may appoint one or more Deputy Registrars of Copyrights.

(2) A Deputy Registrar of Copyrights shall discharge under the superintendence and direction of the Registrar of Copyrights such functions of the Registrar under this Act as the Registrar may, from time to time, assign to him; and any reference in this Act to the Registrar of Copyrights shall include a reference to a Deputy Registrar of Copyrights when so discharging any such functions.

Section 11: Copyright Board

(1) As soon as may be after the commencement of this Act, the Central Government shall constitute a Board to be called the Copyright Board which shall consist of a Chairman and not less than two nor more than eight other members.

(2) The Chairman and other members of the Copyright Board shall hold office for such period and on such terms and conditions as may be prescribed.

(3) The Chairman of the Copyright Board shall be a person who is, or has been, a Judge of the Supreme Court or a High Court or is qualified for appointment as a Judge of a High Court.

(4) The Registrar of Copyrights shall be the Secretary of the Copyright Board and shall perform such functions as may be prescribed.

Section 12: Powers and Procedure of Copyright Board

(1) The Copyright Board shall, subject to any rules that may be made under this Act, have power to regulate its own procedure, including the fixing of places and times of its sittings:

Provided that the Copyright Board shall ordinarily hear any proceeding instituted before it under this Act within the zone in which at the time of the institution of the proceeding, the person instituting the proceeding actually and voluntarily resides or carries on business or personally works for gain.

Explanation: In this sub-section "zone" means a zone specified in (37 of 1956) section 15 of the States Reorganisation Act, 1956.

(2) The Copyright Board may exercise and discharge its powers and functions through Benches constituted by the Chairman of the Copyright Board from amongst its members, each Bench consisting of not less than three members.

(3) If there is a difference of opinion among the members of the Copyright Board or any Bench thereof in respect of any matter coming before it for decision under this Act, the opinion of the majority shall prevail:

Provided that where there is no such majority-

(i) if the Chairman was one of the members who heard the matter, the opinion of the Chairman shall prevail.

(ii) if the Chairman was not one of the members who heard the matter, the matter shall be referred to him for his opinion and that opinion shall prevail.

(4) The Copyright Board may authorize any of its members to exercise any of the powers conferred on it by section 74 and any order made or act done in exercise of those powers by the member so authorized shall be deemed to be the order or act, as the case may be, of the Board.

(5) No member of the Copyright Board shall take part in any proceedings before the Board in respect of any matter in which he has a personal interest.

(6) No act done or proceeding taken by the Copyright Board under this Act shall be questioned on the ground merely of the existence of any vacancy in, or defect in the constitution of, the Board.

(7) The Copyright Board shall be deemed to be a civil for the purposes of Sections 480 and 482 of the Code of Criminal Procedure, 1898(5 of 1898), and all proceedings before the Board shall deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code (45 of 1860).

Section 14: Meaning of Copyright

(1) For the purposes of this Act, "copyright" means the exclusive right, by virtue of and subject to the provisions of, this Act,

- (i) in the case of a literary, dramatic or musical work, to do and authorize the doing of any of the following acts, namely:-
  - a. to reproduce the work in any material form;
  - b. to publish the work;
  - c. to perform the work in public;
  - d. to produce, reproduce, perform or publish any translation of the work;
  - e. to communicate the work by radio-diffusion or to communicate to the public by a loud-speaker or any other similar instrument the radio-diffusion of the work;
  - f. to make any adaptation of the work;
  - g. to do in relation to a translation or an adaptation of the work any of the acts specified in relation to the work in clauses (a) to (f);
- (ii) in the case of an artistic work, to do or authorise the doing of any of the following acts, namely:
  - a. to reproduce the work in any material form;
  - b. to publish the work;
  - c. to include the work in any cinematograph film;
  - d. to make any adaptation of the work;
  - e. to do in relation to an adaptation of the work any of the acts specified in relation to the work in clauses (a) to (c).
- (iii) in the case of a cinematograph film, to do or authorise the doing of any of the following acts, namely:
  - a. to make a copy of the film;
  - b. to cause the film, in so far as it consists of visual images, to be seen in public and, in so far as it consists of sounds, to be heard in public;
  - c. to make any record embodying the recording in any part of the sound track associated with the film by utilising such sound track;
  - d. to communicate the film by radio-diffusion;
- (iv) in the case of a record, to do or authorise the doing of any of the following acts by utilising the record, namely:
  - a. to make any other record embodying the same recording;
  - b. to cause the recording embodied in the record to be heard in public;
  - c. to communicate the recording embodied in the record by radio-diffusion.

(2) Any reference in sub-section (1) to the doing of any act in relation to a work or a translation or an adaptation thereof shall include a reference to the doing of that act in relation to a substantial part thereof.

Section 21: Right of Author to relinquish Copyright

(1) The author of a work may relinquish all or any of the rights comprised in the copyright in the work by giving notice in the prescribed from to the Registrar of Copyrights and thereupon such rights shall, subject to the provisions of sub-section (3), cease to exist from the date of the notice.

(2) On receipt of a notice under sub-section (1), the Registrar of Copyrights shall cause it to be published in the Official Gazette and in such other manner as he may deem fit.

(3) The relinquishment of all or any of the rights comprised in the copyright in a work shall not affect any rights subsisting in favour of any person on the date of the notice referred to in sub-section (1).

Section 30: Licenses by owners of Copyright

The owner of the copyright in any existing work or the prospective owner of the copyright in any future work may grant any interest in the right by license in writing signed by him or by his duly authorized agent:

Provided that in the case of a license relating to copyright in any future work, the license shall take effect only when the work comes into existence.

Explanation: Where a person to whom a license relating to copyright in any future work is granted under this section dies before the work comes into existence, his legal representatives shall, in the absence of any provision to the contrary in the license, be entitled to the benefit of the license.

Section 33: Performing Rights Society to File Statements of Fees, Charges and Royalties

(1) Every performing rights society shall, within the prescribed time and in the prescribed manner, prepare, publish and file with the Registrar of Copyrights, statements of all fees, charges or royalties which it proposes to collect for the grant of licenses for performance in public of works in respect of which it has authority to grant such licenses.

(2) If any such society fails to prepare, publish or file with the Registrar of Copyrights the statements referred to in sub-section (1) in relation to any work in accordance with the provisions of that sub-section, no action or other proceeding to enforce any remedy, civil or criminal, for infringement of the performing rights in that work shall be commenced except with the consent of the Registrar of Copyrights.

Section 37: Broadcast Reproduction Right

(1) Where any programme is broadcast by radio-diffusion by the Government or any other broadcasting authority, a special right to be known as "broadcast reproduction right" shall subsist in such programme.

(2) The Government or other broadcasting authority, as the case may be, shall be the owner of the broadcast reproduction right and such right shall subsist until twenty-five years from the beginning of the calendar year next following year in which the programme is first broadcast.

(3) During the continuance of a broadcast reproduction right in relation to any programme, any person who,

    (i) without the licence of the owner of the right,

        a. rebroadcasts the programme in question or any substantial part thereof; or

        b. causes the programme in question or any substantial part thereof to be heard in public; or

    (ii) without the licence of the owner of the right to utilize the broadcast for the purpose of making a record recording the programme in question or any substantial part thereof, makes any such record, shall be deemed to infringe that broadcast reproduction right.

Section 44: Register of Copyrights

There shall be kept at the Copyright Office a register in the prescribed form to be called the Register of Copyrights in which may be entered the names or title of works and the names and addresses of authors, publishers and owners of copyright and such other particulars as may be prescribed.

Section 57: Authors Special Rights

(1) Independently of the author's copyright and even after the assignment either wholly or partially of the said copyright, the author of a work shall have the right to claim the authorship of the work as well as the right to restrain, or claim damages in respect of,

    (i) any distortion, mutilation or other modification of the said work; or

    (ii) any other action in relation to the said work which would be prejudicial to his honour or reputation.

(2) The right conferred upon an author of a work by sub-section (1), other than the right to claim authorship of the work, may be exercised by the legal representative of the author.

Section 69: Offences by Companies

(1) Where any offence under this Act has been committed by a company, every person who at the time the offence was committed was in charge

of, and was responsible to the company for, the conduct of the business of the company, as well as the company shall be deemed to be guilty of such offence and shall be liable to be proceeded against and punished accordingly.

Provided that nothing contained in this sub-section shall render any person liable to any punishment, if he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of such offence.

(2) Notwithstanding anything contained in sub-section (1), where an offence under this Act has been committed by a company, and it is proved that the offence was committed with the consent or connivance of, or is attributable to any negligence on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

(i) "company" means any body corporate and includes a firm or other association of persons; and

(ii) "director" in relation to a firm means a partner in the firm.

Section 70: Cognizance of Offences

No court inferior to that of a presidency magistrate or a magistrate of the first class shall try any offence under this Act.

Section 71: Appeals against certain orders Of Magistrate

Any person aggrieved by an order under sub-section (2) of section 64 or section 66 may, within thirty days of the date of such order, appeal to the court to which appeals from the court making the order ordinarily lie, and such appellate court may direct that execution of the order be stayed pending disposal of the appeal.

Section 72: Appeals against orders of Registrar of Copyrights and Copyright Board

(1) Any person aggrieved by any final decision or order of the Registrar of Copyrights may, within three months from the date of the order or decision, appeal to the Copyright Board.

(2) Any person aggrieved by any final decision or order of the Copyright Board, not being a decision or order made in an appeal under sub-section (1), may, within three months from the date of such decision or order, appeal to the High Court within whose jurisdiction the appellant actually and voluntarily resides or carries on business or personally works for gain.

Provided that no such appeal shall lie against a decision of the Copyright Board under section 6.

(3) In calculating the period of three months provided for an appeal under this section, the time taken in granting a certified copy of the order or record of the decision appealed against shall be excluded.

1.10 SEBI ACT AND ITS REGULATIONS PERTAINING TO INFORMATION SECURITY

Section 30: Systems and procedures

Every depository shall have systems and procedures which will enable it to co-ordinate with the issuer or its agent, and the participants, to reconcile the records of ownership of securities with the issuer or its agent, as the case may be, and with participants, on a daily basis.

Section 31: Connectivity

Every depository shall maintain continuous electronic means of communication with all its participants, issuers or issuers' agents, as the case may be, clearing houses and clearing corporations of the stock exchanges and with other depositories.

Section 34: Internal monitoring, review and evaluation of systems and controls

Every depository shall have adequate mechanisms for the purposes of reviewing, monitoring and evaluating the depository's controls systems, procedures and safeguards.

Section 35: External monitoring, review and evaluation of systems and controls

Every depository shall cause an inspection of its controls, systems, procedures and safeguards to be carried out annually and forward a copy of the report to the Board.

Section 36: Insurance against risks

Every depository shall take adequate measures including insurance to protect the interests of the beneficial owners against risks likely to be incurred on account of its activities as a depository.

Section 37: Manner of keeping records

Where records are kept electronically by the depository, it shall ensure that the integrity of the automatic data processing systems is maintained at all times and take all precautions necessary to ensure that the records are not lost, destroyed or tampered with and in the event of loss or destruction, ensure that sufficient back up of records is available at all times at a different place.

Section 45: Connectivity

Every participant shall maintain continuous electronic means of communication with each depository in which it is a participant.

Section 46: Monitoring, reviewing and evaluating internal systems and controls

Every participant shall have adequate mechanism for the purpose of reviewing, monitoring and evaluating the participant's internal accounting controls and systems.

Section 50: Manner of keeping records

Where records are kept electronically by the participant it shall ensure that the integrity of the data processing systems is maintained at all times and take all precautions necessary to ensure that the records are not lost, destroyed or tampered with and in the event of loss or destruction, ensure that sufficient back up of records is available at all times at a different place.

1.11 RBI REGULATIONS FOR INFORMATION SECURITY

Reserve Bank of India has set up a 'Working Group on Internet Banking' to examine different aspects of Internet Banking (I-banking). The Group has focussed on three major areas of I-banking, i.e.,

(i) technology and security issues,
(ii) legal issues and
(iii) regulatory and supervisory issues.

RBI has accepted the recommendations of the Group to be implemented in a phased manner. Accordingly, the following guidelines are issued for implementation by banks. Banks are also advised that they may be guided by the original report, for a detailed guidance on different issues.

Technology and Security Standards

(i) Banks should designate a network and database administrator with clearly defined roles as indicated in the Group's report.

(ii) Banks should have a security policy duly approved by the Board of Directors. There should be a segregation of duty of Security Officer / Group dealing exclusively with information systems security and Information Technology Division which actually implements the computer systems. Further, Information Systems Auditor will audit the information systems.

(iii) Banks should introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards or other biometric technologies.

(iv) At the minimum, banks should use the proxy server type of firewall so that there is no direct connection between the Internet and the bank's system. It facilitates a high level of control and in-depth monitoring using logging and auditing tools. For sensitive systems, a stateful inspection firewall is recommended which thoroughly inspects all packets of information, and past and present transactions are compared. These generally include a real time security alert.

(v) All the systems supporting dial up services through modem on the same LAN as the application server should be isolated to prevent intrusions into the network as this may bypass the proxy server.

(vi) PKI (Public Key Infrastructure) is the most favoured technology for secure Internet banking services. However, as it is not yet commonly available, banks should use the following alternative system during the transition, until the PKI is put in place:

a. Usage of SSL (Secured Socket Layer), which ensures server authentication and use of client side certificates issued by the banks themselves using a Certificate Server.

b. The use of at least 128-bit SSL for securing browser to web server communications and, in addition, encryption of sensitive data like passwords in transit within the enterprise itself.

(vii) It is also recommended that all unnecessary services on the application server such as FTP (File Transfer Protocol), telnet should be disabled. The application server should be isolated from the e-mail server.

(viii) All computer accesses, including messages received, should be logged. Security violations (suspected or attempted) should be reported and follow up action taken should be kept in mind while framing future policy. Banks should acquire tools for monitoring systems and the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches. The banks should review their security infrastructure and security policies regularly and optimize them in the light of their own experiences and changing technologies. They should educate their security personnel and also the end-users on a continuous basis.

(ix) The information security officer and the information system auditor should undertake periodic penetration tests of the system, which should include:

a. Attempting to guess passwords using password-cracking tools.

b. Search for back door traps in the programs.

c. Attempt to overload the system using DDoS (Distributed Denial of Service) & DoS (Denial of Service) attacks.

d. Check if commonly known holes in the software, especially the browser and the e-mail software exist.

e. The penetration testing may also be carried out by engaging outside experts (often called 'Ethical Hackers').

(x) Physical access controls should be strictly enforced. Physical security should cover all the information systems and sites where they are housed, both against internal and external threats.

(xi) Banks should have proper infrastructure and schedules for backing up data. The backed-up data should be periodically tested to ensure recovery without loss of transactions in a time frame as given out in the bank's security policy. Business continuity should be ensured by setting up disaster recovery sites. These facilities should also be tested periodically.

(xii) All applications of banks should have proper record keeping facilities for legal purposes. It may be necessary to keep all received and sent messages both in encrypted and decrypted form.

(xiii) Security infrastructure should be properly tested before using the systems and applications for normal operations. Banks should upgrade the systems by installing patches released by developers to remove bugs and loopholes, and upgrade to newer versions which give better security and control

Legal Issues

(1) Considering the legal position prevalent, there is an obligation on the part of banks not only to establish the identity but also to make enquiries about integrity and reputation of the prospective customer. Therefore, even though request for opening account can be accepted over Internet, accounts should be opened only after proper introduction and physical verification of the identity of the customer.

(2) From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature. In India, the Information Technology Act, 2000, in Section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic

record. Any other method used by banks for authentication should be recognized as a source of legal risk.

(3) Under the present regime there is an obligation on banks to maintain secrecy and confidentiality of customers' accounts. In the Internet banking scenario, the risk of banks not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking/ other technological failures. The banks should, therefore, institute adequate risk control measures to manage such risks.

(4) In Internet banking scenario there is very little scope for the banks to act on stop-payment instructions from the customers. Hence, banks should clearly notify to the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted.

(5) The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. Currently, the rights and liabilities of customers availing of Internet banking services are being determined by bilateral agreements between the banks and customers. Considering the banking practice and rights enjoyed by customers in traditional banking, banks' liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. needs to be assessed and banks providing Internet banking should insure themselves against such risks.

Regulatory and Supervisory Issues

As recommended by the Group, the existing regulatory framework over banks will be extended to Internet banking also. In this regard, it is advised that:

(i) Only such banks which are licensed and supervised in India and have a physical presence in India will be permitted to offer Internet banking products to residents of India. Thus, both banks and virtual banks incorporated outside the country and having no physical presence in India will not, for the present, be permitted to offer Internet banking services to Indian residents.

(ii) The products should be restricted to account holders only and should not be offered in other jurisdictions.

(iii) The services should only include local currency products.

(iv) The 'in-out' scenario where customers in cross border jurisdictions are offered banking services by Indian banks (or branches of foreign banks in India) and the 'out-in' scenario where Indian residents are offered banking services by banks operating in cross-border jurisdictions are generally not permitted and this approach will apply to Internet banking also. The existing exceptions for limited purposes under FEMA i.e. where resident Indians have been permitted to continue to maintain their accounts with overseas banks etc., will, however, be permitted.

(v) Overseas branches of Indian banks will be permitted to offer Internet banking services to their overseas customers subject to their satisfying, in addition to the host supervisor, the home supervisor.

Given the regulatory approach as above, banks are advised to follow the following instructions:

a. All banks, who propose to offer transactional services on the Internet should obtain prior approval from RBI. Bank's application for such permission should indicate its business plan, analysis of cost and benefit, operational arrangements like technology adopted, business partners, third party service providers and systems and control procedures the bank proposes to adopt for managing risks. The bank should also submit a security policy covering recommendations made in this circular and a certificate from an independent auditor that the minimum requirements prescribed have been met. After the initial approval the banks will be obliged to inform RBI any material changes in the services / products offered by them.

b. Banks will report to RBI every breach or failure of security systems and procedure and the latter, at its discretion, may decide to commission special audit / inspection of such banks.

c. The guidelines issued by RBI on 'Risks and Controls in Computers and Telecommunications' vide circular DBS.CO.ITC.BC. 10/ 31.09.001/ 97-98 dated 4th February 1998 will equally apply to Internet banking. The RBI as supervisor will cover the entire risks associated with electronic banking as a part of its regular inspections of banks.

d. Banks should develop outsourcing guidelines to manage risks arising out of third party service providers, such as, disruption in service, defective services and personnel of service providers gaining intimate knowledge of banks' systems and misutilizing the same, etc., effectively.

e. With the increasing popularity of e-commerce, it has become necessary to set up 'Inter-bank Payment Gateways' for settlement of such transactions. The protocol for transactions between the customer, the bank and the portal and the framework for setting up of payment gateways as recommended by the Group should be adopted.

f. Only institutions who are members of the cheque clearing system in the country will be permitted to participate in Inter-bank payment gateways for Internet payment. Each gateway must nominate a bank as the clearing bank to settle all transactions. Payments effected using credit cards, payments arising out of cross border e-commerce transactions and all intra-bank payments (i.e., transactions involving only one bank) should be excluded for settlement through an inter-bank payment gateway.

g. Inter-bank payment gateways must have capabilities for both net and gross settlement. All settlement should be intra-day and as far as possible, in real time.

h. Connectivity between the gateway and the computer system of the member bank should be achieved using a leased line network (not through Internet) with appropriate data encryption standard. All transactions must be authenticated. Once, the regulatory framework is in place, the transactions should be digitally certified by any licensed certifying agency. SSL / 128 bit encryption must be used as minimum level of security. Reserve Bank may get the security of the entire infrastructure both at the payment gateway's end and the participating institutions' end certified prior to making the facility available for customers use.

i. Bilateral contracts between the payee and payee's bank, the participating banks and service provider and the banks themselves will form the legal basis for such transactions. The rights and obligations of each party must be clearly defined and should be valid in a court of law.

j. Banks must make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through Internet through a disclosure template. The banks should also provide their latest published financial results over the net.

k. Hyperlinks from banks' websites, often raise the issue of reputational risk. Such links should not mislead the customers into believing that banks sponsor any particular product or any business unrelated to banking. Hyperlinks from a banks' websites should be confined to only those portals with which they have a payment arrangement or sites of their subsidiaries or principals. Hyperlinks to banks' websites from other portals are normally meant for passing on information relating to purchases made by banks' customers in the portal. Banks must follow the minimum recommended security precautions while dealing with request received from other websites, relating to customers' purchases.

The Reserve Bank of India has decided that the Group's recommendations as detailed in this section should be adopted by all banks offering Internet banking services, with immediate effect. Even though the recommendations have been made in the context of Internet banking, these are applicable, in general, to all forms of electronic banking and banks offering any form of electronic banking should adopt the same to the extent relevant.

All banks offering Internet banking are advised to make a review of their systems in the light of this section and report to Reserve Bank the types of services offered, extent of their compliance with the recommendations, deviations and their proposal indicating a time frame for compliance.

CHAPTER 2

BUSINESS CONTINUITY PLANNING

2.1 INTRODUCTION

Business continuity – emphasis on “continuity” – is the ability of a business to continue operations in the face of a disaster condition. This means a business with a viable business continuity plan will be better able to continue doing what it did before a disaster event while assets damaged by the disaster event are recovered – until “business as usual” is resumed.

Business continuity means:

(i) identifying critical business functions
(ii) identifying risks to critical functions
(iii) identifying ways to avoid or mitigate the risks
(iv) having a plan to continue business in the event of a disaster condition
(v) having a plan to quickly restore operations to “business as usual.”

Disaster recovery is an integral part of business continuity. Business continuity does not replace insurance. It is a form of insurance, and should include insurance for life, health, facilities, product and business interruption.

The goal of business continuity and disaster recovery is to mitigate financial, operational, and business impacts to a business unit and to ensure its survivability under various scenarios. It assures that core processes will either be continued or effectively and efficiently restored in accordance with the business mission, which directly assures the overall success of the organization.

Owing largely to increased reliance on information technologies (IT), Contingency Management has been supplanted by the concept of Business Continuity, which focuses on the resiliency of people, processes, workspace, systems, safety, communication and new planning scenarios — loss of life, lack of decision makers, interruption of transportation, building evacuation, loss of physical assets and workspace, lack of communications, crisis command centers, terrorism, bio-terrorism etc.

Traditionally, data centers or offices of computing services alone have borne the responsibility for providing contingency planning. Frequently, this has led to the development of recovery plans to restore computer resources in a manner that is not fully responsive to the needs of the business and/or its customers supported by those resources. Contingency planning is a business issue rather than strictly and IT issue. Long-term operations outages often result in impacts of catastrophic proportions. The development of a viable continuity and recovery strategy for the business must be a product of the collective planning of not only the business's data center, communications and operations centers, but also the users and customers of those services who directly support the success of the business, and management personnel who determine acceptable levels of risk and bear responsibility for protecting the business's assets. Properly written, a BCP is a collection of procedures and information which is developed, compiled and maintained in readiness for use in the event of an emergency or disaster. This would include the elements of a disaster recovery plan (DRP).

Disasters vs. Disaster Conditions

A disaster, according to a planner, is any event that results in death or serious injury, or a business going out of business as a result of an event. A disaster condition is an inconvenience from which everyone and everything can be recovered not necessarily exactly as before the event, but restored to an equal or better footing. "Inconvenience" may be too mild a term for some who experienced a disaster condition, but consider this scenario:

A tornado roars through and flattens the business. If the business has a continuity plan that includes an alternate site, plans to rapidly transfer operations to the site, and includes support services to relieve its employees of worry about their families and possessions, the business can be doing business within an acceptable time, meeting its customers' needs and fending off competitors while restoring the operation to "business as usual" condition. There is an interruption. There most certainly is an inconvenience. There usually is added cost – overtime, rental facilities, expedited ordering and shipping, additional services such as catered meals – but, and this is the critical issue, business continues, income continues – perhaps at a slightly reduced level, but it continues nonetheless. Competitors won't succeed in stealing the business' customers due to missed commitments. Was the event – regardless of type: fire, flood, wind, etc. – a disaster? No. Was it a disaster condition? Yes.

Critical Business Functions

Critical business functions are functions a business must perform in order to stay in business. That means different things to different organizations. If the business' primary function – the one that generates income – is to produce valves, then a disruption to valve production puts the business at risk. There may be IT concerns such as CAD/CAM, customer lists, accounts receivable and accounts payable, but the primary function of the business is to make valves. If the production line is down, if raw material cannot be accepted and finished goods cannot be shipped, the company shuts down. For the valve company, the production line is the critical business and any risks associated with production – no matter how far removed from the actual production line – are legitimate concerns for the planner. Non-profits and governments need business continuity to assure that they can perform their mandated functions. When an assistance payment fails to arrive, there is a ripple effect – the person can't buy necessities, the business selling the necessities either loses business (and product stays in stock) or sells on credit, the wholesaler loses sales to the retailer (or sells on credit), the manufacturer loses an order from the wholesaler, and on and on.

Avoid, Mitigate, Absorb

Once critical functions and risks to those functions are identified, planners have three options:

(i) Avoid a risk, typically through redundancy.
(ii) Mitigate a risk by implementation of "work-arounds."
(iii) Absorb the risk.

The decision to avoid, mitigate, or absorb is a management decision. The planner makes recommendations based on cost vs. effectiveness and efficiency. Is it really necessary to have a very expensive hot site (explained later) for a valve manufacturing production line? Probably not. Is it really necessary to have a very expensive hot site for a 24 hour-a-day data intensive operation (such as Web-based securities sales)? Most assuredly.

In some cases, the decision to avoid, mitigate, or absorb is made for the planner and management by regulatory bodies which demand certain performance levels. In all cases, "fiduciary responsibility" plays a major role in management's decision. Management is liable if it fails to take reasonable and prudent measures to protect investors and employees. Avoiding a risk is a fairly obvious option. It usually is the most expensive and requires the most readiness.
Mitigation options may be fairly obvious; if the business is located in a flood plain, move all critical operations to floors above the 100-year flood level. Absorbing a risk is another matter. Letting an event take its toll seems counter to business continuity's purpose, but consider a company with obsolete equipment – from "AT" class computers to inefficient furnaces. If the obsolete equipment is insured, replacing it with modern equipment might improve the bottom line. Since insurance, an integral part of a business continuity plan, is footing at least part of the replacement cost, the business can buy replacement gear at a "discount."

Business Continuity for the Small Business

Everyone – small business, big business, non-profits, government, even the individual family – needs a business continuity plan, a way to continue their business or personal lives in face of a disaster condition. Business continuity is as much, perhaps more, for the small business as it is for the giant corporation. Unlike giant corporations, smaller enterprises typically are less able to survive a disaster (condition); they lack the financial clout and personnel resources of a Fortune 100. The small business does have some special financial assistance available from federal and state sources. These sources normally look more favorably on an enterprise with a business plan that includes a business continuity plan. Some insurance companies may offer discounts to businesses which implemented planner recommendations.

The Differences in Business Continuity, Disaster Recovery & Contingency Planning

A person builds a house on an ocean beach. A storm washes away the beach. The house collapses. Business continuity would suggest building a barrier reef or moving the house farther inland. Disaster recovery rebuilds the house in time for the next storm. Contingency planning takes the same scenario and says: "A storm will come ashore and damage the house; make sure there is someplace to live while the house is rebuilt."

What to Expect in a Business Continuity Plan

Business Continuity planning typically is a multi-stage (deliverable) process.

Phase 1 – BIA

The minimum expectation from a business continuity plan is a **business impact analysis**, a 'BIA'. The BIA:

(i) identifies business functions critical to the business' survival
(ii) identifies risks to those functions
(iii) rates (prioritizes) risks by probability of occurrence and impact on the business
(iv) identifies ways to avoid or mitigate identified risks
(v) prioritizes recommended avoidance and mitigation options

The plan may include suggested vendors, available financial resources, and other resources which may prove beneficial to implementation of avoidance and mitigation measures. The availability of this supplemental information is determined before planning commences and is in large measure dependent on how much time the planner has for research. (Resources constantly change and a planner should not be held to what was known "yesterday.") The business continuity process normally is suspended for a brief period while management reviews its options. The shorter the break the better since, as with most planning operations, momentum is a valuable asset.

Phase 2 – Disaster Recovery Plan

The disaster recovery plan includes:

(i) Reporting hierarchy, including executive management

(ii) Identifying primary and alternate disaster recovery team members; these are the people responsible to sustain the business operations and to restore or replace physical assets

(iii) Detailed description of each team member's responsibilities during a disaster condition

(iv) A list of internal and external vendors and contact information

(v) A list of regulatory agencies and contact information

(vi) A list of public service agencies and contact information

(vii) Appendix of control forms (report forms, expenses, etc.)

(viii) Minimum resources required to sustain the business operation while physical assets are restored or replaced.

Phase 3 – Disaster Recovery Team Training & Testing

This phase includes:

(i) Development of a test methodology and scenarios

(ii) Training disaster recovery team personnel to respond to a disaster condition with confidence

(iii) Revision of Business Continuity Plan as deficiencies are discovered during plan testing.

(iv) No plan is perfect the first time out; if it is, there is something wrong with the test.

Phase 4 – Plan Maintenance

Plan maintenance is in two parts:

(i) develop a maintenance policy and procedure

(ii) maintain the plan.

Plan maintenance is by both calendar and by "trigger" events. Calendar events are regularly scheduled reviews to assure all minor changes to the business are incorporated into the revised plan. Review frequency depends upon the business' dynamics. Trigger events are events which "trigger" plan maintenance. Such events include equipment, personnel, policy, procedural, product, and vendor changes.

A few quick words about vendors

All businesses depend on vendors. If a critical business function depends directly or indirectly on a vendor, make certain the vendor has a tested and maintained business continuity plan. The plan for your business is defective if the:

(i) Vendor lacks a plan
(ii) Vendor's plan has never been tested
(iii) Vendor's plan was updated more than a year ago.

The vendor's client is responsible to assure the vendor has a viable (tested and maintained) plan.

2.2 UNDERSTANDING BUSINESS IMPACT ANALYSIS (BIA)

What is business impact analysis? At a basic level it is a means of systematically assessing the potential impacts resulting from various (unavailability) events or incidents.

Business continuity planning deals with uncertainty and chance. What is important to note here is that even though you cannot predict whether or when a disaster will happen, that doesn't mean you can't plan for it. Just because we are not planning for an earthquake to hit us tomorrow morning at 10 A.M. doesn't mean that we can't plan the activities required to successfully survive when an earthquake (or similar disaster) does hit. The point of making these plans is to try to think of all the possible disasters that could take place, estimate the potential damage and loss, categorize and prioritize the potential disasters, and develop viable alternatives in case those events do actually happen.

A **business impact analysis (BIA)** is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function's criticality level. But how do we determine a classification scheme based on criticality levels? The BCP committee must identify the threats to the company and map them to the following characteristics:

(i) Maximum tolerable downtime
(ii) Operational disruption and productivity
(iii) Financial considerations
(iv) Regulatory responsibilities
(v) Reputation

The committee will not truly understand all business processes, the steps that must take place, or the resources and supplies that these processes require. So the committee must gather this information from the people who do know, which are department managers and specific employees throughout the organization. The committee starts by identifying the people who will be part of the BIA data-gathering sessions. The committee needs to identify how it will collect the data from the selected employees, be it surveys, interviews, or workshops. Next, the team needs to collect the information by actually conducting surveys, interviews, and workshops. Data points obtained as part of the information gathering will be used later during analysis. It is important that the team members ask about how different tasks get accomplished within the organization, be it a process, transaction, or service, along with any relevant dependencies. Process flow diagrams should be built, which will be used throughout the BIA and plan development stages.

Upon completion of the data collection phase, the BCP committee needs to conduct an analysis to establish which processes, devices, or operational activities are critical. If a system stands on its own, doesn't affect other systems, and is of low criticality, then it can be classified as a tier two or three recovery step. This means that these resources will not be dealt with during the recovery stages until the most critical (tier one) resources are up and running. This analysis can be completed using standard risk assessment and analysis methodologies. Threats can be manmade, natural, or technical. A manmade threat may be an arsonist, a terrorist, or a simple mistake that can have serious outcomes. Natural threats may be tornadoes, floods, hurricanes, or earthquakes. Technical threats may be data corruption, loss of power, device failure, or loss of a data communications line. It is important to identify all possible threats and estimate the probability of them happening.

BIA Steps

The more detailed and granular steps of a BIA are outlined here:

(i) Select individuals to interview for data gathering.
(ii) Create data-gathering techniques (surveys, questionnaires, qualitative and
(iii) quantitative approaches).
(iv) Identify the company's critical business functions.
(v) Identify the resources that these functions depend upon.
(vi) Calculate how long these functions can survive without these resources.
(vii) Identify vulnerabilities and threats to these functions.
(viii) Calculate risk for each different business function.
(ix) Document findings and report them to management.

Some issues may not immediately come to mind when developing these plans, such as an employee strike, vandals, disgruntled employees, or hackers, but they do need to be identified. These issues are often best addressed in a group with scenario-based exercises. This ensures that if a threat becomes reality, the plan includes the ramifications on all business tasks, departments, and critical operations. The more issues that are thought of and planned for, the better prepared a company will be if and when these events take place.

The committee needs to step through scenarios that could produce the following results:

(i) Equipment malfunction or unavailable equipment
(ii) Unavailable utilities (HVAC, power, communications lines)
(iii) Facility becomes unavailable
(iv) Critical personnel become unavailable
(v) Vendor and service providers become unavailable
(vi) Software and/or data corruption

The next step in the risk analysis is to assign a value to the assets that could be affected by each threat. This helps to establish economic feasibility of the overall plan. Assigning values to assets is not as straightforward as it seems. The value of an asset is not just the amount of money that was paid for it. The asset’s role to the company has to be considered along with the labor hours that went into creating it, if it is a piece of software. The value amount could also encompass the liability issues that surround the asset if it were damaged or insecure in any manner.

Qualitative and quantitative impact information should be gathered and then properly analyzed and interpreted. The goal is to see exactly how a business will be affected by different threats. The effects can be economical, operational, or both. Upon completion of the data analysis, it should be reviewed with the most knowledgeable people within the company to ensure that the findings are appropriate and describe the real risks and impacts the organization faces. This will help flush out any additional data points not originally obtained and will give a fuller understanding of all the possible business impacts. Loss criteria must be applied to the individual threats that were identified. The criteria may include the following:

(i) Loss in reputation and public confidence
(ii) Loss of competitive advantages
(iii) Increase in operational expenses
(iv) Violations of contract agreements
(v) Violations of legal and regulatory requirements
(vi) Delayed income costs
(vii) Loss in revenue
(viii) Loss in productivity

These costs can be direct or indirect and must be properly accounted for. So if the BCP team is looking at the threat of a terrorist bombing, it is important to identify which business function most likely would be targeted, how all business functions could be affected, and how each bulleted item in the loss criteria would be directly or indirectly involved. The timeliness of the recovery can be critical for business processes and the company's survival. For example, it may be acceptable to have the customer support functionality out of commission for two days, whereas five days may leave the company in financial ruin.

After identifying the critical functions, it is necessary to find out exactly what is required for these individual business processes to take place. The resources that are required for the identified business processes are not necessarily just computer systems, but may include personnel, procedures, tasks, supplies, and vendor support. It needs to be understood that if one or more of these support mechanisms is not available, the critical function may be doomed. The team must determine what type of effect unavailable resources and systems will have on these critical functions. The BIA identifies the company's critical systems that are needed for survival and estimates the outage time that can be tolerated by the company as a result of various unfortunate events. The outage time that can be endured by a company is referred to as the **maximum tolerable downtime (MTD)**.

Here are some MTD estimates that may be used within an organization:

(i) Nonessential 30 days
(ii) Normal 7 days
(iii) Important 72 hours
(iv) Urgent 24 hours
(v) Critical Minutes to hours

Each business function and asset should be placed in one of these categories, depending upon how long the company can survive without it. These estimates will help the company to determine what backup solutions are necessary to ensure the availability of these resources. For example, if being without a T1 communication line for three hours would cost the company $130,000, the T1 line would be considered critical and thus the company should put in a backup T1 line from a different carrier. If a server going down and being unavailable for ten days will only cost the company $250 in revenue, this would fall into the normal category and thus the company may not need to have a fully redundant server waiting to be swapped out. Instead, the company may choose to count on its vendor service level agreement (SLA), which, for example, may promise to have it back online in eight days. The BCP team must try to think of all possible events that could take place that could turn out to be detrimental to a company. The BCP team also must understand that it will not contemplate all events, and thus protection may not be available for every scenario introduced. Being properly prepared specifically for a flood, earthquake, terrorist attack, or lightning strike is not as important as being properly prepared to respond if one of the following results becomes reality:

(i) Equipment malfunction or unavailable equipment
(ii) Unavailable utilities (HVAC, power, communications lines)

(iii) Facility becomes unavailable
(iv) Critical personnel become unavailable
(v) Vendor and service providers become unavailable
(vi) Software and/or data corruption

All of the previously mentioned disasters could cause these results, but so could a meteor strike, a tornado, or a wing falling off of a plane passing overhead. So the moral to the story is to be prepared for the loss of any or all business resources, instead of focusing on the events that could cause the loss.

NOTE: A BIA is performed at the beginning of business continuity planning to identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. It identifies the company's critical systems needed for survival and estimates the outage time that can be tolerated by the company as a result of a disaster or disruption.

Interdependencies

Operations depend on manufacturing, manufacturing depends on R&D, payroll depends on accounting, and they all depend on IT. It is important to look at a company as a complex animal instead of a static two dimensional entity. It comprises many types of equipment, people, tasks, departments, communications mechanisms, and interfaces to the outer world. The biggest challenge of true continuity planning is understanding all of these intricacies and their interrelationships. A team may develop plans to back up and restore data, implement redundant data processing equipment, educate employees on how to carry out automated tasks manually, and obtain redundant power supplies. But if all of these components don't know how to work together in a different environment to get the products out the door, it might all be a waste of time. The following interrelation and interdependency tasks should be carried out by the BCP team and addressed in the resulting plan:

(i) Define essential business functions and supporting departments.
(ii) Identify interdependencies between these functions and departments.
(iii) Discover all possible disruptions that could affect the mechanisms necessary
(iv) To allow these departments to function together.
(v) Identify and document potential threats that could disrupt interdepartmental communication.
(vi) Gather quantitative and qualitative information pertaining to those threats.
(vii) Provide alternative methods of restoring functionality and communication.
(viii) Provide a brief statement of rationale for each threat and corresponding information.

The main goal of business continuity is to resume business as quickly as possible, spending the least amount of money.

Preventative Measures

During the BIA, the BCP team identified the maximum tolerable downtime for the critical resources. This was done to understand the business impact that would be caused if the assets were unavailable for one reason or another. It only makes sense that the team would try to reduce this impact and mitigate these risks by implementing preventative measures. Not implementing preventative measures would be analogous to going to a doctor, being told to stop eating 300 candy bars a day, increase physical activities, and start taking blood pressure medicine, and then choosing not to follow any of these preventative measures. Why go to the doctor in the first place? The same concept holds true with companies. If a team has been developed to identify risks and has come up with solutions, but the company does not implement at least some of these solutions, why put this team together in the first place? So, instead of just waiting for a disaster to hit to see how the company holds up, countermeasures should be integrated to better fortify the company from the impacts that were recognized. Appropriate and cost-effective, preventative methods and proactive measures are more preferable than reactionary methods. Which types of preventative mechanisms should be put in place depends upon the results of the BIA, but they may include some of the following components:

(i) Fortification of the facility in its construction materials
(ii) Redundant servers and communications links
(iii) Power lines coming in through different transformers
(iv) Redundant vendor support
(v) Purchasing of insurance
(vi) Purchasing of UPS and generators
(vii) Data backup technologies
(viii) Media protection safeguards
(ix) Increased inventory of critical equipment
(x) Fire detection and suppression systems

Recovery Strategies

In the recovery strategy stage, the team approaches this information from a different perspective. It now has to figure out what the company needs to do to actually recover the items that it has identified to be so important to the organization overall. The BIA provides the blueprint for the recovery strategies for all the components, because the business processes are totally dependent upon these other recovery strategies to take place properly. At this point, the findings from the BIA have been reported to management and management has allocated the necessary resources to move into the next phases. The BCP committee now must discover the most cost-effective recovery mechanisms that need to be implemented to address the threats that were identified in the BIA stage. Remember that in the BIA phase, the team calculated the potential losses for each identified threat. (If the facility were unavailable, it would cost the organization $200,000 a day, if the Internet connection were to go down, it would cost the company $12,000 per hour, and so on.) The team will use these values in its cost-benefit analysis when reviewing and choosing the necessary recovery solutions that need to be put into place to mitigate the organization's risk level. So what does the BCP team need to accomplish in the recovery strategy stage? The team needs to actually define the recovery strategies, which are a set of predefined activities that will be implemented and carried out in response to a disaster.

Sounds simple enough, but in reality this phase requires just as much work as the BIA phase. In the BIA, the team has calculated the necessary recovery times that must be met for the different critical business functions and the resources those functions rely upon. For example, let's say that the team has figured out it would cost the company $200,000 per day in lost revenue if its facility were destroyed and unusable. Now the team knows that the company has to be up and running within five to six hours or the company could be financially crippled. This would mean that the company needs to obtain a hot site or redundant facility that would allow it to be up and running in this amount of time. The team has figured out these types of timelines for the individual business functions, operations, and resources. Now it has to identify the recovery mechanisms and strategies that must be implemented to make sure that everything is up and running within the timelines that it has calculated. The team needs to break down these recovery strategies into the following sections:

(1) Business process recovery
(2) Facility recovery
(3) Supply and technology recovery
(4) User environment recovery
(5) Data recovery
(6) Recovery and Restoration

(1) Business Process Recovery

A business process is a set of interrelated steps linked through specific decision activities to accomplish a specific task. Business processes have starting and ending points and are repeatable. The processes should encapsulate the knowledge of services, resources, and operations provided by a company. For example, when a customer requests to buy a car via an organization's e-commerce site, a set of steps must be followed, such as these:

(i) Validate that the car is available.
(ii) Validate where the car is located and how long it would take to ship it to the destination.
(iii) Provide the customer with the price and delivery date.

(iv) Accept the customer’s credit card information.
(v) Validate and process the credit card order.
(vi) Send a receipt and tracking number to the customer.
(vii) Send the order to the car inventory location.
(viii) Restock inventory.
(ix) Send the order to accounting.

The BCP team needs to understand these different steps of the company’s most critical steps. The data is usually presented as a workflow document that contains the roles and resources that are needed for each process.

(2) Facility Recovery

There are three main categories of disruptions and they are usually classified as Non-disasters, disasters, and catastrophes. A non-disaster is a disruption in service as a result of a device malfunction or failure. The solution could include hardware, software, or file restoration. A disaster is an event that causes the entire facility to be unusable for a day or longer. This usually requires the use of an alternate processing facility and restoration of software and data from offsite copies. The alternate site must be available to the company until its main facility is repaired and usable. A catastrophe is a major disruption that destroys the facility altogether. This requires both a short-term solution, which would be an offsite facility, and a long-term solution, which may require rebuilding the original facility. Disasters and catastrophes are rare compared to non-disasters, thank goodness Non-disasters can usually be taken care of by replacing a device or restoring files from onsite backups. The BCP team needs to think through onsite backup requirements and make well-informed decisions. The team needs to identify the critical equipment and estimate the mean time between failure (MTBF) and mean time to repair (MTTR) to provide the necessary statistics of when a device may be meeting its maker and a new device may be required.

> **NOTE:** MTBF is the estimated lifetime of a piece of equipment. MTBF is calculated by the vendor of the equipment or a third party. The reason for using this value is to know approximately when a particular device will need to be replaced. MTTR is an estimate of how long it will take to fix a piece of equipment and get it back into production.

For larger disasters that affect the primary facility, an offsite backup facility must be accessible. Generally, contracts are established with third-party vendors to provide such services. The client pays a monthly fee to retain the right to use the facility in a time of need and then incurs a large activation fee when the facility actually has to be used. In addition, there would be a daily or hourly fee imposed for the duration of the stay. This is why subscription services for backup facilities should be considered a short-term solution and not a long-term solution. It is important to note that most recovery site contracts do not promise to house the company in need at a specific location, but rather promise to provide what has been contracted for somewhere within the company's locale. On and subsequent to September 11, 2001, many organizations with Manhattan offices were surprised when they were redirected by their backup site vendor not to sites located in New Jersey, which were already full, but rather to sites located in Boston, Chicago, or Atlanta. This adds yet another level of complexity to the recovery process, specifically the logistics of transporting people and equipment to locations originally unplanned for. Companies can choose from three main types of leased or rented offsite facilities:

(A) **Hot site:** A facility that is leased or rented and is fully configured and ready to operate within a few hours. The only missing resources from a hot site are usually the data, which will be retrieved from a backup site, and the people who will be processing the data. The equipment and system software must absolutely be compatible with the data being restored from the main site and must not cause any negative interoperability issues. These sites are a good choice for a company that needs to ensure that a site will be available for it as soon as possible. A hot site can support a short or long-term outage. Most hot-site facilities support annual tests that can be done by the company to ensure the site is functioning in the necessary state. This is the most expensive of the three types of offsite facilities and can have problems if a company requires proprietary or unusual hardware or software.

Hot Site Advantages

(i) Ready within hours for operation

(ii) Highly available

(iii) Usually used for short-term solutions, but available for longer stays

(iv) Annual testing available

Hot Site Disadvantages

(i) Very expensive

(ii) Limited on hardware and software choices

Note: The vendor of a hot site will provide the most commonly used hardware and software products to attract the largest customer base. This will most likely not include one specific customer's proprietary or unusual hardware or software products.

(B) **Warm site:** A leased or rented facility that is usually partially configured with some equipment, but not the actual computers. In other words, a warm site is usually a hot site without the expensive equipment. Staging a facility with duplicate hardware and computers configured for immediate operation is extremely expensive, so a warm site provides an alternate facility with some peripheral devices. This is the most widely used model. It is less expensive than a hot site and can be up and running within a reasonably acceptable time period. It may be a better choice for companies that depend upon proprietary and unusual hardware and software, because they will bring their own hardware and software with them to the site after the disaster hits. The odds of finding a remote site vendor that would have a Cray supercomputer that is readily available in a time of need are pretty slim. The drawback, however, is that the annual testing available with hot-site contracts is not usually available with warm-site contracts and thus a company cannot be certain that it will in fact be able to return to an operating state within hours.

(C) **Cold site:** A leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. It may take weeks to get the site activated and ready for work. The cold site could have equipment racks and dark fiber (fiber that does not have the circuit engaged) and maybe even desks, but would require the receipt of equipment from the client, since it does not provide any. The cold site is the least expensive option but takes the most time and effort to actually get up and functioning right after a disaster. Cold sites are often used as backups for call centers, manufacturing plants, and other services that either can be moved lock, stock, and barrel in one shot or would require extensive retooling and building.

Most companies use warm sites, which have some devices such as disk drives, tape drives, and controllers, but very little else. These companies usually cannot afford a hot site, and the extra downtime would not be considered detrimental. A warm site can provide a longer-term solution than a hot site. Companies that decide to go with a cold site must be able to be out of operation for a week or two. The cold site usually includes power, raised flooring, climate control, and wiring. The following provides a quick overview of the differences between offsite facilities:

Warm and Cold Site Advantages

(i) Less expensive
(ii) Availability for longer timeframes because of the reduced costs
(iii) Practical for proprietary hardware or software use

Warm and Cold Site Disadvantages

(i) Not immediately availa ble
(ii) Operational testing not usually available
(iii) Resources for operations not immediately available

Backup tapes or other media should be tested periodically on the equipment kept at the hot site to make sure the media is readable by those systems. If a warm site is used, the tapes should be brought to the original site and tested on those systems. The reason for the difference is that when a company uses a hot site, it depends on the systems located at the hot site; therefore, the media needs to be readable by those systems. If a company depends on a warm site, it will most likely bring its original equipment with it, so the media needs to be readable by the company's systems.

(3) Supply and Technology Recovery

At this point the BCP team has mapped out the necessary business functions that need to be up and running and the specific backup facility option that is best for its organization. Now the team needs to dig down into the more granular items, such as backup solutions for the following:

a. Network and computer equipment
b. Voice and data communications resources
c. Human resources
d. Transportation of equipment and personnel
e. Environment issues (HVAC)
f. Data and personnel security issues
g. Supplies (paper, forms, cabling, and so on)
h. Documentation

The organization's current technical environment must be understood. This means the planners have to know the intimate details of the network, communications technologies, computers, network equipment, and software requirements that are necessary to get the critical functions up and running. What is surprising to some people is that many organizations do not totally understand how their network is configured and how it actually works, because the network was most likely established five to ten years ago and has kept growing like a teenage boy going through puberty. New devices are added, new computers are added, new software packages are added, VoIP may have been integrated, and the DMZ may have been split up into three DMZs, with an extranet for the company's partners. Maybe the company bought and merged with another company and network. Over ten years, a number of technology refreshes most likely have taken place and the individuals who are maintaining the environment now are not the same people who built it ten years ago. Many IT departments experience employee turnover every one to five years. And most organizational network schematics are notoriously out of date, because everyone is busy with their current tasks or will come up with new tasks just to get out of having to update the schematic. So the BCP team has to make sure that if the networked environment is partially or totally destroyed, the recovery team has the knowledge and skill to properly rebuild it. The BCP team needs to take into account several things that are commonly overlooked, such as hardware replacements, software products, documentation, environmental needs, and human resources.

(4) User environment recovery

End users must be provided a functioning environment as soon as possible after a disaster hits. This means that the BCP team needs to understand the current operational and technical functioning environment and examine critical pieces so that they can be replicated. The first issue pertaining to users is how they will be notified of the disaster and who will tell them where to go and when. Each manager of the department would be responsible for notifying the people he is responsible for until everyone is on the same page. Then, one or two people must be in charge of coordinating the issues pertaining to users. This could mean directing them to a new facility, making sure they have the necessary resources to complete their tasks, restoring data, and being a liaison between the different groups.

In most situations, after a disaster, only few employees are put back to work. The BCP committee identified the most critical functions of the company during the analysis stage, and the employees who carry out those functions must be put back to work first. So the recovery process for the user environment should be laid out in different stages. The first stage is to get the most critical departments back online, the next stage is to get the second most important back online, and so on. The BCP team needs to identify user requirements, such as whether users can work on stand-alone PCs or need to be connected in a network to fulfill specific tasks. The BCP team also needs to identify how current automated tasks can be carried out manually if that becomes necessary. For example, if the Internet connection is going to be down for five hours, could the necessary communications take place through phone calls? It is up to the BCP team to realize that technology may be unavailable for a period of time and come up with solutions for those situations.

(5) Data recovery

Data has become one of the most critical assets to nearly all organizations. This data may include financial spreadsheets, blueprints on new products, customer information, product inventory, trade secrets, and more. Management would need to establish another group of individuals who would identify the company’s data, define a loss criterion, and establish the classification structure and processes. The BCP team’s responsibility is to provide solutions to protect this data and identify ways to restore it after a disaster. We’ll look at different ways that data can be protected and restored when needed. Data usually changes more often than hardware and software, so these backup procedures must happen on a continual basis. These backups can be full, differential, or incremental backups and are usually used in some type of combination with each other. A **full backup**, which is just what it sounds like—all data is backed up and saved to some type of storage media. A company can choose to do full backups only, in which case the restoration process is just one step, but the backup and restore processes could take a long time. Most companies choose to combine a full backup with a differential or incremental backup. A **differential process** backs up the files that have been modified since the last full backup. When the data needs to be restored, the full backup is laid down first and then the differential backup is put down on top of it. An incremental process backs up all the files that have changed since the last full or incremental backup. When the data needs to be restored, the full backup data is laid down and then each incremental backup is laid down on top of it in the proper order. If a company experienced a disaster and it used the **incremental process**, it would first need to restore the full backup on its hard drives and lay down every incremental backup that was carried out before the disaster took place. So, if the full backup was done six months ago and the operations department carried out an incremental backup each month, the restoration team would restore the full backup and start with the older incremental backups and restore each one of them until they were all restored.

(6) Recovery and Restoration

The BCP coordinator needs to define several different teams that should be properly trained and available if a disaster hits. The following are some examples of teams that a company may need to construct:

a. Damage assessment team
b. Legal team
c. Media relations team
d. Network recovery team
e. Relocation team
f. Restoration team
g. Salvage team
h. Security team
i. Telecommunications team

The restoration team should be responsible for getting the alternate site into a working and functioning environment, and the salvage team should be responsible for starting the recovery of the original site. Both teams must know how to do many tasks, such as install operating systems, configure workstations and servers, string wire and cabling, set up the network and configure networking services, and install equipment and applications. Both teams must also know how to restore data from backup facilities, and how to do so in a secure manner that ensures that the system's and data's confidentiality, integrity, and availability are not compromised.

2.3 VARIOUS TERMS ASSOCIATED WITH BUSINESS IMPACT ANALYSIS

Exposure factor (EF): This factor represents a measure of the magnitude of loss or impact on the value of an asset. It is expressed as a percent, ranging from 0% to 100%, of asset value loss arising from a threat event. This factor is used in the calculation of single loss expectancy (SLE).

Single Loss expectancy (SLE): This value is classically derived from the following formula to determine the monetary loss (impact) for each occurrence of a threatened event:

ASSET VALUE x EXPOSURE FACTOR = SINGLE LOSS EXPECTANCY

The SLE is usually an end result of a business impact analysis (BIA). A BIA typically stops short of evaluating the related threats' ARO or its significance. The SLE represents only one element of risk, the expected impact, monetary or otherwise, of a specific threat event. Because the BIA usually characterizes the massive losses resulting from a catastrophic event, however improbable, it is often employed as a scare tactic to get management attention and loosen budgetary constraints, often unreasonably.

Annualized rate of occurrence (ARO): This term characterizes, on an annualized basis, the frequency with which a threat is expected to occur. For example, a threat occurring once in 10 years has an ARO of 1/10 or 0.1; a threat occurring 50 times in a given year has an ARO of 50.0. The possible range of frequency values is from 0.0 (the threat is not expected to occur) to some whole number whose magnitude depends on the type and population of threat sources.

Annualized loss expectancy (ALE): This discrete value is derived, classically, from the following formula,

SINGLE LOSS EXPECTANCY x ANNUALIZED RATE OF OCCURRENCE = ANNUALIZED LOSS EXPECTANCY

To effectively identify risk and to plan budgets for information risk management and related risk reduction activity, it is helpful to express loss expectancy in annualized terms. For example, the preceding algorithm will show that the ALE for a threat (with an SLE of Rs1,000,000) that is expected to occur only about once in 10,000 years is Rs1,000,000 divided by 10,000, or only Rs100.00. When the expected threat frequency (ARO) is factored into the equation, the significance of this risk factor is addressed and integrated into the information risk management process. Thus, risk is more accurately portrayed, and the basis for meaningful cost/benefit analysis of risk reduction measures is established.

Developing Goals for the Plans

A goal could be, “Keep the company in business if an earthquake hits.” Good goal, but not overly useful without more clarity and direction. To be useful, a goal must contain certain key information, such as the following:

(i) **Responsibility:** Each individual involved with recovery and continuity should have their responsibilities spelled out in writing to ensure a clear understanding in a chaotic situation. So, for example, instead of just running out of the building screaming, an individual must know that he is responsible for shutting down the servers before he can run out of the building screaming.

(ii) **Authority** In times of crisis, it is important to know who is in charge. Teamwork is important in these situations, and almost every team does much better with an established and trusted leader. Such leaders must know that they are expected to step up to the plate in a time of crisis and understand what type of direction they should provide to the rest of the employees. Clearcut authority will aid in reducing confusion and increasing cooperation.

(iii) **Priorities** It is extremely important to know what is critical versus what is merely nice to have. Different departments provide different functionality for an organization. The critical departments must be singled out from the departments that provide functionality that the company can live without for a week or two. It is necessary to know which department must come online first, which second, and so on. The general priorities must beset by the management with the help of the different departments and IT staff.

(iv) **Implementation and testing**. Once a continuity plan is developed, it actually has to be put into action. It needs to be documented and put in places that are easily accessible in times of crisis. The people who are assigned specific tasks need to be taught and informed how to fulfill those tasks, and dry runs need to be done to walk people through different situations. The drills should take place at least once a year, and the entire program should be continually updated and improved.

Implementing Strategies

Once the strategies have been decided upon, they need to be documented and put into place by the BCP team. This moves the efforts from a purely planning stage to an actual implementation and action phase. Copies of the plans need to be kept in one or more locations other than the primary site, so that if the primary site is destroyed or negatively affected, the continuity plan is still available to the teams. It is also critical that different formats of the plan be available to the team, including both electronic and paper versions. An electronic version of the plan is not very useful if you don't have any electricity to run a computer. In addition to having copies of the recovery documents located at their offices and homes, key individuals should also have easily accessible versions of critical procedures and call tree information.

The actual format of the plan will depend on the environment, goals of the plan, priorities, and identified threats. After each of those items is examined and documented, the topics of the plan can be divided into the necessary categories. Each organization's BCP looks different, but these core topics should be covered in some fashion.

The role of the plan is to provide preplanned and sequenced structure to these different processes. The plan also needs to integrate a degree of flexibility, because no one knows exactly what type of disaster will take place nor its effects. Although procedures need to be documented for the different phases of the plan, a balance between detail and flexibility needs to be achieved so that the company is not ready for only one type of disaster. Some organizations develop individual plans for specific tasks and goals. It is up to management and the BCP team to determine the number and types of plans that should be developed and implemented. The BCP team can choose to integrate many of these components into the BCP, if the company is small, or include these plans as appendices to the BCP. It is usually better to include these stand-alone plans as appendices so that each document is clear, concise, and useable.

2.4 DIFFERENT TYPES OF CONTINUITY PLANS

(i) **Business resumption plan :** Focuses on how to re-create the necessary business processes that need to be reestablished instead of focusing on IT components (i.e., process oriented instead of procedural oriented).

(ii) **Continuity of operations plan (COOP):** Establishes senior management and a headquarters after a disaster. Outlines roles and authorities, orders of succession, and individual role tasks.

(iii) **IT contingency plan:** Plan for systems, networks, and major applications recovery procedures after disruptions. A contingency plan should be developed for each major system and application.

(iv) **Crisis communications plan:** Includes internal and external communications structure and roles. Identifies specific individuals who will communicate with external entities. Contains pre developed statements that are to be released.

(v) **Cyber incident response plan:** Focuses on malware, hackers, intrusions, attacks, and other security issues. Outlines procedures for incident response.

(vi) **Disaster recovery plan:** Focuses on how to recover various IT mechanisms after a disaster. Whereas a contingency plan is usually for non-disasters, a disaster recovery plan is for disasters that require IT processing to take place at another facility.

(vii) **Occupant emergency plan:** Establishes personnel safety and evacuation procedures.

2.5 TESTING AND REVISING THE PLAN

The BCP should be tested regularly, because environments continually change. Tests and disaster recovery drills and exercises should be performed at least once a year. A company should have no real confidence in a developed plan until it has actually been tested. The tests and drills prepare personnel for what they may be faced with and provide a controlled environment to learn the tasks expected of them. These tests and drills also point out issues to the planning team and management that may not have been previously thought about and addressed as part of the planning process. The exercises, in the end, demonstrate whether a company can actually recover after a disaster.

There are a few different types of drills and tests that can take place, each with its own pros and cons. The following sections explain the different types of drills.

Checklist Test

In this type of test, copies of the BCP are distributed to the different departments and functional areas for review. This is done so that each functional manager can review the plan and indicate if anything has been left out or if some approaches should be modified or deleted. This is a method that ensures that some things have not been taken for granted or omitted. Once the departments have reviewed their copies and made suggestions, the planning team then integrates those changes into the master plan.

Structured Walk-Through Test

In this test, representatives from each department or functional area come together to go over the plan to ensure its accuracy. The group reviews the objectives of the plan, discusses the scope and assumptions of the plan, reviews the organization and reporting structure, and evaluates the testing, maintenance, and training requirements described. This gives the people who are responsible for making sure that a disaster recovery happens effectively and efficiently a chance to review what has been decided upon and what is expected of them. The group walks through different scenarios of the plan from beginning to end to make sure nothing was left out. This also raises the awareness of the recovery procedures to team members.

Simulation Test

This type of test takes a lot more planning and people. In this situation, all employees who participate in operational and support functions, or their representatives, come together to practice executing the disaster recovery plan based on a specific scenario. The scenario is used to test the reaction of each operational and support representative. Again, this is done to ensure that specific steps were not left out and certain threats were not overlooked. It acts as a catalyst to raise the awareness of the people involved. The drill includes only those materials that will be available in an actual disaster, to portray a more realistic environment. The simulation test continues up to the point of actual relocation to an offsite facility and actual shipment of replacement equipment.

Parallel Test

A parallel test is done to ensure that the specific systems can actually perform adequately at the alternate offsite facility. Some systems are moved to the alternate site and processing takes place. The results are compared with the regular processing that is done at the original site. This points out any necessary tweaking, reconfiguring, or steps that need to take place.

Full-Interruption Test

This type of test is the most intrusive to regular operations and business productivity. The original site is actually shut down and processing takes place at the alternate site. The recovery team fulfills its obligations in preparing the systems and environment for the alternate site. All processing is done only on devices at the alternate offsite facility. This is a full-blown drill that takes a lot of planning and coordination, but it can reveal many holes in the plan that need to be fixed before an actual disaster hits. Full interruption tests should be performed only after all other types of tests have been successful. They are the most risky and can impact the business in very serious and devastating ways if not managed properly; therefore, senior management approval needs to be obtained prior to performing full-interruption tests. The type of organization and its goals will dictate what approach to the training exercise is most effective. Each organization may have a different approach and unique aspects. If detailed planning methods and processes are going to be taught, then specific training may be required, rather than general training that provides an overview. Higher quality training will result in an increase of employee interest and commitment. During and after each type of test, a record of the significant events should be documented and reported to management so that it is aware of all outcomes of the test.

Maintaining the Plan

Unfortunately, the various plans that have been covered in this chapter can become quickly out of date. An out of date BCP may provide a company with a false sense of security, which could be devastating if and when a disaster actually takes place. The main reasons plans become outdated include the following:

(i) The business continuity process is not integrated into the change management process.
(ii) Infrastructure and environment changes occur.
(iii) Reorganization of the company, layoffs, or mergers occur.
(iv) Changes in hardware, software, and applications occur.
(v) After the plan is constructed, people feel that their job is done.
(vi) Personnel turns over.
(vii) Large plans take a lot of work to maintain.
(viii) Plans do not have a direct line to profitability.

Organizations can keep the plan updated by taking the following actions:

(i) Make business continuity a part of every business decision.
(ii) Insert the maintenance responsibilities into job descriptions.
(iii) Include maintenance in personnel evaluations.
(iv) Perform internal audits that include disaster recovery and continuity documentation and procedures.
(v) Perform regular drills that use the plan.
(vi) Integrate the BCP into the current change management process.

One of the simplest and most cost-effective and process-efficient ways to keep a plan up to date is to incorporate it within the change management process of the organization. When you think about it, it makes a lot of sense. Where do you document new applications, equipment, or services? Where do you document updates and patches? Your change management process should be updated to incorporate fields and triggers that alert the BCP team when a significant change will occur and should provide a means to update the recovery documentation. What's the point of removing the dust bunnies off a plan if it has your configurations from three years ago? There is nothing worse than that feeling at the pit of your stomach when you realize the one thing you thought was going to save you will in fact only serve to keep a fire stoked with combustion material.

Summary

Although business continuity planning is usually given low priority in most organizations today, that does not mean that it is not important and crucial. Unfortunately, many companies have to experience the pain of a disaster to understand how it could have circumvented or mitigated the events that caused the pain to occur. To develop and carry out business continuity efforts successfully, plenty of thought, planning, time, and effort must go into the different phases of this activity. The real threats must be identified and understood, reasonable countermeasures must be put into place, and detailed plans must be outlined for the unfortunate but anticipated day when they are needed.

CHAPTER 3

ACCESS CONTROL

3.1 INTRODUCTION

At its simplest, the goal of access control is to protect an organization's resources from unauthorized access while facilitating seamless and legitimate use of these resources. In today's information age, users need access to those resources through a broad variety of devices, such as PCs, laptops, PDA's, smart phones. Organizations need to provide their business partners, customers, and employees with access to applications, documents, and data from any device whether it is inside or outside the corporate network and as securely as possible.

Fundamental goals of security include **confidentiality** for controlling who gets to access information and resources; **integrity** for providing control of how information changes or resources are used; **availability** for timely access to information and resources; and **accountability** for knowing who has access to information and resources. Access control is a foundational component of security that helps achieve these goals. Access Control is collection of technologies that help organizations realize their **identity and access management** solution while lessen the information security **threats and vulnerabilities**.

3.2 ACCESS CONTROL PRINCIPLES AND OBJECTIVES

Types of Information Security Controls

Security is generally defined as the freedom from danger or as the condition of safety. Computer security, specifically, is the protection of data in a system against unauthorized disclosure, modification, or destruction and protection of the computer system itself against unauthorized use, modification, or denial of service.

Controls for providing information security can be:
(1) Physical
(2) Technical
(3) Administrative

These three categories of controls can be further classified as either
(a) Preventative
(b) Detective

Preventive controls attempt to avoid the occurrence of unwanted events.
Detective controls attempt to identify unwanted events after they have occurred.

Common detective controls include audit trails, intrusion detection methods, and checksums.

Three other types of controls supplement preventive and detective controls are:
(i) Deterrent
(ii) Corrective
(iii) Recovery

Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures. These usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential intruder to not violate security (e.g., threats ranging from embarrassment to severe punishment).

Corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation. Execution of corrective controls could result in changes to existing physical, technical, and administrative controls.

Recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation.
Deterrent, corrective, and recovery controls are considered to be special cases within the major categories of physical, technical, and administrative controls; they do not clearly belong in either preventive or detective categories.

For example, it could be argued that deterrence is a form of prevention because it can cause an intruder to turn away; however, deterrence also involves detecting violations, which may be what the intruder fears most. Corrective controls, on the other hand, are not preventive or detective, but they are clearly linked with technical controls when antiviral software eradicates a virus or with administrative controls when backup procedures enable restoring a damaged data base. Finally, recovery controls are neither preventive nor detective but are included in administrative controls as disaster recovery.

(1) Physical Controls

Physical security is the use of locks, security guards, badges, alarms, and similar measures to control access to computers, related equipment (including utilities), and the processing facility itself. In addition, measures are required for protecting computers, related equipment, and their contents from spying, theft, and destruction or damage by accident, fire, or natural disaster e.g., floods and earthquakes.

a. Preventive Physical Controls

Preventive physical controls are employed to prevent unauthorized personnel from entering computing facilities and to help protect against natural disasters. Examples of these controls include:
Backup files and documentation.

(i) Fences.
(ii) Security guards.
(iii) Badge systems.
(iv) Double door systems.
(v) Locks and keys.
(vi) Backup power.
(vii) Biometric access controls.
(viii) Site selection.
(ix) Fire extinguishers.

b. Detective Physical Controls

Detective physical controls warn protective services personnel that physical security measures are being violated. Examples of these controls include:

(i) Motion detectors.
(ii) Smoke and fire detectors.
(iii) Closed-circuit television monitors.
(iv) Sensors and alarms.

(2) Technical Controls

Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices. Technical controls are sometimes referred to as logical controls.

a. Preventive Technical Controls

Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Examples of these controls include:

(i) Access control software.
(ii) Antivirus software.
(iv) Library control systems.
(v) Passwords.
(vi) Smart cards.
(vii) Encryption.
(viii) Dial-up access control and callback systems.

b. Detective Technical Controls

Detective technical controls warn personnel of violations or attempted violations of preventive technical controls. Examples of these include audit trails and intrusion detection expert systems,

Audit Trails

An audit trail is a record of system activities that enables the reconstruction and examination of the sequence of events of a transaction, from its inception to output of final results.

Intrusion Detection Systems

These expert systems track users (on the basis of their personal profiles) while they are using the system to determine whether their current activities are consistent with an established norm.

(3) Administrative Controls

Administrative, or personnel, security consists of management constraints, operational procedures, accountability procedures, and supplemental administrative controls established to provide an acceptable level of protection for computing resources. In addition, administrative controls include procedures established to ensure that all personnel who have access to computing resources have the required authorizations and appropriate security clearances.

a. Preventive Administrative Controls

Preventive administrative controls are personnel-oriented techniques for controlling people's behavior to ensure the confidentiality, integrity, and availability of computing data and programs. Examples of preventive administrative controls include:

(i) Security awareness and technical training.
(ii) Separation of duties.
(iii) Procedures for recruiting and terminating employees.
(iv) Security policies and procedures.
(v) Supervision.
(vi) Disaster recovery, contingency, and emergency plans.
(vii) User registration for computer access.

Security Awareness and Technical Training

Security awareness training is a preventive measure that helps users to understand the benefits of security practices. If employees do not understand the need for the controls being imposed, they may eventually circumvent them and thereby weaken the security program or render it ineffective.

Separation of Duties

This administrative control separates a process into component parts, with different users responsible for different parts of the process. Judicious separation of duties prevents one individual from obtaining control of an entire process and forces collusion with others in order to manipulate the process for personal gain.

Recruitment and Termination Procedures

Appropriate recruitment procedures can prevent the hiring of people who are likely to violate security policies. A thorough background investigation should be conducted, including checking on the applicant's criminal history and references. Although this does not necessarily screen individuals for honesty and integrity, it can help identify areas that should be investigated further.

Security Policies and Procedures

Appropriate policies and procedures are key to the establishment of an effective information security program. Policies and procedures should reflect the general policies of the organization as regards the protection of information and computing resources. Policies should cover the use of computing resources, marking of sensitive information, movement of computing resources outside the facility, introduction of personal computing equipment and media into the facility, disposal of sensitive waste, and computer and data security incident reporting. Enforcement of these policies is essential to their effectiveness.

Supervision

Often, an alert supervisor is the first person to notice a change in an employee's attitude. Early signs of job dissatisfaction or personal distress should prompt supervisors to consider subtly moving the employee out of a critical or sensitive position.

Disaster Recovery, Contingency, and Emergency Plans

The disaster recovery plan is a document containing procedures for emergency response, extended backup operations, and recovery should a computer installation experience a partial or total loss of computing resources or physical facilities (or of access to such facilities). The primary objective of this plan, used in conjunction with the contingency plans, is to provide reasonable assurance that a computing installation can recover from disasters, continue to process critical applications in a degraded mode, and return to a normal mode of operation within a reasonable time. A key part of disaster recovery planning is to provide for processing at an alternative site during the time that the original facility is unavailable.

User Registration for Computer Access

Formal user registration ensures that all users are properly authorized for system and service access. In addition, it provides the opportunity to acquaint users with their responsibilities for the security of computing resources and to obtain their agreement to comply with related policies and procedures.

b. Detective Administrative Controls

Detective administrative controls are used to determine how well security policies and procedures are complied with, to detect fraud, and to avoid employing persons that represent an unacceptable security risk. This type of control includes:

(i) Security reviews and audits.
(ii) Performance evaluations.
(iii) Required vacations.
(iv) Background investigations.
(v) Rotation of duties.

Security Reviews and Audits

Reviews and audits can identify instances in which policies and procedures are not being followed satisfactorily. Management involvement in correcting deficiencies can be a significant factor in obtaining user support for the computer security program.

Performance Evaluations

Regularly conducted performance evaluations are an important element in encouraging quality performance. In addition, they can be an effective forum for reinforcing management's support of information security principles.

Required Vacations

Tense employees are more likely to have accidents or make errors and omissions while performing their duties. Vacations contribute to the health of employees by relieving the tensions and anxieties that typically develop from long periods of work.

Background Investigations

Background investigations may disclose past performances that might indicate the potential risks of future performance. Background investigations should be conducted on all employees being considered for promotion or transfer into a position of trust; such investigations should be completed before the employee is actually placed in a sensitive position. Job applicants being considered for sensitive positions should also be investigated for potential problems. Companies involved in government-classified projects should conduct these investigations while obtaining the required security clearance for the employee.

Rotation of Duties

Like required vacations, rotation of duties (i.e., moving employees from one job to another at random intervals) helps deter fraud. An additional benefit is that as a result of rotating duties, employees are cross-trained to perform each other's functions in case of illness, vacation, or termination.

3.3 ACCESS CONTROL TECHNIQUES

Access control techniques are generally categorized as either

(1) discretionary
(2) mandatory
(3) role-based

(1) DISCRETIONARY ACCESS CONTROL (DAC)

DAC is an access policy determined by the owner of a file (or other resource). The owner decides who is allowed access to the file and what privileges they have. Two important concepts in DAC are File and data ownership: Every object in a system must have an owner. The access policy is determined by the owner of the resource (including files, directories, data, system resources, and devices). Theoretically, an object without an owner is left unprotected. Normally, the owner of a resource is the person who created the resource (such as a file or directory).

Access rights and permissions: These are the controls that an owner can assign to individual users or groups for specific resources.

Discretionary access control in RDBMS

This section describes the discretionary access control (DAC) facilities included in the SQL standard and also the limitations associated with it.

SQL Privileges

The creator of a relation in an SQL data base is its owner and can grant other users access to that relation. The access privileges or modes recognized in SQL correspond directly to the CREATE, INSERT, SELECT, DELETE, and UPDATE. In addition, a REFERENCES privilege controls the establishment of foreign keys to a relation.

The CREATE Statement

SQL does not require explicit permission for a user to create a relation, unless the relation is defined to have a foreign key to another relation. In this case, the user must have the REFERENCES privilege for appropriate columns of the referenced relation. To create a view, a user must have the SELECT privilege on every relation mentioned in definition of the view. If a user has INSERT, DELETE, or UPDATE privileges on these relations, corresponding privileges will be obtained on the view (if it is updatable).

The GRANT Statement

The owner of a relation can grant one or more access privileges to another user. This can be done with or without the GRANT OPTION. If the owner grants SELECT with the GRANT OPTION, the user receiving this grant can further grant SELECT to other users. The latter GRANT can be done with or without the GRANT OPTION at the granting user's discretion.
The general format of a grant operation in SQL is as follows:

GRANT privileges [ON relation] TO users [WITH GRANT OPTION]

The GRANT command applies to base relations as well as to views. The brackets on the ON and WITH clauses denotes that these are optional and may not be present in every GRANT command. It is not possible to grant a user the grant option on a privilege, without allowing the grant option itself to be further granted.

The REVOKE Statement

It is often necessary that revocation cascade. In a cascading revoke, not only is the privilege revoked, so too are all GRANTs based on the revoked privilege. For example, if user Tom grants Dick SELECT on relation R with the GRANT OPTION, Dick subsequently grants Harry SELECT on R, and Tom revokes SELECT on R from Dick, the SELECT on R privilege is taken away not only from Dick but also from Harry. The precise mechanics of a cascading revoke is somewhat complicated. If Dick had received the SELECT on R privilege (with GRANT OPTION) not only from Tom but also from Jane before Dick granted SELECT to Harry, Tom's revocation of the SELECT from R privilege from Dick would not cause either Dick or Tom to lose this privilege. This is because the GRANT from Jane remains valid.

Cascading revocation is not always desirable. A user's privileges to a given table are often revoked because the user's job functions and responsibilities have changed. For example, if Mary, the head of a department moves on to a different assignment, her privileges to her former department's data should be revoked. However, a cascading revoke could cause lots of employees of that department to lose their privileges. These privileges must then be re-granted to keep the department functioning.
SQL'92 allows a revocation to be cascading or not cascading, as specified by the revoker. This is a partial solution to the more general problem of how to reassign responsibility for managing access to data from one user to another as their job assignments change.

Limitations of DAC

The standard access controls of SQL are said to be discretionary because the granting of access is under user control. Discretionary controls have a fundamental weakness, however. Even when access to a relation is strictly controlled, a user with SELECT access can create a copy of the relation, thereby circumventing these controls. Furthermore, even if users can be trusted not to engage deliberately in such mischief, programs infected with Trojan horses can have the same disastrous effect.

For example, in the following GRANT operation:

TOM: GRANT SELECT ON EMPLOYEE TO DICK

Tom has not conferred the GRANT option on Dick. Tom's intention is that Dick should not be allowed to further grant SELECT access on EMPLOYEE to other users. However, this intent is easily subverted as follows. Dick creates a new relation, COPY-OF-EMPLOYEE, into which he copies all the rows of EMPLOYEE.

As the creator of COPY-OF-EMPLOYEE, Dick can grant any privileges for it to any user. Dick can therefore grant Harry access to COPY-OF-EMPLOYEE as follows:

DICK: GRANT SELECT ON COPY-OF-EMPLOYEE TO HARRY

At this point, Harry has access to all the information in the original EMPLOYEE relation. For all practical purposes, Harry has SELECT access to EMPLOYEE, so long as Dick keeps COPY-OF-EMPLOYEE reasonably up to date with respect to EMPLOYEE.

The problem, however, is actually worse than this scenario indicates. It portrays Dick as a cooperative participant in this process. For example, it might be assumed that Dick is a trusted confidant of Tom and would not deliberately subvert Tom's intentions regarding the EMPLOYEE relation. But if Dick were to use a text editor supplied by Harry, which Harry had programmed to create the COPY-OF-EMPLOYEE relation and execute the preceding GRANT operation, the situation might be different. Such software is said to be a Trojan horse because in addition to the normal functions expected by its user it also engages in surreptitious actions to subvert security. Thus, a Trojan horse executed by Tom could actually grant Harry the privilege to SELECT on EMPLOYEE.

Organizations trying to avoid such scenarios can require that all software they run on relational data bases be free of Trojan horses, but this is generally not considered a practical option. The solution is to impose mandatory controls that cannot be violated, even by Trojan horses.

(2) MANDATORY ACCESS CONTROLS (MAC)

Mandatory access control is also known as **Bell-Lapadula mobel**. MAC is an access policy determined by the system, not the owner. MAC is used in multilevel systems that process highly sensitive data, such as classified government and military information. A multilevel system is a single computer system that handles multiple classification levels between subjects and objects. Mandatory access controls (MACs) are based on security labels associated with each data item and each user. A label on a data item is called a security **classification**; a label on a user is called security **clearance**. In a computer system, every program run by a user inherits the user's security clearance.

In general, security labels form a lattice structure. This discussion assumes the simplest situation, in which there are only two labels: S for secret and U for unclassified. It is forbidden for S information to flow into U data items i.e. label S > label U. Two mandatory access controls rules achieve this objective:

Simple security property

A U-user cannot read S-data.

***(Star) property**

A S-user cannot write U-data.

Some important points should be clearly understood in this context. First, the rules assume that a human being with S clearance can log in to the system as a S-user or a U-user. Otherwise, the star property prevents top executives from writing publicly readable data. Second, these rules prevent only the observable reading and writing of data. Finally, mandatory access controls in relational data bases usually enforce a strong star property:

Strong star property

A S-user cannot write U-data, and a U-user cannot write S-data. The strong star property limits users to writing at their own level, for reasons of integrity. The (weak) star property allows a U-user to write S-data. This can result in overwriting, and therefore destruction, of S-data by U-users.

Labeling Granularity

Security labels can be assigned to data at different levels of granularity in relational data bases. Assigning labels to entire relations can be useful but is generally inconvenient. For example, if some salaries are secret but others are not, these salaries must be placed in different relations. Assigning labels to an entire column of a relation is similarly inconvenient in the general case.

The finest granularity of labeling is at the level of individual attributes of each tuple or row or at the level of individual element-level labeling. This offers considerable flexibility. Most of the products emerging offer labeling at the level of a tuple. Although not so flexible as element-level labeling, this approach is definitely more convenient than using relation- or column-level labels. Products in the short term can be expected to offer tuple-level labeling.

(3) ROLE-BASED ACCESS CONTROL

Traditional DACs are proving to be inadequate for the security needs of many organizations. At the same time, MACs based on security labels are inappropriate for many situations. In recent years, the notion of role-based access control (RBAC) has emerged as a candidate for filling the gap between traditional DAC and MAC.

One of weaknesses of DAC in SQL is that it does not facilitate the management of access rights. Each user must be explicitly granted every privilege necessary to accomplish his or her tasks. Often groups of users need similar or identical privileges. All supervisors in a department might require identical privileges;

similarly, all clerks might require identical privileges, different from those of the supervisors. RBAC allows the creation of roles for supervisors and clerks. Privileges appropriate to these roles are explicitly assigned to the role, and individual users are enrolled in appropriate roles from where they inherit these privileges. This arrangement separates two concerns: (1) what privileges should a role get and (2) which user should be authorized to each role. RBAC eases the task of reassigning users from one role to another or altering the privileges for an existing role.

Current efforts at evolving SQL, commonly called SQL3, have included proposals for RBAC based on vendor implementations, such as in Oracle. In the future, consensus on a standard approach to RBAC in relational data bases should emerge. However, this is a relatively new area, and a number of questions remain to be addressed before consensus on standards is obtained.

3.4 USAGE AND IMPORTANCE OF LOGICAL & PHYSICAL ACCESS CONTROLS

Logical access control

Logical access control should include the following: user ID, password, portable security device such as a smart token, diskette, smart card, smart disk, etc. used in combination with user profiles, electronic delegation matrices, and security software.

Usage

- Ensure the Integrity of the information stored on their computer systems.
- Preserve the Confidentiality of sensitive data.
- Ensure the continued Availability of their information systems.
- Ensure the conformity to laws, regulations and standards.

Physical access controls

Physical access control, include providing a secure area, locked rooms or security device attached to the computer. The need and nature of physical access controls of the various components of the system should be based on threat and risk assessments.Because of the dangers of theft, vandalism and unauthorized use of your systems, you should consider restricting the number of people who have physical access to the area in which your computers are housed. This requirement should be taken into account when premises are being chosen.

Usage

Any access control system is likely to have to handle the following categories of personnel, each of whom will have different access conditions:

- Operators and, sometimes, system users who regularly work within the secure area,
- Engineers and other support staff who require periodic access,
- Others, who require access only rarely.

Importance of Access Controls

Detailed or highly configurable access control is important because it ensures that only authorized users can access your organization's content, protecting against mistakes or risks from unauthorized or unknowledgeable people. Access control usually comes in the form of user log-in, managed by the system administrator. The more detailed or configurable this control is the more secure and useful the content will be. Administrators know the balance between security and productivity is a delicate one. If they put up too many roadblocks in the system, users won't be able to access the content they need when they need it. If they put up too few, the content will be open to risk.

Having access control is important in an educational setting, where various people, including students and teachers, will have access to the same databases. Controls must be in place to authenticate the users, you don’t want students accessing records that are meant for administrators and teachers.

Access control is important to companies that spend hundreds of millions, even billions, developing new products. Compromising security in such environments can lead to lost market advantage, jeopardized product trials, etc

3.5 ACCESS CONTROL DEVICES

We shall discuss some of the most popular access control devices.

Biometrics

Biometrics refers to the science and technology of authentication of persons using automatic verification of personal attributes such as fingers, hands, face, eyes and voice using prints, geometry and pattern recognition. Fears about Internet privacy and fraud, coupled with security changes by National governments and trans-national organization have brought biometrics centre-stage after years of being regarded as a “possibly useful” technology. Also, recent cost improvements in manufacture have made it economical for organizations to deploy biometric devices at points of customer service and admission. Equally, companies and individuals now have the ability to secure Internet access, online purchasing, banking and electronic business with fingerprint readers on the desktop.

Characteristics of Biometrics system

These are the important factors necessary for any effective biometric system:

(1) Accuracy

Accuracy is the most critical characteristic of a biometric identifying verification system. If the system cannot accurately separate authentic persons from impostors, it should not even be termed a biometric identification system.

(2) False Reject Rate

The rate, generally stated as a percentage, at which authentic, enrolled persons are rejected as unidentified or unverified persons by a biometric system is termed the false reject rate. False rejection is sometimes called a Type I error. In access control, if the requirement is to keep the "bad guys" out, false rejection is considered the least important error. In other words FRR is, the percentage of valid subjects that are falsely rejected.

(3) False Accept Rate

The rate, generally stated as a percentage, at which un-enrolled or impostor persons are accepted as authentic, enrolled persons by a biometric system is termed the false accept rate. False acceptance is sometimes called a Type II error. This is usually considered to be the most important error for a biometric access control system. In other words FAR is, the percentage of invalid subjects that are falsely accepted.

(4) Crossover Error Rate (CER)

This is also called the equal error rate and is the point, generally stated as a percentage, at which the false rejection rate and the false acceptance rate are equal. This has become the most important measure of biometric system accuracy.

All biometric systems have sensitivity adjustment capability. If false acceptance is not desired, the system can be set to require (nearly) perfect matches of enrollment data and input data. If tested in this configuration, the system can truthfully be stated to achieve a (near) zero false accept rate. If false rejection is not desired, this system can be readjusted to accept input data that only approximate a match with enrollment data. If tested in this configuration, the system can be truthfully stated to achieve a (near) zero false rejection rate.

However, the reality is that biometric systems can operate on only one sensitivity setting at a time.

(5) Speed and Throughput Rate

The speed and throughput rate are the most important biometric system characteristics. Speed is often related to the data processing capability of the system and is stated as how fast the accept or reject decision is annunciated.

(6) Acceptability to Users

System acceptability to the people who must use it has been a little noticed but increasingly important factor in biometric identification operations. Moreover, management has the final decision on whether the biometric system benefits outweigh its liabilities.

(7) Uniqueness of Biometric Organ and Action

Only three physical characteristics or human organs used for biometric identification are unique: the fingerprint, the retina of the eye (i.e., the blood-vessel pattern inside the back of the eyeball), and the iris of the eye (i.e., random pattern of features in the colored portion of the eye surrounding the pupil). These features include freckles, rings, pits, striations, vasculature, coronas, and crypts.

(8) Resistance to Counterfeiting

The ability to detect or reject counterfeit input data is vital to a biometric access control system meeting high security requirements. Resistance to counterfeit data remains a criterion of high-quality, high-accuracy systems.

(9) Reliability

It is vital that biometric identifying verification systems remain in continuous, accurate operation. These include use of rubber, plastic, or even hands or fingers of the deceased in hand or fingerprint systems, and mimicked or recorded input to voice systems. The system must allow authorized persons access while precluding others, without breakdown or deterioration in performance accuracy or speed. In addition, these performance standards must be sustained without high levels of maintenance or frequent diagnostics and system adjustments.

(10) Data Storage Requirements

Data storage requirements are a far less significant issue today than in the earlier biometric systems when storage media were very expensive. Nevertheless, the size of biometric data files remains a factor of interest. Even with current ultra-high-speed processors, large data files take longer to process than small files, especially in systems that perform full identification, matching the input file against every file in the data base. Biometric file size varies between 9 and 10,000 bytes, with most falling in the 256- to 1,000-byte range.

(11) Enrollment Time

Enrollment time is also a less significant factor today. Early biometric systems sometimes had enrollment procedures requiring many repetitions and several minutes to complete. A system requiring a 5-minute enrollment instead of 2 minutes causes 50 hours of expensive nonproductive time if 1,000 users must be enrolled. Moreover, when line waiting time is considered, the cost increases several times. The accepted standard for enrollment time is 2 minutes per person. Most of the systems in the marketplace today meet this standard.

(12) Intrusiveness of Data Collection

Originally, this factor developed because of user concerns regarding collection of biometric data from inside the body, specifically, the retina inside the eyeball. Early systems illuminated the retina with a red light beam. However, this coincided with increasing public awareness of lasers, sometimes demonstrated as red light beams cutting steel. There has never been an allegation of user injury from retina scanning, but user sensitivity expanded from resistance to red lights intruding inside the body to include any intrusion inside the body. This user sensitivity has now increased to concerns about intrusions into perceived personal space.

(13) Subject and System Contact Requirements

This factor could possibly be considered as a next step or continuation of intrusiveness. Indications are that biometric system users are becoming increasingly sensitive to being required to make firm physical contact with surfaces where up to hundreds of other unknown (to them) persons are required to make contact for biometric data collection. These concerns include voice systems that require holding and speaking into a handset close to the lips.

There seems to be some user feeling that: “if I choose to do something, it is OK, but if an organization, or society, requires me to do the same thing, it is wrong.” Whether or not this makes sense, it is an attitude spreading through society which is having an impact on the use of biometric systems. Systems using video camera data acquisition do not fall into this category.

Smart Cards

Smart cards are usually about the size of a credit card and contain a chip with logic functions and information that can be read at a remote terminal to identify a specific user’s privileges. Smart cards now carry prerecorded, usually encrypted access control information that is compared with data that the user provides (e.g., a personal ID number or biometric data) to verify authorization to access the computer or network.

Smart cards empower people. They facilitate secure access to services and are a vital element in building trust and confidence. Smart cards together with the needed infrastructure, supported by policy and legislation, provide the means to protect the privacy and the confidentiality of Citizens that are of paramount importance for the acceptance of electronic services.

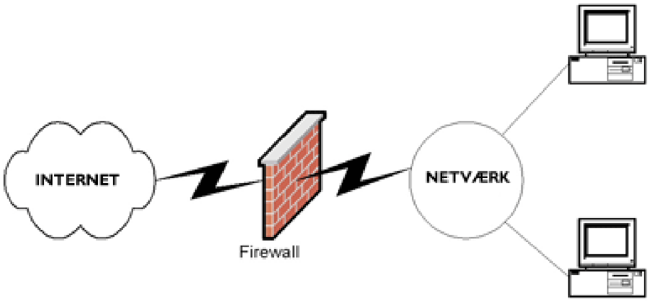
Smart cards offer a secure, private, environment for the storage of information. This information might be non-sensitive information that is merely being stored in a handy, portable, and tamper-resistant device. For example, it is not clear that the level of credit on a phone card is necessarily sensitive information. However we would certainly want the value held securely so that it could not be increased without authorization. By contrast, we might well hold a private cryptographic key in a tamper-resistant device and it would be vital that the value of that key was never revealed.

Used only for its secure storage capabilities, smart cards are restricted to stored-value applications from phone card applications through to the secure storage of credentials. However, when using the secure computing environment that the card provides the range of applications change dramatically from stored-value to electronic purse and from the storage of credentials to dynamic authentication via the use of digital signatures.

Smart cards range from being rather dumb to being surprisingly versatile. The simplest “smart” cards are memory cards providing little, or no, processing power. Older smart cards and legacy deployments might use an 8-bit processor but today 32-bit processors are routinely available.

It is interesting to ask just how important performance really is. At first sight it might appear to be a very important feature of a smart card implementation since the user is waiting for the smart card to do something. However provided an implementation is “fast enough”, even if this is slow by PC standards, then additional performance is just not important. Inserting a card in a reader, moving data to and from the card, waiting for user input and accounting for any other application overheads typically means that any computation costs are mitigated across the total transaction time. Even the most costly cryptographic operation – typically signing with a 1024-bit RSA modulus [30] – generally requires only a fraction of a second. RSA signature verification would require much less time while secret-key operations and hash function evaluations require even less. Of course such rules of thumb are dependent on implementation, processor, and architectural features.

Firewalls



A Firewall notation

A personal firewall ensures that your personal computer is protected from malicious hackers and other intruders while preventing unauthorized access from your computer to a network. In essence, a personal firewall makes your protected computer invisible to the outside world. It also protects your computer by actively looking for hostile intruders and Trojan Horse applications. If an intrusion attempt occurs, the personal firewall detects it in real-time with a built-in host and application based intrusion detection technology, while blocking it by default.

There are two general classes of firewalls: hardware and software. To make matters more confusing, a hardware firewall actually uses software to provide the actual control functionality.

Hardware-based firewalls typically use hardware and software from the same vendor, with hardware and software components tightly integrated.

Why Does My Organization Need a Firewall?

A firewall capable of supporting your organization's most advanced information-protection needs. A highly flexible firewall, can add value to your organization in a number of ways. For example, it can serve as a:

Network perimeter firewall, located between the Internet and your organization's private network.

Departmental LAN firewall, protecting and sectioning off particularly sensitive portions of your internal network.

VPN gateway, connecting your remote-office networks to both the Internet and your main office in a highly secure manner. This role also includes monitoring and tracking the flow of information between networks.

Single Sign On

It is very common for people to shopping on the web, or have the Internet banking. To concern about the security issue, the online vendors often require a client authentication by a username and a password. However, a problem might occur at his point, which is the multiple username and password for different accounts. Users might have different usernames and passwords, sometimes to remember all of that is very difficult, and it's not a good solution to write down the username and password due to the security reason.

An ideal solution for above problem is one user only need single username and password to be authenticated by multiple services. Single sign-on is a way to solve this problem. Single sign-on is the term used to represent a system whereby users need only remember one username and password, and authentication can be provided for multiple services.

Single sign-on is a mechanism to let "users sign onto a site only once and are given access to one or more applications in a single domain or across multiple domains."[1]. It can be illustrated in two different scopes. One is in the client/server relationship; the other is in the e-commerce domain.

In any **client/server** relationship, single sign-on is a session/user **authentication** process that permits a user to enter one name and password in order to access multiple applications. When the session is initiated, the single sign-on will be requested, after pass the authentication, it then will authenticates the user to access to all the partner domains, and eliminates future authentication prompts when the user switches applications during that particular session.

In e-commerce, the single sign-on (SSO) is designed to centralize consumer financial information on one **server** not only for the consumer's convenience, but also to offer increased security by limiting the number of times the consumer enters credit card numbers or other sensitive information used in billing.

3.6 ACCESS CONTROL METHODOLOGIES

Centralized/Remote Authentication Access Controls

RADIUS (Remote Authentication Dial in User Server)

A protocol for carrying authentication, authorization, and configuration information between a Network Access Server, which desires to authenticate its links and a shared Authentication Server. Uses the Client/Server model.

Transactions between the client and the RADIUS server are authenticated through the use of a shared secret, which is never sent of the network.

RADIUS is a security service for authenticating and authorizing dial-up users. A typical enterprise network may have an access server attached to a modem pool, along with a RADIUS server to provide authentication services. Remote users dial into the access server, and the access server sends authentication requests to the RADIUS server. The RADIUS server authenticates users and authorizes access to internal network resources. Remote users are clients to the access server and the access server is a client to the RADIUS server.

RADIUS is an open protocol and is distributed as source code. Because RADIUS is open, it can be adapted to work with third-party security products or proprietary security systems. Any access server that supports the RADIUS client protocol can communicate with a RADIUS server.

RADIUS is often referred to as RADIUS AAA, referring to its authentication, authorization, and accounting functions. "Accounting" refers to the ability of RADIUS to gather information about user sessions that can be processed for billing and network analysis. The basic RADIUS authentication system uses its own user database, but other sources of user information include UNIX password files, Sun's NIS (Network Information Service), and directories that can be accessed via LDAP (Lightweight Directory Access Protocol).

The most important feature of RADIUS is its distributed security model. Basically, the communication server (access server or NAS) is separate from the authentication server. This approach is more scalable and secure. The user account information is stored on a central RADIUS server that can be accessed by any number of access servers. This distributed approach is essential for large ISPs that handle hundreds or thousands of dial-up accounts from multiple access servers.

The RADIUS authentication mechanism works as follows:

(1) Users dial in and establish a PPP connection with a network access server.

(2) The user and the access server then negotiate an authentication mechanism, usually CHAP (Challenge Handshake Authentication Protocol) or EAP (Extensible Authentication Protocol).

(3) The user and the access server exchange authentication information.

(4) The access server then packages the access information into an "authentication request packet," along with information about the access server itself and the port being used. The password is encrypted as a precaution against eavesdroppers, using a secret key shared with the RADIUS server.

(5) The packet is sent to the RADIUS server over whatever connection is in use (LAN, WAN, switch, and so on).

(6) When the RADIUS server receives the authentication request packet, it attempts to validate the user against the account information to which it has access. The RADIUS server then returns either an "Authentication Acknowledgment" or an "Authentication Reject" message to the access server.

If a user is validated and an acknowledgment is sent, additional information about the user may be sent as well, such as link requirements and/or policy information that defines service levels for the user. Filters may also be included to restrict access to parts of the network.

TACACS (Terminal Access Controller Access Control System)

A client/server protocol for handling authentication, authorization, and accounting messages. It uses TCP for reliable connections between clients and servers.

TACACS is a remote authentication protocol that is used to communicate with an authentication server commonly used in UNIX networks. TACACS allows a remote access server to communicate with an authentication server in order to determine if the user has access to the network.

TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon or simply TACACSD. This server was normally a program running on a host. The host would determine whether to accept or deny the request and send a response back. The TIP would then allow access or not, based upon the response. In this way, the process of making the decision is "opened up" and the algorithms and data used to make the decision are under the complete control of whoever is running the TACACS daemon.

A later version of TACACS introduced in 1990 was called XTACACS (extended TACACS). These two versions have generally been replaced by TACACS+ and RADIUS in newer or updated networks. TACACS+ is a completely new protocol and is therefore not compatible with TACACS or XTACACS. TACACS+ is the latest Cisco implementation. It provides attribute control (authorization) and accounting. Authorization can be done on a per-user/per-group basis, and is dynamic.

Decentralized Access Control Administration

A decentralized access control administration method gives control of access to the people closer to the resources—the people who may better understand who should and should not have access to certain files, data, and resources. In this approach, it is often the functional manager who assigns access control rights to employees. An organization may choose to use a decentralized model if its managers have better judgment regarding which users should be able to access different resources, and there is no business requirement that dictates that strict control through a centralized body is necessary. Changes can happen faster through this type of administration because not just one entity is making changes for the whole organization.

However, there is a possibility that conflicts of interest could arise that may not benefit the organization. Because no single entity controls access as a whole, different managers and departments can practice security and access control in different ways. This does not provide uniformity and fairness across the organization. One manager could be too busy with daily tasks and decide that it is easier to let everyone have full control over all the systems in the department. Another department may practice a more strict and detail-oriented method of control by giving employees only the level of permissions needed to fulfill their tasks. Also, certain controls can overlap, in which case actions may not be properly proscribed or restricted.

If Mike is part of the accounting group and recently has been under suspicion for altering personnel account information, the accounting manager may restrict his access to these files to read-only access. However, the accounting manager does not realize that Mike still has full-control access under the network group he is also a member of. This type of administration does not provide methods for consistent control, as a centralized method would.

Another issue that comes up with decentralized administration is lack of proper consistency pertaining to the company's protection. For example, when Sean is fired for looking at pornography on his computer, some of the groups Sean is a member of may not disable his account. So, Sean may still have access after he is terminated, which could cause the company heartache if Sean is vindictive.

3.7 ACCESS CONTROL MODELS

Biba Model

The Biba model is latticed-based and uses the less than or equal to relation. Focuses on Integrity. Biba specifies the three following integrity axioms:

a) **Simple Integrity Axiom** – States that a subject at one level of integrity is not permitted to observe (read) an object of a lower integrity (no read down).

b) **Integrity Axiom (Star)** – States that an object at one level of integrity is not permitted to modify (write to) an object of a higher level of integrity (no write up). For example, if a process can write above its security level, trustworthy data could be contaminated by the addition of less trustworthy data.

c) A subject at one level of integrity cannot invoke a subject at a higher level of integrity.

Clark-Wilson Model

The Clark-Wilson model, published in 1987 and updated in 1989, involves two primary elements for achieving data integrity — the well-formed transaction and separation of duties. Well-formed transactions, as previously mentioned, prevent users from manipulating data, thus ensuring the internal consistency of data. Separation of duties prevents authorized users from making improper modifications, thus preserving the external consistency of data by ensuring that data in the system reflects the real-world data it represents.

The Clark-Wilson model differs from the other models that are subject and object oriented by introducing a third access element — programs — resulting in what is called an access triple, which prevents unauthorized users from modifying data or programs. In addition, this model uses integrity verification and transformation procedures to maintain internal and external consistency of data. The verification procedures confirm that the data conforms to the integrity specifications at the time the verification is performed. The transformation procedures are designed to take the system from one valid state to the next. The Clark-Wilson model is believed to address all three goals of integrity.

Non-Interference Model

This model is related to the information flow model with restrictions on the information flow. The basic principle of this model is that a group of users (A), who are using the commands (C), do not interfere with the user group (B), who are using the commands (D).

State Machine Model

This model captures the state of a systems. A state can change only at discrete points in time, i.e.; triggered by a clock or input event.
How to use state machine models?
Define the state set so that it captures ‘security’
Check that all state transitions starting in a ‘secure’ state yield a ‘secure state’
Check that the initial state of the system is ‘secure’
A state transition is secure if it goes from secure state to a secure state.

Access Matrix Model

Defined as the policy for user authentication, and has several implementations such as access control lists (ACLs) and capabilities. It is used to describe which users have access to what objects.

The matrix consists of four major parts:

- A list of objects
- A list of subjects
- A function T that returns an objects type
- The matrix itself, with objects making the columns and the subjects making the rows.

The two most used implementations are access control lists and capabilities. ACLs are achieved by placing on each object a list of users and their associated rights (Columns). Capabilities are accomplished by storing on each subject a list of rights the subject as for every object (Rows).

Information Flow Model

This model is based on a state machine, and it consists of objects, state transitions, and lattice states. In this context, objects can also represent users. Each object is assigned a security class and value, and information is constrained to flow in the directions that are permitted by the security policy.

CHAPTER 4

APPLICATION SECURITY

4.1 INTRODUCTION

Systems are often developed without security in mind. This omission is primarily because the application programmer is focusing more on trying to learn the domain rather than worrying about how to protect the system. The developer is building prototypes and learning what is needed to satisfy the needs of the users. In these cases, security is usually the last thing he or she needs or wants to worry about. When the time arrives to deploy these systems, it quickly becomes apparent that adding security is much harder than just adding a password protected login screen.

Applications and computer systems are usually developed for functionality first, not security first. To get the best of both worlds, security and functionality would have to be designed and developed at the same time. Security should be interwoven into the core of a product and provide protection at different layers; this is a better approach than trying to develop a front end or wrapper that may reduce the overall functionality and leave security holes when the product has to be integrated with other applications. Application system controls come in various flavors with many different goals. They can control input, processing, number-crunching methods, interprocess communication, interfacing to the system and other programs, access, and output. They should be developed with the potential risks in mind, and many types of threat models and risk analyses should be invoked at different stages of development. The goal is to prevent security compromises and to reduce the vulnerabilities and the possibility of data corruption. The controls can be preventive, detective, or corrective. They can come in the form of administrative and physical controls, but are usually more technical in this context.

The specific application controls depend upon the application itself, its objectives, the security goals of the developers, and the environment the application will be placed in. If an application is purely proprietary and will run only in closed, trusted environments, fewer security controls may be needed than those required for applications that will connect businesses over the Internet and provide financial transactions. The trick is to understand the security needs of an application, implement the right controls and mechanisms, thoroughly test the mechanisms and how they integrate into the application, follow structured development methodologies, and provide secure and reliable distribution methods. This can be harder than it sounds.

Application and device security

Today, many security efforts look to solve security problems through devices such as firewalls, intrusion detection systems (IDSs), sensors, and vulnerability scanners. This reliance on devices occurs because networks and how they are thought of work on a basic outside and inside notion. The bad people and potential threats are on the outside, and what needs to be protected is on the inside.

This notion has worked, to an extent, because networks were closed environments, which usually meant controlled environments. However, our environments then incorporated electronic data interchange (EDI), remote dial-in capabilities, Internet sites, and virtual private networks (VPNs). Now environments are incorporating wireless communication, instant messaging, and business-to-business (B2B) capabilities, which add complexity to the concept of us and them and inside and outside. The division between software security and device security deals with providing security at the beginning stages of software development versus providing devices (firewalls, routers, ACLs, IDS, bastion hosts) that protect the perimeters of networks.

The perimeter devices try to prevent attackers from exploiting the security holes that reside in the software. Firewalls and IDSs are studied and talked about within circles of security much more than inadvertent flaws in design and poorly written software. In reality, the flaws within the software cause a majority of the vulnerabilities in the first place.

Several reasons explain why perimeter devices are more often considered than software development for security:

(i) In the past, it was not crucial to implement security during the software development stages; thus, many programmers do not practice these procedures.

(ii) Many security professionals are not software developers.

(iii) Many software developers do not have security as a main focus.

(iv) Software vendors are trying to rush their products to market with their eyes set on functionality, not security.

(v) The computing community is used to receiving software with bugs and applying patches.

Finger pointing and quick judgments are neither useful nor necessarily fair at this stage of our computing evolution. Twenty years ago, mainframes had tight security because only a handful of people knew how to run them, users worked on computers (dumb terminals) that could not introduce malicious code to the mainframe, and environments were closed. The core protocols and framework were developed at a time when threats and attacks were not prevalent. There was no need for such stringent security. Then computer and software evolution took off, and the possibilities splintered into a thousand different directions. The high demand for computer technology and different types of software increased the demand for programmers, system designers, administrators, and engineers. This demand brought in a wave of people who had little experience. The lack of experience, the high change rate of technolo gy, and the race to market add problems to security that are not always clearly understood. Although it is easy to blame the big software vendors in the sky for producing flawed or buggy software, this is driven by customer demand. Understanding how security works within programs, how programs integrate into environments, and how compromises take place will cause consumers to demand more security-oriented software and better programming and development practices. This requires a shift from reactive to proactive actions toward security problems to ensure that they do not happen in the first place, or at least happen to a smaller extent.

4.2 SECURITY IN DATABASES

Data base security is primarily concerned with the secrecy of data. Secrecy means protecting a data base from unauthorized access by users and software applications. Secrecy, in the context of data base security, includes a variety of threats incurred through unauthorized access. These threats range from the intentional theft or destruction of data to the acquisition of information through more subtle measures, such as inference.

There are three generally accepted categories of secrecy-related problems in data base systems:

(i) **The improper release of information from reading data that was intentionally or accidentally accessed by unauthorized users**.

Securing data bases from unauthorized access is more difficult than controlling access to files managed by operating systems. This problem arises from the finer granularity that is used by data bases when handling files, attributes, and values. This type of problem also includes the violations to secrecy that result from the problem of inference, which is the deduction of unauthorized information from the observation of authorized information. Inference is one of the most difficult factors to control in any attempts to secure data. Because the information in a data base is semantically related, it is possible to determine the value of an attribute without accessing it directly. Inference problems are most serious in statistical data bases where users can trace back information on individual entities from the statistical aggregated data.

(ii) **The improper modification of data**

This threat includes violations of the security of data through mishandling and modifications by unauthorized users. These violations can result from errors, viruses, sabotage, or failures in the data that arise from access by unauthorized users.

(iii) **Denial-of-service threats**

Actions that could prevent users from using system resources or accessing data are among the most serious. This threat has been demonstrated to a significant degree recently with the SYN flooding attacks against network service providers.

Discretionary vs. Mandatory Access Control Policies

Both traditional relational data base management system (RDBMS) security models and OO data base models make use of two general types of access control policies to protect the information in multilevel systems. The first of these policies is the discretionary policy. In the discretionary access control (DAC) policy, access is restricted based on the authorizations granted to the user.

The mandatory access control (MAC) policy secures information by assigning sensitivity levels, or labels, to data entities. MAC policies are generally more secure than DAC policies and they are used in systems in which security is critical, such as military applications. However, the price that is usually paid for this tightened security is reduced performance of the data base management system. Most MAC policies also incorporate DAC measures as well.

Relational DBMS Security

The principal methods of security in traditional RDBMSs are through the appropriate use and manipulation of views and the structured query language (SQL) GRANT and REVOKE statements. These measures are reasonably effective because of their mathematical foundation in relational algebra and relational calculus.

View-Based Access Control

Views allow the data base to be conceptually divided into pieces in ways that allow sensitive data to be hidden from unauthorized users. In the relational model, views provide a powerful mechanism for specifying data-dependent authorizations for data retrieval. Although the individual user who creates a view is the owner and is entitled to drop the view, he or she may not be authorized to execute all privileges on it. The authorizations that the owner may exercise depend on the view semantics and on the authorizations that the owner is allowed to implement on the tables directly accessed by the view. For the owner to exercise a specific authorization on a view that he or she creates, the owner must possess the same authorization on all tables that the view uses. The privileges the owner possesses on the view are determined at the time of view definition. Each privilege the owner possesses on the tables is defined for the view. If, later on, the owner receives additional privileges on the tables used by the view, these additional privileges will not be passed onto the view. In order to use the new privileges within a view, the owner will need to create a new view.

The biggest problem with view-based mandatory access controls is that it is impractical to verify that the software performs the view interpretation and processing. If the correct authorizations are to be assured, the system must contain some type of mechanism to verify the classification of the sensitivity of the information in the data base. The classification must be done automatically, and the software that handles the classification must be trusted. However, any trusted software for the automatic classification process would be extremely complex. Furthermore, attempting to use a query language such as SQL to specify classifications quickly becomes convoluted and complex. Even when the complexity of the classification scheme is overcome, the view can do nothing more than limit what the user sees it cannot restrict the operations that may be performed on the views.

GRANT and REVOKE Privileges

GRANT and REVOKE statements allow users to selectively and dynamically grant privileges to other users and subsequently revoke them if necessary. These two statements are considered to be the principal user interfaces in the authorization subsystem. There is, however, a security-related problem inherent in the use of the GRANT statement. If a user is granted rights without the GRANT option, he or she should not be able to pass GRANT authority on to other users. However, the system can be subverted by a user by simply making a complete copy of the relation. Because the user creating the copy is now the owner, he or she can provide GRANT authority to other users. As a result, unauthorized users are able to access the same information that had been contained in the original relation. Although this copy is not updated with the original relation, the user making the copy could continue making similar copies of the relation, and continue to provide the same data to other users.

The REVOKE statement functions similarly to the GRANT statement, with the opposite result. One of the characteristics of the use of the REVOKE statement is that it has a cascading effect. When the rights previously granted to a user are subsequently revoked, all similar rights are revoked for all users who may have been provided access by the originator.

Other Relational Security Mechanisms

Although views and GRANT/ REVOKE statements are the most frequently used security measures in traditional RDBMSs, they are not the only mechanisms included in most security systems using the relational model. Another security method used with traditional relational data base managers, which is similar to GRANT/REVOKE statements, is the use of query modification.

This method involves modifying a user's query before the information is retrieved, based on the authorities granted to the user. Although query modification is not incorporated within SQL, the concept is supported by the Cobb-Date relational data base model.

Most relational data base management systems also rely on the security measures present in the operating system of the host computer. Traditional RDMBSs such as DB2 work closely with the operating system to ensure that the data base security system is not circumvented by permitting access to data through the operating system. However, many operating systems provide insufficient security. In addition, because of the portability of many newer data base packages, the security of the operating system should not be assumed to be adequate for the protection of the wealth of information in a data base.

Object-Oriented DBMS Characteristics

Unlike traditional RDBMSs, secure OODBMSs have certain characteristics that make them unique. Furthermore, only a limited number of security models have been designed specifically for OO data bases. The proposed security models make use of the concepts of encapsulation, inheritance, information hiding, methods, and the ability to model real-world entities that are present in OO environments.

The object-oriented data base model also permits the classification of an object's sensitivity through the use of class (of entities) and instance. When an instance of a class is created, the object can automatically inherit the level of sensitivity of the superclass. Although the ability to pass classifications through inheritance is possible in object-oriented data bases, class instances are usually classified at a higher level within the object's class hierarchy. This prevents a flow control problem, where information passes from higher to lower classification levels.

OODBMSs also use unique characteristics that allow these models to control the access to the data in the data base. They incorporate features such as flexible data structure, inheritance, and late binding. Access control models for

OODBMSs must be consistent with such features. Users can define methods, some of which are open for other users as public methods. Moreover, the OODBMS may encapsulate a series of basic access commands into a method and make it public for users, while keeping basic commands themselves away from users.

Proposed OODBMS Security Models

Currently only a few models use discretionary access control measures in secure object-oriented data base management systems.

Explicit Authorizations

The ORION authorization model permits access to data on the basis of explicit authorizations provided to each group of users. These authorizations are classified as positive authorizations because they specifically allow a user access to an object. Similarly, a negative authorization is used to specifically deny a user access to an object.

The placement of an individual into one or more groups is based on the role that the individual plays in the organization. In addition to the positive authorizations that are provided to users within each group, there are a variety of implicit authorizations that may be granted based on the relationships between subjects and access modes.

Data-Hiding Model

A similar discretionary access control secure model is the data-hiding model proposed by Dr. Elisa Bertino of the Universita' di Genova. This model distinguishes between public methods and private methods.

The data-hiding model is based on authorizations for users to execute methods on objects. The authorizations specify which methods the user is authorized to invoke. Authorizations can only be granted to users on public methods. However, the fact that a user can access a method does not automatically mean that the user can execute all actions associated with the method. As a result, several access controls may need to be performed during the execution, and all of the authorizations for the different accesses must exist if the user is to complete the processing.

Similar to the use of GRANT statements in traditional relational data base management systems, the creator of an object is able to grant authorizations to the object to different users. The “creator” is also able to revoke the authorizations from users in a manner similar to REVOKE statements. However, unlike traditional RDBMS GRANT statements, the data-hiding model includes the notion of protection mode. When authorizations are provided to users in the protection mode, the authorizations actually checked by the system are those of the creator and not the individual executing the method. As a result, the creator is able to grant a user access to a method without granting the user the authorizations for the methods called by the original method. In other words, the creator can provide a user access to specific data without being forced to give the user complete access to all related information in the object.

Other DAC Models for OODBMS Security

Rafiul Ahad has proposed a similar model that is based on the control of function evaluations. Authorizations are provided to groups or individual users to execute specific methods. The focus in Ahad’s model is to protect the system by restricting access to the methods in the data base, not the objects. The model uses proxy functions, specific functions, and guard functions to restrict the execution of certain methods by users and enforce content-dependent authorizations.

Another secure model that uses authorizations to execute methods has been presented by **Joel Richardson**. This model has some similarity to the data-hiding model’s use of GRANT/REVOKE-type statements. The creator of an object can specify which users may execute the methods within the object.

A final authorization-dependent model emerging from OODBMS security research has been proposed by **Dr. Eduardo B. Fernandez** of Florida Atlantic University. In this model the authorizations are divided into positive and negative authorizations. The Fernandez model also permits the creation of new authorizations from those originally specified by the user through the use of the semantic relationships in the data.

Dr. Naftaly H. Minsky of Rutgers University has developed a model that limits unrestricted access to objects through the use of a view mechanism similar to that used in traditional relational systems data base management systems. Minsky’s concept is to provide multiple interfaces to the objects within the data base. The model includes a list of laws, or rules, that govern the access constraints to the objects. The laws within the data base specify which actions must be taken by the system when a message is sent from one object to another. The system may allow the message to continue unaltered, block the sending of the message, send the message to another object, or send a different message to the intended object.

Although the discretionary access control models do provide varying levels of security for the information within the data base, none of the DAC models effectively addresses the problem of the authorizations provided to users. A higher level of protection within a secure OO data base model is provided through the use of mandatory access control.

MAC Methods for OODBMS Security

Dr. Bhavani Thuraisingham of MITRE Corp. proposed in 1989 a mandatory security policy called SORION. This model extends the ORION model to encompass mandatory access control. The model specifies subjects, objects, and access modes within the system, and it assigns security/sensitivity levels to each entity. Certain properties regulate the assignment of the sensitivity levels to each of the subjects, objects, and access modes. In order to gain access to the instance variables and methods in the objects, certain properties that are based on the various sensitivity levels must be satisfied.

A similar approach has been proposed in the **Millen-Lunt model**. This model, developed by Jonathan K. Millen of MITRE Corp. and Teresa Lunt of SRI/DARPA (Defense Advanced Research Projects Agency), also uses the assignment of sensitivity levels to the objects, subjects, and access modes within the data base. In the Millen-Lunt model, the properties that regulate the access to the information are specified as axioms within the model. This model further attempts to classify information according to three different cases:

(i) The data itself is classified
(ii) The existence of the data is classified
(iii) The reason for classifying the information is also classified

These three classifications broadly cover the specifics of the items to be secured within the data base; however, the classification method also greatly increases the complexity of the system.

The SODA Model

Dr. Thomas F. Keefe of Pennsylvania State University proposes a model called Secure Object-Oriented Data Base (SODA). The SODA model was one of the first models to address the specific concepts in the OO paradigm. It is often used as a standard example of secure object-oriented models from which other models are compared.

The SODA model complies with MAC properties and is executed in a multilevel security system. SODA assigns classification levels to the data through the use of inheritance. However, multiple inheritance is not supported in the SODA model.

Similar to other secure models, SODA assigns security levels to subjects in the system and sensitivity levels to objects. The security classifications of subjects are checked against the sensitivity level of the information before access is allowed.

Polyinstantiation

Unlike many current secure object-oriented models, SODA allows the use of polyinstantiation as a solution to the multiparty update conflict. This problem arises when users with different security levels attempt to use the same information. The variety of clearances and sensitivities in a secure data base system result in conflicts between the objects that can be accessed and modified by the users. Through the use of polyinstantiation, information is located in more than one location, usually with different security levels. Obviously, the more sensitive information is omitted from the instances with lower security levels. Although polyinstantiation solves the multiparty update conflict problem, it raises a potentially greater problem in the form of ensuring the integrity of the data within the data base. Without some method of simultaneously updating all occurrences of the data in the data base, the integrity of the information quickly disappears. In essence, the system becomes a collection of several distinct data base systems, each with its own data.

Conclusion

The move to object-oriented DBMSs is likely to continue for the foreseeable future. Because of the increasing need for security in distributed processing environments, the expanded selection of tools available for securing information in this environment should be used fully to ensure that the data are as secure as possible. In addition, with the continuing dependence on distributed data the security of these systems must be fully integrated into existing and future network security policies and procedures.

The techniques that are ultimately used to secure commercial OODBMS implementations will depend in large part on the approaches promoted by the leading data base vendors. However, the applied research that has been conducted to date is also laying the groundwork for the security components that will in turn be incorporated in the commercial OODBMSs.

4.3 SYSTEM DEVELOPMENT

Security is most effective if it is planned and managed throughout the life cycle of a system or application, versus applying a third-party package as a front end at the end after the development. Many security risks, analyses, and events occur during a product’s lifetime, and these issues should be dealt with from the initial planning stage and continue through the design, coding, implementation, and operational stages. If security is added at the end of a project development rather than at each step of the life cycle, the cost and time of adding security increases dramatically. Security should not be looked at as a short sprint, but should be seen as a long run with many hills and obstacles. Many developers, programmers, and architects know that adding security at a later phase of the system's life cycle is much more expensive and complicated than integrating it into the planning and design phase. Different security components can affect many different aspects of a system, and if they are thrown in at the last moment, they will surely affect other mechanisms negatively, restrict some already developed functionality, and cause the system to perform in unusual and unexpected ways. This approach costs more money because of the number of times the developers have to go back to the drawing board, recode completed work, and rethink different aspects of the system's architecture.

The security plan and project management activities may likely be audited so that security-related decisions can be understood. When assurance in the system needs to be guaranteed, indicating that security was fully considered in each phase of the life cycle, the procedures, development, decisions, and activities that took place during the project will be reviewed. The documentation must accurately reflect how the system or product was built and how it operates once implemented into an environment.

Life-Cycle Phases

Several types of models are used for system and application development, which include varying life cycles. Each model basically accomplishes the same thing; the main difference is how the development and lifetime of a system is broken into sections.
The different models integrate the following phases in one fashion or another:

(1) Project initiation
(2) Functional design analysis and planning
(3) System design specifications
(4) Software development
(5) Installation/implementation
(6) Operational/maintenance
(7) Disposal

Security is not listed as an individual bullet point because it should be embedded throughout all phases.

(1) Project Initiation

This is the phase when everyone involved attempts to understand why the project is needed and what the scope of the project entails. Either a specific customer needs a new system or application or a demand for the product exists in the market. During this phase, the project management team examines the characteristics of the system and proposed functionality, brainstorming sessions take place, and obvious restrictions are reviewed. In this phase, the user needs are identified and basic security objectives of the product are acknowledged. An initial risk analysis should be initiated that evaluates threats and vulnerabilities to estimate the cost/benefit ratios of the different security countermeasures. Issues pertaining to security integrity, confidentiality, and availability need to be addressed. A basic security framework is designed for the project to follow, and risk management processes are established.

(2) Functional Design Analysis and Planning

In this phase, a project plan is developed by the software architectures to define the security activities and to create security checkpoints to ensure that quality assurance for security controls takes place and that the configuration and change control process is identified. At this point in the project, resources are identified, test schedules start to form, and evaluation criteria are developed to be able to properly test the security controls. A formal functional baseline is formed, meaning the expectations of the product are outlined in a formal manner, usually through documentation. A test plan is developed, which will be updated through each phase to ensure that all issues are properly tested. Security requirements can be derived from several different sources:

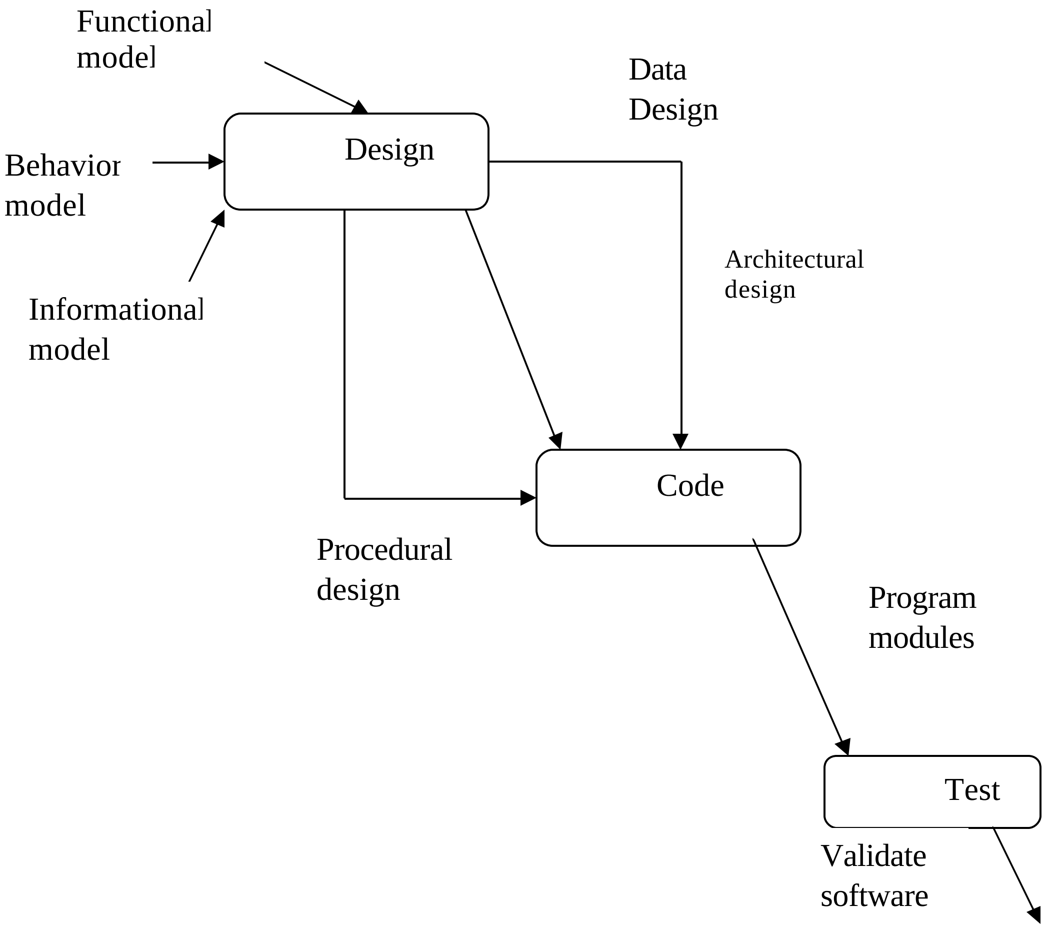
(i) Functional needs of the system or application
(ii) National, international, or organizational standards and guidelines
(iii) Export restrictions
(iv) Sensitivity level of data being processed (militarily strategic data versus
private-sector data)
(v) Relevant security policies
(vi) Cost/benefit analysis results
(vii) Required level of assurance to achieve the targeted security level rating

(3) System Design Specifications

Software requirements come from three models:

(1) Informational model: Dictates the type of information to be processed and
how it will be processed
(2) Functional model: Outlines the tasks and functions that the application needs to carry out
(3) Behavioral model: Explains the states that the application will be in during and after specific transitions take place

The informational, functional, and behavioral model data goes into the software design as requirements. What comes out of the design is the data, architectural, and procedural design, as shown in Figure below:



(4) Software Development

This is the phase where the programmers and developers become deeply involved. They are usually involved up to this point for their direction and advice, but at this phase, it is basically put into their laps. Let the programming and testing begin. This is the stage where the programmers should code in a way that does not permit software compromises. Among other issues to address, the programmers need to check input lengths so buffer overflows cannot take place, code to prevent the presence of covert channels, check for proper data types, make sure checkpoints cannot be bypassed by users, verify syntax, and perform checksums. Different attack scenarios should be played out to see how the code could be attacked or modified in an unauthorized fashion. Debugging and code reviews should be carried out by peer developers, and everything should be clearly documented.

(5) Installation / Implementation

The implementation stage focuses on how to use and operate the developed system or application. At this phase, the customer has purchased the developed product and installed it into its environment. The product would then be configured for the right level of protection. Functionality and performance tests should be performed, and the results should be analyzed and compared with the company's security requirements. The configurations should be documented by the vendor and supplied with product for the customer to use. User guides and operation and maintenance manuals are developed so that users know how to properly use the systems and the technical staff know how to properly configure the product if needed. Security activities need to be monitored to ensure that the system or application performs in the manner promised by the service level agreement. Once management is sure of the security provided by the new system and understands and accepts the risk, it should issue a formal accreditation statement. Auditing needs to be enabled and monitored, and contingency recovery plans and procedures should be developed and tested to make sure the system and product react as planned in the event of a system failure or emergency situation.

(6) Operational and Maintenance

Security is important during the operational phase than during earlier phases. The initial part of this phase includes configuring the new system and inserting it properly into the network and environment. Many times, security controls are not enabled or properly configured for the environment, so even if they were correctly coded from the beginning, it does not really matter if they are not actually used or are used in an unintended way. Operational assurance is carried out by continually conducting vulnerability tests, monitoring activities, and auditing events. It is through operational assurance activities that an administrator learns of new vulnerabilities or security compromises, so that the proper actions can take place. If major changes happen to the system, product, or environment, a new risk analysis may need to be performed along with a new certification and accreditation process. These major changes could include adding new systems and/or new applications, relocating the facility, or changing data sensitivity or criticality.

(7) Disposal

When it is time for "out with the old and in with the new," certain steps may need to take place to make sure this transition happens in a secure manner. Depending on the sensitivity level of the data held on a system, various disposal activities may be necessary. Information may need to be archived, backed up to another system, discarded, or destroyed. If the data is sensitive and needs to be destroyed, it may need to be purged by overwriting, degaussing, or physically destroying the media. It depends on the data and the company's policy about destroying sensitive information. If the product that is being replaced is just a word processor or an antivirus software package, this phase can be easily taken care of. But if the software is integrated into every part of the company's processing infrastructure, properly extracting it without affecting productivity and security can be an overwhelming task.

Software Development Methods

There are several different life-cycle models that outline the significant phases of software development. The following list provides a quick glimpse at some of these different models:

(1) **Waterfall**: A classical method that uses discrete phases of development that requires formal reviews and documentation before moving into the next phase of the project.

(2) **Spiral**: A method that builds upon the waterfall method with an emphasis on risk analysis, prototypes, and simulations at different phases of the development cycle.

(3) **Joint Analysis Development (JAD)**: A method that uses a team approach in application development in a workshop-oriented environment.

(4) **Rapid Application Development (RAD):** A method of determining user requirements and developing systems quickly to satisfy immediate needs.

(5) **Cleanroom:** An approach that attempts to prevent errors or mistakes by following structured and formal methods of developing and testing. This approach is used for high-quality and critical applications that will be put through a strict certification process.

4.4 BASIC CONCEPTS OF SECURITY IN CLIENT-SERVER ARCHITECTURE

Client/Server computing is a style of computing involving multiple processors, one of which is typically a workstation and across which a single business transaction is completed. Client/Server computing recognizes that business users, and not a mainframe, are the center of a business. Therefore, Client/Server is also called "client-centric" computing. Today, Client/Server computing is extended to the Internet - netcentric computing (network centric computing), the concepts of business users have expanded greatly.

The characteristics of Client/Server computing includes:

(i) There are multiple processors.

(ii) A complete business transaction is processed across multiple servers

Netcentric computing - as an evolution of Client/Server model, has brought new technology to the forefront, especially in the area of external presence and access, ease of distribution, and media capabilities.

Architectures for Client/Server System

Both traditional Client/Server as well as netcentric computing are tiered architectures. In both cases, there is a distribution of presentation services, application code, and data across clients and servers. In both cases, there is a networking protocol that is used for communication between clients and servers. In both cases, they support a style of computing where processes on different machines communicate using messages. In this style, the "client" delegates business functions or other tasks (such as data manipulation logic) to one or more server processes. Server processes respond to messages from clients.

A Client/Server system has several layers, which can be visualized in either a conceptual or a physical manner. Viewed conceptually, the layers are presentation, process, and database. Viewed physically, the layers are server, client, middleware, and network.

Client/Server 2-tiered architecture

2-tiered architecture is also known as the client-centric model, which implements a "fat" client. Nearly all of the processing happens on the client, and client accesses the database directly rather than through any middleware. In this model, all of the presentation logic and the business logic are implemented as processes on the client. 2-tiered architecture is the simplest one to implement.

Modified 2-tiered architecture

Because of the nightmare of maintenance of the 2-tiered Client/Server architecture, the business logic is moved to the database side, implemented using triggers and procedures. This kind of model is known as modified 2-tiered architecture.

3-tiered architecture

For 3-tiered architecture, the application is divided into a presentation tier, a middle tier, and a data tier. The middle tier is composed of one or more application servers distributed across one or more physical machines. This architecture is also termed the “the thin client—fat server” approach.

More on Client-Server model

Today, a network administrator is in an overwhelming position of having to integrate different applications and computer systems to keep up with her company’s demand on expandable functionality and the new gee-whiz components that executives buy into and demand quick implementation of. This integration is further frustrated by the company’s race to provide a well-known presence on the Internet by implementing web sites with the capabilities of taking online orders, storing credit card information, and setting up extranets with partners. This can quickly turn into a confusing ball of protocols, devices, interfaces, incompatibility issues, routing and switching techniques, telecommunications routines, and management procedures. It could make an administrator choose to buy some land in Montana and raise goats instead.

On top of this, security is expected, required, and depended upon. When security compromises creep in, the finger pointing starts, liability issues are tossed like hot potatoes, and people might even lose their jobs. An understanding of the environment, what is currently in it, and how it works is required so that the new technologies can be implemented in a more controlled and comprehendible fashion.

The days of developing a simple web page and posting it on the Internet to sell candles are long gone. Today, customer front-end, complex middleware, and three tiered architectures must be developed and work seamlessly. As the complexity of this type of environment grows, tracking down errors and security compromises becomes an awesome task.
Basically, the client/server architecture enables an application system to be divided across multiple platforms that vary in operating systems and hardware. The client requests services and the server fulfills these requests. The server handles the data-processing services and provides the processed result to the client. The client performs the front-end portion of an application, and the server performs the back-end portion, which is usually more labor intensive.

The front end usually includes the user interface and local data-manipulation capabilities, and provides the communications mechanisms that can request services from the server portion of the application.

Security in Client-Server Architecture

For internet-based Client/Server systems, security testing for the web server is important. The web server is your LAN's window to the world and, conversely, is the world's window to your LAN. It's a maxim in system security circles that buggy software opens up security holes. It's a maxim in software development circles that large, complex programs contain bugs. Unfortunately, web servers are large, complex programs that can contain security holes. Furthermore, the open architecture of web server allows arbitrary CGI scripts to be executed on the server's side of the connection in response to remote requests. Any CGI script installed at your site may contain bugs, and every such bug is a potential security hole.

Three types of security risks have been identified.

(i) The primary risk is errors in the web server side misconfiguration that would allow remote users to:

   a. Steal confidential information
   b. Execute commands on the server host, thus allowing the users to modify the system
   c. Gain information about the server host that would allow them to break into the system
   d. Launch attacks that will bring the system down.

(ii) The secondary risk occurs on the Browser-side

   a. Active content that crashes the browser, damages your system, breaches your company's privacy, or creates an annoyance.
   b. The misuse of personal information provided by the end user.

(iii) The tertiary risk is data interception during data transfer.

The above risks are also the focuses of web server security.

4.5 BASIC CONCEPTS OF WEB APPLICATION SECURITY

Why does web application security matter?

With a rapid development and deployment of web-based applications, the implications with regard to the security of customers' databases and networks must clearly be taken into account. It is still quite often heard from managers that there is no reason to invest more in security since the company is protected by a great firewall and the web application uses SSL. For sure, firewalls are great tools and help a lot to secure your applications. But they are only one element of the security chain. They protect the network. They filter network traffic. But they do not help to detect if an intrusion occurred and they can also be bypassed. Just like in a house, security involves more than locking doors: usually, there is an alarm system and a fire-resistant safe for example. Computer security is not different. You need a firewall to protect your network. But, you also need (among others), ways to detect intrusions (the alarm system), protection around the computer and around the application running on that computer (the safe).

On the one hand, firewalls can prevent hackers from accessing machines or services (programs running on a machine) without authorization. But, by definition, a web application must be accessible from the internet. Otherwise, nobody can use the application. Usually, system administrators restrict network access to a minimum, allowing only web traffic (http) to the web server through the http port 80. When hackers encounter such a configuration, they do not have much choice. They can only use the http protocol to connect to your site, so they must use http. They only have access to your web server, so they can try to find weaknesses in your web server configuration or in the web server itself if it is not properly patched. They only have access to the applications running on the web server, so they can try to exploit weaknesses in the application. There are potential weaknesses in web applications. Since hackers usually have no other choice, exploiting web applications vulnerabilities becomes more and more popular. This is the primary reason why investing in protecting web applications is important. On the other hand, SSL is a protocol that encrypts the communication between the browser and the web server. When using SSL, somebody able to listen to the communication between the client (the browser) and the server cannot understand the dialog because the channel is encrypted. But, on each end of channel, the information must be decrypted and is stored in clear at some point in time. It is therefore possible for a user of the client machine to edit specific data before it is sent to the server. There are ways to attack unprotected web applications using some technique. SSL does not help to prevent such attacks.

It is very important to consider web application security because the firewall does not help. By definition, http traffic must be allowed to go through the firewall. Otherwise no web application is possible. SSL does not help either. People don't usually think about securing web applications. Usually web sites are protected by well configured firewalls and attacking your web application might be one of the only ways for a hacker to get in.

Overview of problems

Data manipulation

Data is passed between the browser and the server either in the URL itself, in hidden fields contained in forms or in cookies. Since URLs and hidden fields values are hard-coded in the HTML source code, they are very easy to modify. An attacker simply uses the "display source" option of the browser and modifies the source. Modifying cookies is a bit more complex but still feasible. There are two types of cookies: persistent and non persistent. Persistent cookies are stored on disk and can be easily modified. Non persistent cookies are stored in memory only. This makes them a little harder to modify but there are tools available. This technique is called Data Manipulation.

SQL Query manipulation

This method consists of injecting SQL queries into database systems. The following is an example. Imagine a web form allowing you to change your password. Usually the form contains 4 fields: your userid (let's name the field uid), your old password (oldpwd), the new password (newpwd), and a “confirm new password” field (newpwdconfirm). The application will check that newpwd and newpwdconfirm are identical, that your old password is correct and then issue a query to the database to update your password. The query looks like:

(the ‘$INPUT[fieldname]’ syntax is used to represent the value entered in the html form ‘fieldname’ field).

Update usertable set pwd=’$input[newpwd]’ where uid=’$input[uid]’;

Everything works fine if the user follows the rules and inputs his or her uid. What if, the user sends the following value in the uid field: “myuid' or uid=’administrator”?

The query really sent to the database will be: Update usertable set pwd=’newpassword]’ where uid=’myuid' or uid='administrator’; Yes, the administrator password has been reset with the user password. If you are not quite sure of the exact uid of the administrator account, you can try the following value uid=“myuid' or uid like ‘%admin%”, resetting the password of all accounts containing the string admin. This kind of technique is known as SQL query manipulation.

Buffer overflows

A buffer overflow occurs when the size of data received from the client is larger than the size of the buffer where the data must be stored. Data is than copied outside the border of the buffer. That extra data may contain malicious code or may crash the system. Some developers try to prevent the user from entering long strings in a HTML form field by setting the “maxlength” parameter of the form field. But of course, since this information is contained in the HTML source code, it can be changed too. There is absolutely no guarantee that the value of the field sent to the server will not be longer than expected.

Session hijacking

Before understanding the principles behind session hijacking, let us understand what a session is and why we need it. HTTP is a stateless protocol. Every time you ask for a page, or for a graphic within a page, a new connection is set up between your browser and the web server. There is no relationship at all between one connection and another. There is no state. The second connection does not know anything about what took place during the first connection. Though, this is perfectly acceptable when using the web to search for information, it is not appropriate for a web application where a context needs to be transmitted from page to page. For example, an e-commerce site, on the page where you enter your credit card number to complete the transaction, needs to know exactly the items that you have chosen on previous pages in order to compute the total amount. The e-commerce site needs a mechanism that identifies a “session”, a virtual “established connection” between a browser and a web server to pass a context from page to page. Technically, this is done as follows: when the browser connects to the web server for the first time, the user has not been authenticated yet. The web server asks for credentials and generates a unique identifier (the session ID). The server can associate a context to each session ID, storing any kind of information in that context. The generated session ID is sent back to the browser. For every subsequent call to the server, the browser sends the session ID to the server. The server can then use the context associated with the transmitted session ID and “remember” data from page to page.

The system is working fine but there are risks associated with the technique. Since all you need to get access to the application is a valid session ID, one must make sure that it is not possible to guess a session ID or to steal a valid one. The process of stealing a session ID is called “session hijacking”. Once a hacker has successfully obtained access to a legitimate user’s session, "he or she can perform all normal application functions with the same privileges of the legitimate user". Web sites have been vulnerable to this kind of attack because "while it is generally clear that username/password pairs are indeed authentication data and therefore sensitive, it is not generally understood that these session IDs are also just as sensitive".

Cross Site Scripting

Web browsers can execute client-side languages like JavaScript, VBScript. A script could potentially access local data and transmit it to a third party. Typically, session IDs stored in cookies can be obtained with that technique. This is not really a web application problem. It is more a client browser problem. But since the technique could be used to hijack sessions, it is worth mentioning. Discussion groups or news lists give the possibility to directly input HTML into the messages. To exploit the vulnerability described in the previous paragraph, a hacker simply posts a message containing the malicious script in a discussion group. Anyone reading the message will run the script. It is worth mentioning that more and more engines (like Yahoo for example) now filter the input and replace the malicious commands with harmless text.

Summary

We learnt several methods to attack web applications while perfectly respecting the http protocol, making firewalls and intrusion detection systems unable to detect the attacks. Usually, the methods described in this topic are entry points to the system. For example, a very small hole can widen and lead to a fully compromised system. The most important points to remember from the topic are:

For developers

(i) The way you program your application has a tremendous influence on the overall security.
(ii) Always strongly validate any information coming from the client
(iii) Make sure your session mechanism is bullet-proof.
(iv) Use an appropriate authentication mechanism.

For system administrators

(i) Apply all best practices regarding network and host security.
(ii) Run the application under accounts with the fewest possible privileges.
(iii) Separate services as much as possible.

For managers

(i) Plan for security from the very beginning of the project.
(ii) Make sure developers and system administrators work hand in hand.

The Open Web Application Security Project (OWASP)

The Open Web Application Security Project (OWASP) is dedicated to helping organizations understand and improve the security of their web applications and web services. This list was created to focus corporations and government agencies on the most serious of these vulnerabilities. Web application security has become a hot topic as companies race to make content and services accessible though the web. At the same time, hackers are turning their attention to the common weaknesses created by application developers.

The OWASP Top Ten is a list of vulnerabilities that require immediate remediation. Existing code should be checked for these vulnerabilities immediately, as these flaws are being actively targeted by attackers. Development projects should address these vulnerabilities in their requirements documents and design, build, and test their applications to ensure that they have not been introduced. Project managers should include time and budget for application security activities including developer training, application security policy development, security mechanism design and development, penetration testing, and security code review.

Authentication and session management includes all aspects of handling user authentication and managing active sessions. Authentication is a critical aspect of this process, but even solid authentication mechanisms can be undermined by flawed credential management functions, including password change, forgot my password, remember my password, account update, and other related functions. Because “walk by” attacks are likely for many web applications, all account management functions should require reauthentication even if the user has a valid session id.

The Top Ten List[1]

The following is a short summary of the most significant web application security vulnerabilities. Each of these is described in more detail in the following sections.

Top Vulnerabilities in Web Applications		
A1	**Unvalidated Input**	Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.

[1] From www.owasp.org

A2	**Broken Access Control**	Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.
A3	**Broken Authentication and Session Management**	Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.
A4	**Cross Site Scripting (XSS) Flaws**	The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
A5	**Buffer Overflows**	Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and web application server components.
A6	**Injection Flaws**	Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application.
A7	**Improper Error Handling**	Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.

A8	**Insecure Storage**	Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.
A9	**Denial of Service**	Attackers can consume web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.
A10	**Insecure Configuration Management**	Having a strong server configuration standard is critical to a secure web application. These servers have many configuration options that affect security and are not secure out of the box.

CHAPTER 5

COMMUNICATIONS AND OPERATIONS MANAGEMENT

5.1 COMMUNICATIONS SECURITY

Introduction

Telecommunications and networking use various mechanisms, devices, software, and protocols that are interrelated and integrated. Networking is one of the more complex topics in the computer field, mainly because so many technologies and concepts are involved. A network administrator or engineer must know how to configure networking software, protocols and services, and devices; deal with interoperability issues; install, configure, and interface with telecommunications software and devices; and troubleshoot effectively.

A security professional must understand these issues and be able to analyze them a few levels deeper to recognize fully where vulnerabilities can arise within networks. This can be an overwhelming and challenging task. However, if you are someone who enjoys challenges and appreciates the intricacies of technology, then maintaining security and networking infrastructures may be more fun than work.

To secure a network architecture, you must understand the various networking platforms involved, network devices, and how data flows through a network. You must understand how various protocols work, their purposes, their interactions with other protocols, how they may provide exploitable vulnerabilities, and how to choose and implement the appropriate types of protocols in a given environment. You must also understand the different types of firewalls, routers, switches, and bridges, when one is more appropriate than the other, where they are to be placed, their interactions with other devices, and the degree of security each provides. There are many different types of devices, protocols, and security mechanisms within an environment provide different functionality, but they also provide a layered approach to security. Layers within security are important, so that if an attacker is able to bypass one layer, another layer stands in the way to protect the internal network. Many networks have routers, firewalls, intrusion detection systems (IDSs), antivirus software, and more. Each specializes in a certain piece of security, but they all should work in concert to provide a layered approach to security.

Telecommunications is the electrical transmission of data among systems, whether through analog, digital, or wireless transmission types. The data can flow across copper wires, coaxial cable, fiber, or airwaves, the telephone company's public-switched telephone network (PSTN), or a service provider's fiber cables, switches, and routers.

LAN Devices

Several types of devices are used in LANs, MANs, and WANs to provide intercommunication between computers and networks. The use of these devices varies according to their functionality, capabilities, intelligence, and network placement. The following devices are used in networking: Repeaters, Bridges, Routers, Switches, etc
From security point of few we will talk about devices used in implementing security.

Firewalls

Firewalls are used to restrict access to one network from another network. Most companies use firewalls to restrict access to their networks from the Internet. They may also use firewalls to restrict one internal network segment from accessing another internal segment. For example, if the network administrator wants to make sure that employees cannot access the Research and Development network, he would place a firewall between this network and all other networks and configure the firewall to allow only the type of traffic he deems acceptable.

A firewall device supports and enforces the company's network security policy. An organizational security policy provides high-level instructions on acceptable and un- acceptable actions as they pertain to security. The firewall has a more defined and granular security policy that dictates what services are allowed to be accessed, what IP addresses and ranges are to be restricted, and what ports can be accessed. The firewall is described as a "choke point" in the network, because all communication should flow through it, and this is where traffic is inspected and restricted.

Many times, companies set up firewalls to construct a **demilitarized zone (DMZ)**, which is a network segment that is located between the protected and the unprotected networks. The DMZ provides a buffer zone between the dangerous Internet and the goodies within the internal network that the company is trying to protect. Two firewalls are usually installed to form the DMZ. The DMZ usually contains web, mail, and DNS servers, which must be hardened systems because they would be the first in line for attacks. Many

DMZs also have an IDS sensor that listens for malicious and suspicious behavior.

The types of firewalls we will review are:
(1) Packet filtering
(2) Stateful
(3) Proxy
(4) Dynamic packet filtering
(5) Kernel proxy

We will then dive into the three main firewall architectures, which are:
(i) Screened host
(ii) Dual-home
() Screened subnet

Types of firewalls

(1) Packet Filtering Firewalls

Packet filtering is a security method of controlling what data can flow into and out of a network. Packet filtering takes place by using ACLs, which are developed and applied to a device. ACLs are lines of text, called rules, that the device applies to each packet that it receives. The lines of text provide specific information pertaining to what packets can be accepted and what packets must be denied. Packet filtering is the method used by the first-generation firewall—that is, it is the first type that was created and used, and other types that were developed subsequently fall into later generations.

Pros and Cons of Packet Filtering
Pros:
(i) Scaleable
(ii) Provides high performance
(iii) Application independent
Cons:
(i) Does not look into the packet past the header information
(ii) Low security relative to other options
(iii) Does not keep track of the state of a connection

(2) Stateful Firewalls

When packet filtering is used, a packet arrives at the router, and the router runs through its ACLs to determine whether this packet should be allowed or denied. If the packet is allowed, it is passed on to the destination host, or to another router, and the router forgets about the packet. This is different from stateful inspection filtering, which remembers and keeps track of what packets went where until each particular connection is closed.

A stateful inspection firewall is nosier than a regular filtering device, because it keeps track of what computers say to each other. This requires that the firewall maintain a **state table**, which is like a score sheet of who said what to whom. Stateful inspection firewalls also make decisions on what packets to allow or disallow, but their functionality goes a step further. Because the state table has information about a previous request for these packets, the firewall allows the packets to pass through. Regular packet filtering compares incoming packets to rules defined in the firewall's ACLs. When a stateful inspection firewall receives a packet, it first looks in its state table to see whether a connection has already been established and whether this data was requested. If there was no previous connection and the state table holds no information about the packet, the packet is compared to the device's ACLs. If the ACL allows this type of traffic, the packet is allowed to access the network. If that type of traffic is not allowed, the packet is dropped.

Most stateful inspection firewalls work at the network and transport layers. It depends upon the product, but many times when a connection begins, the firewall investigates all layers of the packet (all headers, payload, and trailers). Once the initial packets go through this in-depth inspection, the firewall then just reviews the network and transport header portions for the rest of the session. Scaling down the inspection in this manner is done to increase performance. Although stateful inspection provides an extra step of protection, it also adds more complexity because this device must now keep a dynamic state table and remember connections. Stateful inspection firewalls unfortunately have been the victims of many types of denial-of-service (DoS) attacks. Several types of attacks are aimed at flooding the state table with bogus information. The state table is a resource, similar to a system's hard drive space, memory, and CPU. When the state table is stuffed full of bogus information, the device may either freeze or reboot. In addition, if this firewall has to be rebooted for some reason, it will lose its information on all recent connections; thus, it may deny legitimate packets.

(3) Proxy Firewalls

A **proxy** is a middleman. A proxy intercepts and inspects messages before delivering them to the intended recipients. Suppose you need to give a box and a message to the president of the United States; you could not just walk up to the president and hand over these items. Instead, you would have to go through a middleman, likely the secret service, who would accept the box and message and thoroughly inspect the box to en-sure that nothing dangerous was inside. This is what a proxy firewall does—it accepts messages either entering or leaving a network, inspects them for malicious information, and, when it decides the messages are okay, passes the data on to the destination computer. Proxy firewalls are second-generation firewalls.

Pros and Cons of Proxy Firewalls

Pros:

(i) Looks at the information within a packet, possibly all the way up to the application layer.

(ii) Provides better security than packet filtering.

(iii) Breaks the connection between trusted and untrusted systems.

Cons:

(i) Some proxy firewalls support only a limited number of applications.

(ii) Degrades traffic performance.

(iii) Application-based proxy firewalls may have scalability and performance issues.

(iv) Breaks client/server model, which is good for security but sometimes bad for functionality.

Two types of proxy firewalls can be used—application-level and circuit-level.

Proxy Firewall Characteristics

Application-level proxy firewall:

a. Different proxy required for each service allowed

b. Provides more intricate control than circuit-level proxy firewalls

c. Requires more processing per packet and thus is slower than a circuitlevel proxy firewall

Circuit-level proxy firewall:

a. Does not require a proxy for each and every service

b. Does not provide the detailed access control that an application-level proxy firewall provides

c. Provides security for a wider range of protocols

(4) Dynamic Packet Filtering

When an internal system needs to communicate to an entity outside of its trusted network, it has to choose a source port so that the receiving system knows how to respond properly. The receiving system requires an IP address and a port number so that its response can properly find its way to the sender's computer. Ports up to 1023 are called well-known ports and are reserved for server-side services. The sender must choose a dynamic port higher than 1023 when it sets up a connection with another entity. The dynamic packet-filtering firewall then creates an ACL that allows the external entity to communicate with the internal system via this high port. If this were not an available option for your dynamic packet-filtering firewall, you would have to allow "punch holes" in your firewalls for all ports above 1023, because the client side chooses these ports dynamically and the firewall would never know exactly on which port to allow or disallow traffic.

An internal system could choose a source port of 11,111 for its message to the outside system. This frame goes to the dynamic packet-filtering firewall and builds an ACL, that indicates that a response from the destination computer to this internal system's IP address and port 11,111 is to be allowed. When the destination system sends a response, the firewall allows it. These ACLs are dynamic in nature, so once the connection is finished (either an FIN or RST packet is received), the ACL is removed from the list. On connectionless protocols, such as UDP, the connection times out and then the ACL is pulled. The benefit of a dynamic packet-filtering firewall, which is a fourth-generation firewall, is that it gives you the option of allowing any type of traffic outbound and allowing only response traffic inbound.

(5) Kernel Proxy Firewalls

A K**ernel Proxy Firewall** is considered a fifth-generation firewall. It differs from all the previously discussed firewall technologies because it creates dynamic, customized TCP/IP stacks when a packet needs to be evaluated. When a packet arrives at a kernel proxy firewall, a new virtual network stack is created, which is made up of only the protocol proxies that are necessary to examine this specific packet properly. If it is an FTP packet, only the FTP proxy is loaded in the stack.

The packet is scrutinized at every layer of the stack, not just at the data payload. This means the data link header will be evaluated along with the network header, transport header, session layer information, and the application layer data. If anything is deemed unsafe at any one of these layers, the packet is discarded.

Kernel proxy firewalls are faster than application layer proxy firewalls because all of the inspection and processing takes place in the kernel and does not need to be passed up to a higher software layer in the operating system. It is still a proxy-based system, so the connection between the internal and external entity is broken by the proxy acting as a middleman, and it can perform NAT by changing the source address, as do the preceding proxy-based firewalls.

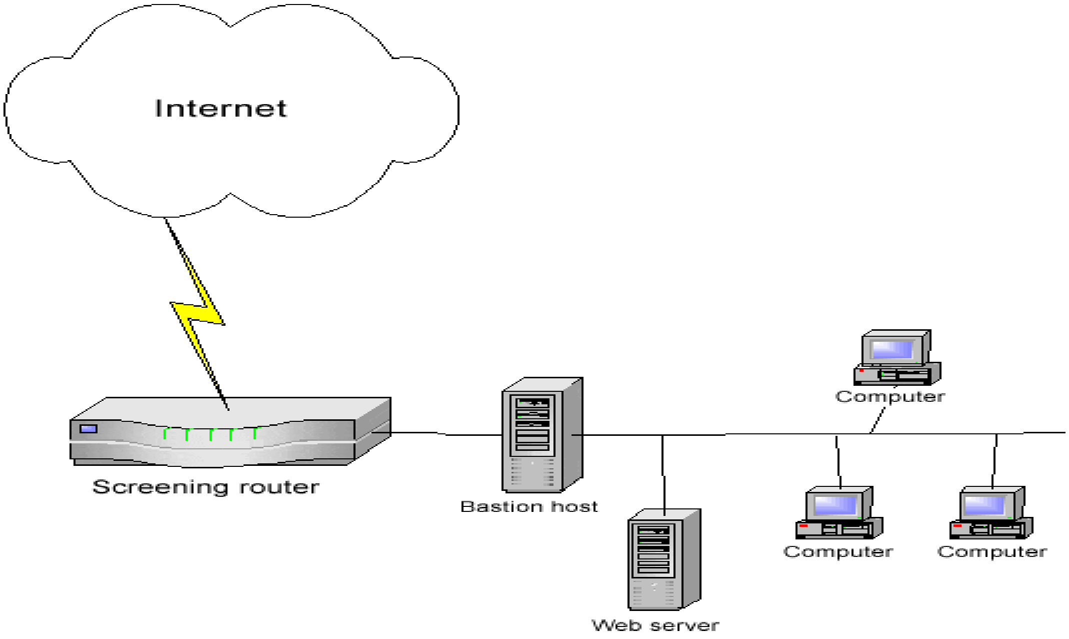
Differences between Firewalls

Firewall Type	**OSI Layer**	**Characteristics**
Packet filtering	Network layer	Looks at destination and source addresses, ports, and services requested. Routers using ACLs dictate acceptable access to a network.
Application level proxy	Application layer	Looks deep into packets and makes granular access
Circuit-level proxy	Network layer	Looks only at the header packet information. It protects a wider range of protocols and services than does an application-level proxy, but does not provide the detailed level of control available to an application-level proxy.
Stateful	Network layer	Looks at the state and context of packets. Keeps track of each conversation using a state table.
Kernel proxy	Application layer	Faster because processing is done in the kernel. One network stack is created for each packet.

Firewall architectures

(i) Bastion Host

Bastion host is just another name for a locked-down (or hardened) system. A bastion host is usually a highly exposed device, because it is the front line in a network's security and its existence is known on the Internet. This means that the device must be extremely secure—no unnecessary services should be running, unused subsystems must be disabled, vulnerabilities must be patched, unnecessary user accounts must be disabled, and ports that are not needed must be closed. A bastion host is not tied to firewall software and activities; it is just a system that is properly locked down. Any system that resides within the DMZ should be installed on a bastion host since it is closer to the Internet and most likely closer to those who would like to do it harm. If firewall software is not installed on a locked-down operating system, or bastion host, the firewall is vulnerable.



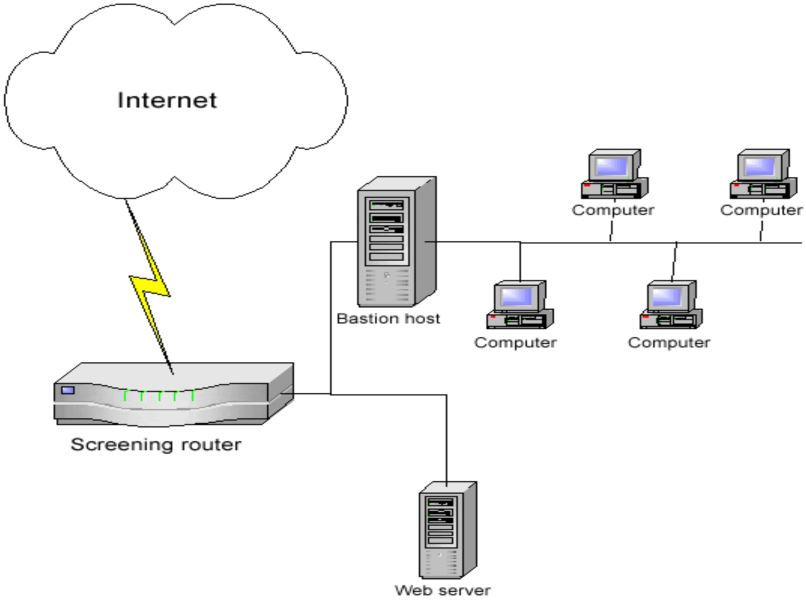
Bastion Host Architecture[2]

(ii) Dual-Homed Firewall

Dual-homed refers to a device that has two interfaces: one facing the external network and the other facing the internal network. If firewall software is installed on a dual-homed device, and it usually is, the underlining operating system should have packet forwarding and routing turned off, for security reasons. If they are enabled, the computer will not apply the necessary ACLs, rules, or other restrictions required of a firewall. When a packet comes to the external NIC from the untrusted network on a dual-homed firewall, and the operating system has forwarding enabled, the operating system will forward the traffic instead of passing it up to the firewall software for inspection.

[2] Pcture from www.techrepublic.com.

Many network devices today are multihomed, which just means that they have several NICs that are used to connect several different networks. Multihomed devices are commonly used to house firewall software, since the job of a firewall is to control the traffic as it goes from one network to another. A common multihomed firewall architecture allows a company to have several DMZs. One DMZ may hold devices that are shared between companies in an extranet, another DMZ may house the company's DNS and mail servers, and yet another DMZ may hold the company's web servers. Different DMZs are used for two reasons: to control the different traffic types and to ensure that if one system on one DMZ is compromised, the other systems in the rest of the DMZs are not accessible to this attacker.



Dual-Homed Firewall[3]

[3] techrepublic.com

(iii) Screened Host

A screened host is a firewall that is screened by a router[4]

A **screened host** is a firewall that communicates directly with a perimeter router and the internal network. Traffic that is received from the Internet is first filtered via packet filtering on the outer router. The traffic that makes it past this phase is sent to the screened-host firewall, which applies more rules to the traffic and drops the denied packets. Then the traffic moves to the internal destination hosts. The screened host (the firewall) is the only device that receives traffic directly from the router. No traffic goes directly from the Internet, through the router, and to the internal network. The screened host is always part of this equation.

If the firewall is an application-based system, protection is provided at the network layer by the router and at the application layer by the proxy. This arrangement offers a high degree of security, because for an attacker to be successful, she would have to compromise two systems.

[4] All in one CISSP by Shon Harris

Screening means, the router is a screening device and the firewall is the screened host. This just means that there is a layer that scans the traffic and gets rid of a lot of the "junk" before it is directed toward the firewall. A screened host is different from a screened subnet, which is described next.

(iv) Screened Subnet

When using a screened subnet, two firewalls are used to create a DMZ[5]

A screened-subnet architecture adds another layer of security to the screened-host architecture. It applies packet filtering to data entering the network and ports the traffic to the firewall. However, instead of the firewall then redirecting the traffic to the internal network, an interior router also filters the traffic. The use of these two physical firewalls creates a DMZ. In an environment with only a screened host, if an attacker successfully breaks through the firewall, nothing lies in her way to prevent her from having full access to the internal network. In an environment using a screened subnet, the attacker would have to hack through another router (or firewall) to gain access. In this layered approach to security, the more layers provided, the better the protection.

The screened-subnet approach provides more protection than a stand-alone firewall or a screened-host firewall because three devices are working together

[5] All in one CISSP by Shon Harris

and all three devices must be compromised before an attacker can gain access to the internal network. This architecture also sets up a DMZ between the two routers, which functions as a small network isolated among the trusted internal and untrusted external networks.

The internal users usually have limited access to the servers within this area. Web, email, and other public servers often are placed within the DMZ. Although this solution provides the highest security, it also is the most complex. Configuration and maintenance can prove to be difficult in this setup, and when new services need to be added, three systems may need to be reconfigured instead of just one. The complexity and configuration of the DMZ, perimeter network, and screened hosts and subnets are dictated by the company security policy. The required level of security, and the services that need to be available to internal and external users, should be clearly outlined in this policy.

Disadvantages of firewalls

(i) Most of the time a distributed approach needs to be used to control all network access points, which cannot usually happen through the use of just one firewall.
(ii) Firewalls can present a potential bottleneck to the flow of traffic.
(iii) Firewalls can restrict desirable services that users may want to access (this is a disadvantage to the users, but an advantage to the security professional).
(iv) Most firewalls do not provide protection from viruses being downloaded or passed through e-mail, and hooks to virus-detection techniques are needed.
(v) Border firewalls provide little protection against the inside attacker.
(vi) Firewalls do not protect against rogue modems in listening mode.
(vii) Firewalls do not protect against rogue wireless APs.

Honeypot

A honeypot system is a computer that usually sits in the screened subnet, or DMZ, and attempts to lure attackers to it instead of to actual production computers. To make a honeypot system lure attackers, administrators may enable services and ports that are popular to exploit. However, the administrator must be careful to ensure that this box is isolated in such a way that, when it is attacked, the hacker is not successful at accessing other computers on the network. Some honeypot systems have services emulated, meaning the actual service is not running but software that acts like those services is available.

Virtual Private Network (VPN)

A virtual private network (VPN) is a secure, private connection through a public network or an otherwise unsecure environment. It is a private connection because the encryption and tunneling protocols are used to ensure the confidentiality and integrity of the data in transit. It is important to remember that VPN technology requires a tunnel to work and it assumes encryption. The protocols that can be used for VPNs are Point-to-Point Tunneling Protocol (PPTP), IPSec, and L2TP. The sending and receiving ends must have the necessary hardware and software to set up an encrypted tunnel, which provides the private link. The tunneling encryption protocol that is used encrypts the data and protects it as it travels through the untrusted public network, usually the Internet. Remote users, or road warriors, can use VPNs to connect to their company network to access their e-mail, network resources, and corporate assets. A remote user must have the necessary software loaded on his computer to use a VPN. The user first makes a PPP connection to an ISP, and the ISP makes a full connection for the user to the destination network. PPP encapsulates datagrams to be properly transmitted over a telecommunication link. Once this connection has been made, the user's software initiates a VPN connection with the destination network. Because data exchanged between the two entities will be encrypted, the two entities go through a handshaking phase to agree upon the type of encryption that will be used and the key that will be employed to encrypt their data. The ISP is involved with the creation of the PPP connection, which is a type of foundation for the VPN connection. Once the PPP connection is set up, the ISP is out of the picture and the VPN parameters are negotiated and decided upon by the user and the destination network. After this is complete, the user and network can then communicate securely through their newly created virtual connection. VPN connections can be used not only by remote users to access a network but also to provide a connection between two routers (many times called a gateway-to-gateway connection) or two users. It is a flexible connection, and the only requirements are that each entity must have a connection, VPN software, the necessary protocols, and the same encryption mechanisms. Once the VPN connection is made, the user can access network resources in the same manner that he can access them via dial-up connections.

Up to this point, we have been discussing a VPN that exists over dial-up and Internet connections; but a VPN can also take place between firewalls that have VPN functionality. Within a network, the VPN device sits on the outer edge of the security domain. When a company implements a firewall that has VPN functionality embedded, the company can centralize administration for the VPN and firewall. In this type of configuration, packets that enter the network can come in encrypted through the VPN connection and must be decrypted to allow the firewall to inspect the packets and either allow or deny them. Because extra work is being done on the packets as they enter and leave a network, much more overhead is generated, which causes degradation in performance. However, today most of the processing that takes place is being moved to hardware and integrated circuits, which can work at much faster speeds than pure software.

Tunneling Protocols

VPNs use tunneling protocols. A tunnel is a virtual path across a network that delivers packets that are encapsulated and possibly encrypted. Encapsulation and encryption sound alike, but they describe two different reasons a tunnel would be used in the first place. If one network uses NetBIOS Enhanced User Interface (NetBEUI) and needs to be connected to another network that also uses NetBEUI, but they are two states apart, NetBEUI is nonroutable. So for these two networks to communicate, the NetBEUI packets must be encapsulated within a routable protocol, such as IP. This type of encapsulation happens all the time on the Internet and between networks. When an Ethernet network is connected to an FDDI backbone, that FDDI network does not understand the Ethernet frame format; thus, the packets must be encapsulated within the FDDI protocol when they are sent over the FDDI network. If two networks use IPX and need to communicate across the Internet, these messages must also be encapsulated in a protocol that the Internet can understand, such as IP. The second variation to a tunnel is one that uses encapsulation and encryption. The encapsulation reasons stay the same, and the encryption is used to protect the data's confidentiality and integrity as it travels through untrusted environments. These are both ways of tunneling through another network. Tunneling is the main ingredient to a VPN because that is how the VPN creates its private connection.

Three main tunneling protocols are used in VPN connections: PPTP, L2TP, and IPSec.

(i) Internet Protocol Security (IPSec)

The Internet Protocol Security (IPSec) protocol suite provides a method of setting up a secure channel for protected data exchange between two devices. The devices that share this secure channel can be two servers, two routers, a workstation and a server, or two gateways between different networks. IPSec is a widely accepted standard for providing network layer protection. It can be more flexible and less expensive than end-to-end and link encryption methods. IPSec has strong encryption and authentication methods, it is used to establish virtual private networks (VPNs) among networks across the Internet.

IPSec is not a strict protocol that dictates the type of algorithm, keys, and authentication method to use; rather, it is an open, modular framework that provides a lot of flexibility for companies when they choose to use this type of technology. IPSec uses two basic security protocols: **Authentication Header (AH)** and **Encapsulating Security Payload (ESP)**. AH is the authenticating protocol, and ESP is an authenticating and encrypting protocol that uses cryptographic mechanisms to provide source authentication, confidentiality, and message integrity.

IPSec can work in one of two modes: **transport mode**, in which the payload of the message is protected, and **tunnel mode**, in which the payload and the routing and header information are protected. ESP in transport mode encrypts the actual message information so that it cannot be sniffed and uncovered by an unauthorized entity.

Tunnel mode provides a higher level of protection by also protecting the header and trailer data that an attacker may find useful. Each device will have at least one **security association (SA)** for each VPN it uses. The SA, which is critical to the IPSec architecture, is a record of the configurations the device needs to support an IPSec connection. When two devices complete their handshaking process, which means that they have agreed upon a long list of parameters they will use to communicate, this data must be recorded and stored somewhere, which is in the SA. The SA can contain the authentication and encryption keys, the agreed-upon algorithms, key lifetime, and the source IP address. When a device receives a packet via the IPSec protocol, it is the SA that tells the device what to do with the packet. So if device B receives a packet from device C via IPSec, device B will look to the corresponding SA to tell it how to decrypt the packet, how to properly authenticate the source of the packet, which key to use, and how to reply to the message if necessary.

IPSec can authenticate the sending devices of the packet by using MAC. The ESP protocol can provide authentication, integrity, and confidentiality if the devices are configured for this type of functionality. So if a company just needs to make sure it knows the source of the sender and needs to be assured of the integrity of the packets, it would choose to use AH. If the company would like to use these services and also have confidentiality, then it would use the ESP protocol because it provides encryption functionality. In most cases, the reason that ESP is employed is that the company needs to set up a secure VPN connection. IPSec is very complex with all of its components and possible configurations. This complexity is what provides for a great degree of flexibility, because a company has many different configuration choices to achieve just the right level of protection.

(ii) Point-to-Point Protocol

Point-to-Point Protocol *(PPP)* is not really a tunneling protocol, but an encapsulation protocol. It does not need to wrap up current frames with special headers and trailers, which will be taken off at the destination. Instead it allows TCP/IP traffic to be transmitted over a medium that was developed for telephone voice data. PPP is used to encapsulate messages and transmit them over a serial line. Therefore, it allows TCP/IP and other protocols to be carried across telecommunication lines. PPP is used to establish telecommunication connections between routers, user-to-router, and user-to-user. It is also used to establish an Internet connection between a computer and an Internet point of presence (PoP)—usually a bank of modems and access servers at an ISP location. The user dials into this PoP over a telecommunications line and communicates using PPP.

PPP has, for the most part, replaced **Serial Line Internet Protocol (SLIP)**, an older protocol that was used to encapsulate data to be sent over serial connection links. PPP has several capabilities that SLIP does not have:

(i) Implements header and data compression for efficiency and better use of bandwidth

(ii) Has error correction

(iii) Supports different authentication methods

(iv) Can encapsulate protocols other than just IP

(v) Does not require both ends to have an IP address assigned before data transfer can occur.

(iii) PPTP

PPTP, a Microsoft protocol, allows remote users to set up a PPP connection to a local ISP and then create a secure VPN to their destination. PPTP has been the de facto industry-standard tunneling protocol for years, but the new de facto standard for VPNs is IPSec. Although tunneling does not by default mean that the user's data is encrypted, in most implementations tunneling and encryption are both used. When using PPTP, the PPP payload is encrypted with Microsoft Point-to-Point Encryption (MPPE) using MSCHAP or EAP-TLS. The keys used in encrypting this data are generated during the authentication process between the user and the authentication server.

Along with encryption, the frame has to be encapsulated as well. A series of encapsulations takes place in this technology. The user's data is encapsulated within PPP, and then this frame is encapsulated by PPTP with a Generic Routing Encapsulation (GRE) header and IP header. This encapsulation allows the resulting frame to be routable over public networks, such as the Internet. One limitation of PPTP is that it can work only over IP networks, so other protocols must be used to move data over frame relay, X.25, and ATM links. Cisco started to develop a protocol, Layer 2 Forwarding (L2F), that would tunnel PPP traffic through these other types of networks, but it was asked by the IETF to combine its work with PPTP for the sake of interoperability. As a result, Cisco developed Layer 2 Tunneling Protocol (L2TP), which combines the best of PPTP and L2F.

(iv) L2TP

L2TP provides the functionality of PPTP, but it can work over networks other than just IP, and it provides a higher level of security when combined with IPSec. L2TP does not provide any encryption or authentication services, so it needs to be combined with IPSec if those services are required. The processes that L2TP uses for encapsulation are similar to those used by PPTP. The PPP frame is encapsulated with L2TP. When the destination system receives the L2TP frame, it processes the headers. Once it gets to the IPSec trailer, it verifies the integrity and authentication of the frame. Then it uses the information in the ESP header to decrypt the rest of the headers and data payload properly.

The following items outline the differences between PPTP and L2TP:

(i) PPTP can run only on top of IP networks. It is dependent on IP. L2TP, on the other hand, can run on top and tunnel through networks that use other protocols, such as frame relay, X.25, and ATM.
(ii) PPTP is an encryption protocol and L2TP is not; thus, L2TP lacks the security to be called a true VPN solution. L2TP is often used in conjunction with IPSec to provide the necessary encryption.
(iii) L2TP supports TACACS+ and RADIUS, and PPTP does not.

Authentication Protocols

(i) Password Authentication Protocol (PAP)

PAP is used by remote users to authenticate over PPP lines. It provides identification and authentication of the user who is attempting to access a network from a remote system. This protocol requires a user to enter a password before being authenticated. The password and the username credentials are sent over the network to the authentication server after a connection has been established via PPP. The authentication server has a database of user credentials that are compared to the supplied credentials to authenticate users.

PAP is one of the least secure authentication methods, because the credentials are sent in cleartext, which renders them easy to capture by network sniffers. Although it is not recommended, some systems revert to PAP if they cannot agree on any other authentication protocol. During the handshake process of a connection, the two entities negotiate how authentication is going to take place, what connection parameters to use, the speed of data flow, and other factors. Both entities will try to negotiate and agree upon the most secure method of authentication; they may start with EAP, and if one computer does not have EAP capabilities, they will try to agree upon CHAP; if one of the computers does not have CHAP capabilities, they may be forced to use PAP. If this type of authentication is unacceptable, the administrator will configure the RAS to accept only CHAP authentication and higher, and PAP cannot be used at all.

(ii) Challenge Handshake Authentication Protocol (CHAP)

Challenge Handshake Authentication Protocol (CHAP) addresses some of the vulnerabilities found in PAP. It uses a challenge/response mechanism to authenticate the user instead of sending a password. When a user wants to establish a PPP connection and both ends have agreed that CHAP will be used for authentication purposes, the user's computer sends the authentication server a logon request. The server sends the user a challenge, which is a random value. This challenge is encrypted with the use of a predefined password as an encryption key, and the encrypted challenge value is returned to the server. The authentication server also uses the predefined password as an encryption key and decrypts the challenge value, comparing it to the original value that was sent. If the two results are the same, the authentication server deduces that the user must have entered the correct password, and authentication is granted.

(iii) Extensible Authentication Protocol (EAP)

Extensible Authentication Protocol (EAP) is also supported by PPP. Actually, EAP is not a specific authentication mechanism as are PAP and CHAP; instead, it provides a framework to enable many types of authentication techniques to be used during PPP connections. As the name states, it extends the authentication possibilities from the norm (PAP and CHAP) to other methods such as one-time passwords, token cards, biometrics, Kerberos, and future mechanisms. So when a user dials into an authentication server and both have EAP capabilities, they can negotiate between a longer list of possible authentication methods.

Internet Security

The Internet is the collection of physical devices and communication protocols used to transverse these web sites and interact with them. The web sites look the way they look because the creator used a language that dictates the look, feel, and functionality of the page. Web browsers enable users to read web pages by enabling them to request and accept web pages via HTTP, and the user's browser converts the language (HTML, DHTML, and XML) into a format that can be viewed on the monitor. The browser is the user's window to the World Wide Web. Browsers can understand a variety of protocols and have the capability to process many types of commands, but they do not understand them all. Let's go through many of the technologies and protocols that make up the World Wide Web.

(i) HTTP

TCP/IP is the protocol suite of the Internet, and HTTP is the protocol of the Web. HTTP sits on top of TCP/IP. When a user clicks his mouse on a link within a web page, his browser uses HTTP to send a request to the web server hosting that web site. The web server finds the corresponding file to that link and sends it to the user via HTTP. The TCP protocol controls the handshaking and maintains the connection between the user and the server, and the IP protocol makes sure that the file is routed properly throughout the Internet to get from the web server to the user. So, the IP protocol finds the way to get from A to Z, TCP makes sure that the origin and destination are correct and that no packets are lost along the way, and, upon arrival at the destination, HTTP presents the payload, which is a web page. HTTP is a stateless protocol, which means the client and web server make and break a connection for each operation. When a user requests to view a web page, that web server finds the requested web page, presents it to the user, and then terminates the connection. If the user requests a link within the newly received web page, a new connection has to be set up, the request goes to the web server, and the web server sends the requested item and breaks the connection. The web server never remembers the users that ask for different web pages, because otherwise the web server would use and commit a lot of resources.

(ii) HTTP Secure

HTTP Secure (HTTPS) is HTTP running over SSL. HTTP works at the application layer and SSL works at the transport layer. Secure Sockets Layer (SSL) uses public key encryption and provides data encryption, server authentication, message integrity, and optional client authentication. When a client accesses a web site, that web site may have both secured and public portions. The secured portion would require the user to be authenticated in some fashion. When the client goes from a public page on the web site to a secured page, the web server will start the necessary tasks to invoke SSL and protect this type of communication. The server sends a message back to the client, indicating that a secure session needs to be established, and the client in response sends its security parameters. The server compares those security parameters to its own until it finds a match. This is the handshaking phase. The server authenticates to the client by sending it a digital certificate, and if the client decides to trust the server, the process continues. The server can require the client to send over a digital certificate for mutual authentication, but that is rare. The client generates a session key and encrypts it with the server's public key. This encrypted key is sent to the web server, and they both use this symmetric key to encrypt the data they send back and forth. This is how the secure channel is established. SSL keeps the communication path open until one of the parties requests to end the session. The session is usually ended when the client sends the server a FIN packet, which is an indication to close out the channel.

SSL requires an SSL-enabled server and browser. SSL provides security for the connection but does not provide security for the data once it is received. This means that the data is encrypted while it is being transmitted, but not after it is received by a computer. So if a user sends bank account information to a financial institution via a connection protected by SSL, that communication path is protected, but the user must trust the financial institution that receives this information, because at this point, SSL's job is done. The user can verify that a connection is secure by looking at the URL to see that it includes https://. The user can also check for a padlock or key icon, depending on the browser type, at the bottom corner of the browser window. In the protocol stack, SSL lies beneath the application layer and above the network layer. This ensures that SSL is not limited to specific application protocols and can still use the communication transport standards of the Internet.

(iii) Secure HTTP

Secure HTTP (S-HTTP) and HTTP Secure (HTTPS) are different protocols. S-HTTP is a technology that protects each message that is sent between two computers. HTTPS protects the communication channel between two computers, messages and all. HTTPS uses SSL and HTTP to provide a protected circuit between a client and server. So, S-HTTP is used if an individual message needs to be encrypted, but if all information that passes between two computers needs to be encrypted, then HTTPS is used, which is SSL over HTTP.

(iv) Secure Electronic Transaction

Secure Electronic Transaction (SET) is a security technology proposed by Visa and MasterCard to allow for more secure credit card transaction possibilities than what is currently available. SET has received acceptance as a standard for quite some time. Although SET provides an effective way of transmitting credit card information, businesses and users do not see it as efficient because it requires more parties to coordinate their efforts, more software installation and configuration for each entity involved, and more effort and cost than the widely used SSL method. SET is a cryptographic protocol and infrastructure developed to send encrypted credit card numbers over the Internet. The following entities would be involved with a SET transaction, which would require each of them to upgrade their software and possibly hardware:

(i) **Issuer (cardholder's bank)** Financial institution that provides a credit card to individual

(ii) **Cardholder** Individual authorized to use a credit card

(iii) **Merchant** Entity providing goods

(iv) **Acquirer (merchant's bank)** Financial institution that processes payment cards

(v) **Payment gateway** Processes merchant payment; may be acquirer

To use SET, a user must enter her credit card number into her electronic wallet software. This information is stored on the user's hard drive or on a smart card. The software then creates a public key and a private key used specifically for encrypting financial information before it is sent. This is basically a very secure way of doing business over the Internet, but today everyone seems to be happy enough with the security SSL provides. They do not feel motivated enough to move to a different and more encompassing technology. The lack of motivation comes from all of the changes that would need to take place to our current processes and the amount of money that these changes would require.

(v) Secure Shell

Secure Shell (SSH) functions as a type of tunneling mechanism that provides terminal like access to remote computers. SSH is a program and a protocol that can be used to log into another computer over a network. For example, the program can let Parul, who is on computer A, access computer B's files, run applications on computer B, and retrieve files from computer B without ever physically touching that computer. SSH provides authentication and secure transmission over vulnerable channels like the Internet. SSH should be used instead of Telnet, FTP, rlogin, rexec, or rsh, which provide the same type of functionality that SSH provides but in a much less secure manner. SSH is a program and a set of protocols that work together to provide a secure tunnel between two computers. The two computers go through a handshaking process and exchange via Diffie-Hellman a session key that will be used during the session to encrypt and protect the data that is exchanged.

Once the handshake takes place and a secure channel is established, the two computers have a pathway to exchange data with the assurance that the information will be encrypted and its integrity will be protected.

Summary

In this section we saw many of the different technologies within different types of networks, including how they work together to provide an environment in which users can communicate, share resources, and be productive. Each piece of networking is important to security, because almost any piece can introduce unwanted vulnerabilities and weaknesses into the infrastructure. It is important that you understand how the various devices, protocols, authentication mechanisms, and services work individually and how they interface and interact with other entities. This may appear to be an overwhelming task because of all the possible technologies involved. However, knowledge and hard work will keep you up to speed and hopefully in front of the hackers and attackers.

5.2 OPERATIONS SECURITY

Introduction

Operations security and controls safeguard information assets while the data is resident in the computer or otherwise directly associated with the computing environment. The controls address both software and hardware as well as such processes as change control and problem management. Operations security pertains to everything that takes place to keep a network, computer systems, applications, and environment up and running in a secure and protected manner. It consists of ensuring that people, applications, and servers have the proper access privileges to only the resources that they are entitled to and that oversight is implemented via monitoring, auditing, and reporting controls. Operations take place after the network is developed and implemented. This includes the continual maintenance of an environment and the activities that should take place on a day-to-day or week-to-week basis. These activities are routine in nature and enable the network and individual computer systems to continue to run correctly and securely.

Networks and computing environments are evolving entities; just because they are secure one week does not mean that they are still secure three weeks later. Many companies pay security consultants to come in and advise them on how to improve their infrastructure, policies, and procedures. A company can then spend thousands or even hundreds of thousands of rupees to implement the consultant's suggestions, install properly configured firewalls, intrusion detection systems (IDSs), and antivirus software, and patch management systems. However, if the IDS and antivirus software do not continually have updated signatures, if the systems are not continually patched, and if firewalls and devices are not tested for vulnerabilities, then the company can easily slip back into an insecure and dangerous place. This can happen if the company does not keep its operations security tasks up to date.

Role of the Operations Department

The continual effort to make sure that the correct policies, procedures, standards, and guidelines are in place and being followed. The right steps need to be taken to achieve the necessary level of security, while balancing ease of use, compliance with regulatory requirements, and cost constraints. It takes continued effort and discipline to retain the proper level of security. Operations security is all about ensuring that people, applications, equipment, and the overall environment are properly and adequately secured.

Although operations security is the practice of continual maintenance to keep an environment running at a necessary security level, liability and legal responsibilities also exist when performing these tasks. Companies, and senior executives at those companies, often have legal obligations to ensure that resources are protected, safety measures are in place, and security mechanisms are tested to guarantee that they are actually providing the necessary level of protection. If these operations security responsibilities are not fulfilled, the company may have more than antivirus signatures to be concerned about.

It is important to identify systems and operations that are sensitive, meaning they need to be protected from disclosure, and critical, meaning they must remain available at all times. It is also important to note that while organizations have a significant portion of their operations activities tied to computing resources, they still rely on physical resources as well to make things work, including paper documents and data stored on microfilm, tapes, and other removable media. A large part of operations security includes ensuring that the physical and environmental concerns are adequately addressed, such as temperature and humidity controls, media reuse, disposal, and destruction of media containing sensitive information. Overall, operations security is about configuration, performance, fault tolerance, security, and accounting and verification management to ensure that proper standards of operations and compliance requirements are met.

Administrative Management

Administrative management is a very important piece of operations security. One aspect of administrative management is dealing with personnel issues. This includes **separation of duties** and job rotation. The objective of separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way. High-risk activities should be broken up into different parts and distributed to different individuals or departments. That way, the company does not need to put a dangerously high level of trust in certain individuals. Separation of duties, therefore, is a preventive measure that requires collusion to occur in order for someone to commit an act that is against policy. Below are many of the common roles within organizations and their corresponding job definitions.

Organizational Role Core Responsibilities

(i) Control Group: Obtains and validates information obtained from analysts, administrators, and users and passes it on to various user groups.
(ii) Systems Analyst: Designs data flow of systems based on operational and user requirements.
(iii) Application Programmer: Develops and maintains production software.
(iv) Help Desk/Support: Resolves end user and system technical or operations problems.
(v) IT Engineer: Performs the day-to-day operational duties on systems and applications.
(vi) Database Administrator: Creates new database tables and manages the database.
(vii) Network Administrator: Installs and maintains the LAN/WAN environment.

(viii) Security Administrator: Defines, configures, and maintains the security mechanisms protecting the organization.

(ix) Tape Librarian: Receives, records, releases, and protects system and application files backed up on media such as tapes or disks.

(x) Quality Assurance: Can consist of both Quality Assurance (QA) and Quality Control (QC). QA ensures that activities meet the prescribed standards regarding supporting documentation and nomenclature. QC ensures that the activities, services, equipment, and personnel operate within the accepted standards.

Job rotation means that, over time, more than one person fulfills the tasks of one position within the company. This enables the company to have more than one person who understands the tasks and responsibilities of a specific job title, which provides backup and redundancy if a person leaves the company or is absent. Job rotation also helps identify fraudulent activities, and therefore can be considered a detective type of control. If Ajay has performed Karan's position, Ajay knows the regular tasks and routines that are to be completed to fulfill the responsibilities of that job. Thus, Ajay is better able to identify if Karan does something out of the ordinary and suspicious.

Least privilege and need to know are also administrative-type controls that should be implemented in an operations environment. **Least privilege** means that an individual should have just enough permissions and rights to fulfill his role in the company and no more. If an individual has excessive permissions and rights, it could open the door to abuse of access and put the company at more risk than is necessary. For example, if Sunil is a technical writer for a company, he does not necessarily need to have access to the company's source code. So, the mechanisms that control Sunil's access to resources should not let him access source code. This would properly fulfill operations security controls that are in place to protect resources.

Mandatory vacations are another type of administrative control. It makes sure that employees take their vacations, the reasons include being able to identify fraudulent activities and enabling job rotation to take place. If an accounting employee has been performing a salami attack by shaving off pennies from multiple accounts and putting the money into his own account, a company would have a better chance of figuring this out if that employee is required to take a vacation for a week or longer. When the employee is on vacation, another employee has to fill in. She might uncover questionable documents and clues of previous activities, or the company may see a change in certain patterns once the employee who is committing fraud is gone for a week or two. Again, the idea behind mandatory vacations is that, traditionally, those employees who have committed fraud are usually the ones who have resisted going on vacation because of their fear of being found out while away.

Accountability

Access and use must be specific to an individual user at a particular moment in time; it must be possible to track access and use to that individual. Throughout the entire protection process, user access must be appropriately controlled and limited to prevent excess privileges and the opportunity for serious errors. Tracking must always be an important dimension of this control. At the conclusion of the entire cycle, violations occurring during access and data manipulation phases must be reported on a regular basis so that these security problems can be solved.

Activity must be tracked to specific individuals to determine accountability. Responsibility for all actions is an integral part of accountability; holding someone accountable without assigning responsibility is meaningless. Conversely, to assign responsibility without accountability makes it impossible to enforce responsibility. Therefore, any method for protecting resources requires both responsibility and accountability for all of the parties involved in developing, maintaining, and using processing resources.

An example of providing accountability and responsibility can be found in the way some organizations handle passwords. Users are taught that their passwords are to be stored in a secure location and not disclosed to anyone. In some organizations, first-time violators are reprimanded; if they continue to expose organizational information, however, penalties may be imposed, including dismissal.

Security Operations and Product Evaluation

When products are evaluated for the level of trust and assurance they provide, many times operational assurance and life-cycle assurance are part of the evaluation process.

Operational assurance concentrates on the product's architecture, embedded features, and functionality that enable a customer to continually obtain the necessary level of protection when using the product. Examples of operational assurances examined in the evaluation process are access control mechanisms, the separation of privileged and user program code, auditing and monitoring capabilities, covert channel analysis, and trusted recovery when the product experiences unexpected circumstances.

Life-cycle assurance pertains to how the product was developed and maintained. Each stage of the product's life cycle has standards and expectations it must fulfill before it can be deemed a highly trusted product. Examples of life-cycle assurance standards are design specifications, clipping-level configurations, unit and integration testing, configuration management, and trusted distribution. Vendors that are looking to achieve one of the higher security ratings for its products will have each of these issues evaluated and tested.

Clipping Levels

Companies can set predefined thresholds for the number of certain types of errors that will be allowed before the activity is considered suspicious. The threshold is a baseline for violation activities that may be normal for a user to commit before alarms are raised. This baseline is referred to as a clipping level.

Configuration Management

Every company should have a policy indicating how changes take place within a facility, who can make the changes, how the changes are approved, and how the changes are documented and communicated to other employees. The changes can happen to network configurations, system parameters, applications, and settings when adding new technologies, application configurations, or devices, or when modifying the facility's environmental systems. Change control is important not only for an environment, but also for a product during its development and life cycle. Changes must be effective and orderly, because time and money can be wasted by continually making changes that do not meet an ultimate goal.

A well-structured change management process should be put into place to aid staff members through many different types of changes to the environment. This process should be laid out in the change control policy. Although the types of changes vary, a standard list of procedures can help keep the process under control and ensure that it is carried out in a predictable manner.

The following steps are examples of the types of procedures that should be part of any change control policy:

(i) **Request for a change to take place** Requests should be presented to an individual or group that is responsible for approving changes and overseeing the activities of changes that take place within an environment.

(ii) **Approval of the change** The individual requesting the change must justify the reasons and clearly show the benefits and possible pitfalls of the change. Sometimes the requester is asked to conduct more research and provide more information before the change is approved.

(iii) **Documentation of the change** Once the change is approved, it should be entered into a change log. The log should be updated as the process continues toward completion.

(iv) **Tested and presented** The change must be fully tested to uncover any unforeseen results. Depending on the severity of the change and the company's organization, the change and implementation may need to be presented to a change control committee. This helps show different sides to the purpose and outcome of the change and the possible ramifications.

(v) **Implementation** Once the change is fully tested and approved, a schedule should be developed that outlines the projected phases of the change being implemented and the necessary milestones. These steps should be fully documented and progress should be monitored.

(vi) **Report change to management** A full report summarizing the change should be submitted to management. This report can be submitted on a periodic basis to keep management up to date and ensure continual support.

These steps, of course, usually apply to large changes that take place within a facility. These types of changes are usually expensive and can have lasting effects on a company. It is also critical that the operations department create approved backout plans before implementing changes to systems or the network. To ensure that productivity is not negatively affected by these issues, a backout plan needs to be developed. This plan describes how the team will restore the system to its original state, before the change was implemented.

Change Control Documentation: Failing to document changes to systems and networks is only asking for trouble, because no one will remember, for example, what was done to that one server in the DMZ six months ago or how the main router was fixed when it was acting up last year. Changes to software configurations and network devices take place pretty often in most environments; keeping all of these details properly organized is impossible, unless someone keeps a log of this type of activity. Numerous changes can take place in a company, some of which are listed here:

(i) New computers installed
(ii) New applications installed
(iii) Different configurations implemented
(iv) Patches and updates installed
(v) New technologies integrated
(vi) Policies, procedures, and standards updated
(vii) New regulations and requirements implemented
(viii) Network or system problems identified and fixes implemented
(ix) Different network configuration implemented
(x) New networking devices integrated into the network
(xi) Company acquired by or merged with another company

The list could go on and on and could be general or detailed. Many companies have experienced some major problem that affects the network and employee productivity.

The IT department may run around trying to figure out the issue and go through hours or days of trial-and-error exercises to find and apply the necessary fix. If no one properly documents the incident and what was done to fix the issue, the company may be doomed to repeat the same scramble six months to a year down the road.

Media Controls

Media and devices that can be found in an operations environment require a variety of controls to ensure that they are properly preserved and that the integrity, confidentiality, and availability of the data that is held on them are not compromised.

The operational controls that pertain to these issues come in many flavors. The first are controls that prevent unauthorized access, which can be physical, administrative and technical controls that are put into place. If the company's backup tapes are to be properly protected, they need to be stored in a place where only authorized people have access to them, which could be in a locked server room or an offsite facility. If the tapes need to be protected from environmental issues such as humidity, heat, cold, fire, and natural disasters, they should be kept in a fireproof safe in a regulated environment or in an offsite facility that controls the environment to be hospitable to data processing components. Companies may have a media library with a librarian in charge of protecting its resources. Users may be required to check out specific types of media and resources, instead of having the resources readily available for anyone to access them. If the library controls backed-up data, each tape should be labeled with the following information:

(i) The date of creation
(ii) The individual who created the backup
(iii) The retention period (how long the data needs to be maintained)
(iv) The classification
(v) The volume name and version

Media should be clearly marked and logged, its integrity should be verified, and it should be properly erased of data when necessary. When media is cleared of its contents, it is said to be **sanitized**. There are several methods to sanitize media: overwriting (zeroization), degaussing, and destruction. Deleting files on a piece of media does not actually make the data disappear; it only deletes the pointers to where those files still live on the disk. This is how companies that specialize in restoration can recover the deleted files intact after they have been apparently destroyed.

Data remanence is the residual physical representation of information that was saved and then erased in some fashion. This remanence may be enough to enable the data to be reconstructed and restored to a readable form. This can pose a security threat to a company that thinks it has properly erased confidential data from its media. If the media does not hold confidential or sensitive information, overwriting or deleting the files may be the appropriate step to take. If the data is sensitive, degaussing may be required. If the data is highly confidential or the media cannot be properly degaussed, the appropriate action would be to physically destroy it.

System Controls

System controls are also part of operations security. Within the operating system itself, certain controls must be in place to ensure that instructions are being executed in the correct security context. The system has mechanisms that restrict the execution of certain types of instructions so that they can take place only when the operating system is in a privileged or supervisor state. This protects the overall security and state of the system and helps to ensure that it runs in a stable and predictable manner. Operational procedures need to be developed that indicate what constitutes the proper operation of a system or resource. This would include a system startup and shutdown sequence, error handling, and restoration from a known good source. An operating system does not provide direct access to hardware by processes of lower privilege, which are usually processes used by user applications. If a program needs to send instructions to hardware devices, the request is passed off to a process of higher privilege. To execute privileged hardware instructions, a process must be running in a restrictive and protective state. This is an integral part of the operating system's architecture, and the determination of what processes can submit what type of instructions is made based on the operating system's control tables. Many input/output (I/O) instructions are defined as privileged and can be executed only by the operating system kernel processes. When a user program needs to send I/O information, it must notify the system's core, privileged processes that work at the inner rings of the system. These processes (called system services) authorize either the user program processes to perform these actions and temporarily increase their privileged state or the system's processes are used to complete the request on behalf of the user program.

Trusted Recovery

When an operating system or application crashes or freezes, it should not put the system in any type of insecure state. The usual reason for a system crash in the first place is that it encountered something that it perceived as insecure or did not understand and decided that it was safer to freeze, shut down, or reboot than to perform the current activity. An operating system's response to a type of failure can be classified as one of the following:

(i) System reboot
(ii) Emergency system restart
(iii) System cold start

A **system reboot** takes place after the system shuts itself down in a controlled manner in response to a trusted computing base (TCB) failure.

An **emergency system restart** takes place after a system failure happens in an uncontrolled manner. This could be a TCB or media failure caused by lower-privileged user processes attempting to access memory segments that are restricted.

A **system cold start** takes place when an unexpected TCB or media failure happens and the regular recovery procedure cannot recover the system to a more consistent state. It is important to ensure that the system does not enter an insecure state when it is affected by any of these types of problems, and that it shuts down and recovers properly to a secure and stable state.

Network and Resource Availability

Network and resource availability often is not fully appreciated until it is gone. That is why administrators and engineers need to implement effective backup and redundant systems to make sure that when something happens (and something will happen), users' productivity will not be drastically affected. A majority of networks use Ethernet technology, which is very resistant to failure. Token Ring was designed to be fault tolerant and does a good job when all the computers within this topology are configured and act correctly. If one network interface card (NIC) is working at a different speed than the others, the whole ring can be affected and traffic may be disrupted. Also, if two systems have the same MAC address, the whole network can be brought down. These issues need to be considered when maintaining an existing network. If an engineer is installing a NIC on a Token Ring network, she should ensure that it is set to work at the same speed as the others and that there is no possibility for duplicate MAC addresses.

Single Points of Failure

A **single point of failure** poses a lot of potential risk to a network, because if the device fails, a segment or even the entire network is negatively affected. Devices that could represent single points of failure are firewalls, routers, network access servers, T1 lines, switches, bridges, hubs, and authentication servers—to name a few. The best defenses against being vulnerable to these single points of failure are proper maintenance, regular backups, and redundancy. An uninterruptible power supply (UPS) and redundant array of inexpensive disks (RAID) should be in place and properly configured.

RAID

Redundant array of inexpensive disks (RAID) is a technology used for redundancy and performance improvement. It combines several physical disks and aggregates them into logical arrays. When data is saved, it is written across all drives. A RAID appears as a single drive to applications and other devices. When data is written across all drives, the technique of **striping** is used. This activity divides and writes the data over several drives. The write performance is not affected, but the read performance is increased dramatically because more than one head is retrieving data at the same time. It might take the RAID system six seconds to write a block of data to the drives and only two seconds or less to read the same data from the disks. Various levels of RAID dictate the type of activity that will take place within the RAID system. The most common RAID levels used today are levels 1, 3, and 5.

Following Table describes each of the possible RAID levels.

RAID	**Level Activity**	**Name**
0	Data striped over several drives. No redundancy or parity is involved. If one volume fails, the entire volume is unusable. It is used for performance only.	Striping
1	Mirroring of drives. Data is written to two drives at once. If one drive fails, the other drive has the exact same data available.	Mirroring
2	Data striping over all drives at the bit level. Parity data is created with a hamming code, which identifies any errors. This level specifies that up to 39 disks can be used: 32 for storage and 7 for error recovery data. This is not used in production today.	Hamming code parity
3	Data striping over all drives and parity data held on one drive. If a drive fails, it can be reconstructed from parity drive.	Byte-level parity
4	Same as level 3, except parity is created at the block level instead of the byte level.	Block-level parity

RAID	Level Activity	Name
5	Data is written in disk sector units to all drives. Parity is written to all drives also, which ensures that there is no single point of failure.	Interleave parity
6	Similar to level 5 but with added fault tolerance, which is a second set of parity data written to all drives.	Second parity data (or double parity)
10	Data is simultaneously mirrored and striped across several drives and can support multiple drive failures.	Striping and mirroring

Clustering

Clustering is a fault-tolerant server technology that is similar to redundant servers, except each server takes part in processing services that are requested. A server cluster is a group of servers that are viewed logically as one server to users and can be managed as a single logical system. Clustering provides for availability and scalability. It groups physically different systems and combines them logically, which provides immunity to faults and improves performance. Clusters work as an intelligent unit to balance traffic, and users who access the cluster do not know that they may be accessing different systems at different times. To the users, all servers within the cluster are seen as one unit. If one of the systems within the cluster fails, processing continues because the rest pick up the load, although degradation in performance could occur. This is more attractive, however, than having a secondary server that waits in the wings in case a primary server fails, because this secondary server may just sit idle for a long period of time, which is wasteful. When clustering is used, all systems are used to process requests and none sits in the background waiting for something to fail. Clustering offers a lot more than just availability, however. It also provides load balancing (each system takes a part of the processing load), redundancy, and failover (other systems continue to work if one fails).

Backups

Backing up software and having backup hardware devices are two large parts of network availability. You need to be able to restore data if a hard drive fails, a disaster takes place, or some type of software corruption occurs. A policy should be developed that indicates what gets backed up, how often it gets backed up, and how these processes should occur. If users have important information on their workstations, the operations department needs to develop a method that indicates that backups include certain directories on users' workstations or that users move their critical data to a server share at the end of each day to ensure that it gets backed up. Backups may occur once or twice a week, every day, or every three hours. It is up to the company to determine this routine. The more frequent the backups, the more staff time that will be dedicated to it, so there needs to be a balance between backup costs and the actual risk of potentially losing data.

A company may find that conducting automatic backups through specialized software is more economical and effective than spending IT work hours on the task. The integrity of these backups needs to be checked to ensure that they are happening as expected—rather than finding out right after two major servers blow up that the automatic backups were saving only temporary files.

5.3 E-MAIL SECURITY

E-mail has become an important and integrated part of people's lives. It is used to communicate with family and friends, business partners and customers, coworkers and management, and online merchants and government offices. Generally, the security, authenticity, and integrity of an e-mail message are not considered in day-to-day use. Users are more aware that attachments can carry viruses than of the fact that an e-mail can be easily spoofed and that its contents can be changed while in transmission.

It is very easy to **spoof** e-mail messages, which means to alter the name in the From field. All an attacker needs to do is modify information within the Preferences section of his mail client and restart the application. As an example of a spoofed e-mail message, an attacker could change the name in the From field to the name of the network administrator and send an e-mail message to the CEO's secretary, telling her that the IT department is having problems with some servers and needs her to change her network logon to "password." If she receives this e-mail and sees that the From field has the network administrator's name in it, she will probably fulfill this request without thinking twice.

The solution to this and similar types of attacks is to require proper authentication to ensure that the message actually came from the source indicated. Companies that regard security as one of their top priorities would implement an e-mail protection application that can digitally sign messages, like Pretty Good Privacy (PGP), or use a public key infrastructure (PKI). These companies may also consider using an encryption protocol to help fight network sniffing and unauthorized interception of messages.

If a user is going to use a security scheme to protect his messages from eavesdropping, modification, and forgery, he and the recipient must use the same encryption scheme. If public key cryptography is going to be used, both users must have a way to exchange encryption keys. This is true for PGP, digital signatures, and products that follow the S/MIME standard. If an administrator, or security professional, wants to ensure that all messages are encrypted between two points and does not want to have to depend on the users to properly encrypt their messages, she can implement a VPN. All these standards are explained in another domain.

Hack and Attack Methods

A majority of the tools used by hackers have dual capabilities in that they can be used for good or evil. An attacker could use tool ABC to find a vulnerability to exploit, and a security professional could use the same tool to identify a vulnerability so that she could fix it. When this tool is used by black hats (attackers), it is referred to as hacking. When a white hat (security professional) uses this tool, it is considered ethical hacking or penetration testing.

The tools used to perform attacks on networks and systems have, over time, become so sophisticated that they offer even a moderately skilled individual (sometimes called a script kiddie) the ability to perform very damaging attacks. The tools are simple to use and often come with a GUI that walks the person through the steps of resource identification, network mapping, and the actual attack. The person no longer needs to understand protocol stacks, know what protocols' fields are used by different systems, understand how operating systems process program and assembly code, or know how to write program code at all. The hacker just needs to insert an IP range within a GUI tool and click Go. There are now many different types of tools used by the attacker community, some of which are even capable of generating virus and worm autocode and building specific exploits for a given operating system, platform, or application release level.

Any network administrator who maintains a firewall, or any person who runs a personal firewall on a computer, knows how active the Internet is with probes and port scanners. These front-end protection devices are continually getting hit with packets requesting information. Some probes look for specific types of computers, such as Unix systems, web servers, or databases, because the attacker has specific types of attacks she wants to carry out, and these attacks target specific types of operating systems or applications. These probes could also be looking to plant Trojan horses or viruses in computers in the hope of causing destruction or compromising the systems so that they can be used in future distributed denial-of-service (DDoS) attacks. These probes scan thousands of networks and computers with no one target in mind. They just look for any and all vulnerabilities, and the attacker does not necessarily care where the vulnerable system happens to be located.

When an attacker identifies her target, she will do network mapping and port scanning. Network-mapping tools send out seemingly non dangerous packets to many different systems on a network. These systems respond to the packets, and the mapping tool interrogates the returned packets to find out what systems are up and running, the types of operating systems that responded, and possibly their place within the network. When the tool receives these two slightly different responses, it can determine what type of operating system just replied. The tool and the attacker start to put together the topology of the victim's network.

The network-mapping tool may have a database that maps operating systems, applications, and versions to the type of responses and message fields they use. So if the networking tool received a reply from its ICMP ping sweep, which sends out ICMP packets to targets within a configured IP address range, and one reply has the ICMP "Don't fragment" bit enabled, the tool may determine that the target is a Unix host. Or if the tool sent out a TCP SYN packet and the response received was an FIN/ACK, the tool may determine that the target is a Windows NT system. This activity is referred to as **operating system fingerprinting**.

So, the first step for the attacker is to find out what systems are alive, attempt to find out what type of operating systems the targets are running, and start to build the networks topology. The next step for an attacker is to do **port scanning** on the target machines, which identifies open ports on a computer. Ports provide doors into the operating system for other computers, processes, protocols, and attackers. If an attacker can find out what ports are open, she can have a pretty good idea of what services are running on the systems. Knowing what services are available can further clarify the type of system the target is. For example, if a target computer responds to an SMTP packet sent to its port 25, the attacker could conclude that this computer may be an e-mail server. However, more work would need to be done to confirm this.

The attacker wants to know what operating systems, applications, and services are running so that she knows what types of attacks to run. If she finds a Unix server running Apache, she would run totally different types of attacks on it than she would run for a Windows 2000 server running IIS. Each operating system, application, and service has its own vulnerabilities, and properly identifying these enables the attacker to be more successful in her attack. There are 65,535 TCP and 65,535 UDP ports on every computer system. The first 1024 are said to be **well-known ports**. This means that a specific port number under 1025 is usually mapped to a well-known and used protocol. For instance, port 80 is almost always mapped to the Hypertext Transfer Protocol (HTTP), port 21 is mapped to the File Transfer Protocol (FTP), and port 25 is mapped to SMTP. These ports can be reconfigured so that port 21 is mapped to HTTP, let's say, but that is very uncommon.

A port-scanning utility is used to find out what ports are open on a system so that the attacker knows what doors are available to her. This tool will send packets to each and every port on a system and listen for its response. If there is no response or a message indicating “Port Unreachable,” this usually indicates that the port and its corresponding service is disabled. If a predictable response comes from the port, the attacker knows the port is open and available for attack. A port needs to be open and available for functionality. For example, most networks require the use of SMTP, port 25, for e-mail activity. The administrator needs to put a barrier between the potential attackers and this vulnerable port and its service. Of course, the first step is to implement a perimeter network with firewalls, proxy servers, and routers that only permit acceptable connections to the internal hosts. However, if an administrator or security professional wanted to add another layer of protection, he could implement **TCP wrappers**.

These software components (wrappers) monitor incoming network traffic and control what can and cannot access the services mapped to specific ports. When a request comes to a computer at a specific port, the target operating system will check to see if this port is enabled. If it is enabled and the operating system sees that the corresponding service is wrapped, it knows to look at an access control list, which spells out who can access this service. If the person or computer attempting to access this service is allowed within the access control list, the operating system allows the connection to be made. If this person or computer is not allowed, the packet is dropped or a message is sent back to the initiator of the request, indicating that the request is refused. At this point, the attacker has an idea of what systems are alive, what ports are open, and what services are listening and available for attack. Although the search for exploitable vulnerabilities is becoming more focused, there is still an incredible number of possible vulnerabilities one network can have. Sometimes attackers specialize in a few specific attacks that they know well enough to carry out manually or have scripts that carry out specific attacks for them. But many attackers want a large range of possible attacks available to them, so they use **vulnerability scanning tools**.

Vulnerability scanning tools have a large database of vulnerabilities and the capability to exploit many of the vulnerabilities they identify. New vulnerabilities are found each week in operating systems, web servers, database software, and applications. It can be overwhelming to try to keep up to date on each of these and the proper steps to carry them out. The vulnerability scanners can do this for the security professional and, unfortunately, for the attacker. These tools have an engine that can connect to the target machine and run through its database of vulnerabilities to see which apply to the target machine. Some tools can even go a step further and attempt the exploit to determine the actual degree of vulnerability.

As stated earlier, these tools are dual purpose in nature. Network administrators and security professionals should be using these types of tools on their environments to see what vulnerabilities are present and available to potential attackers. That way, when a vulnerability or weakness is uncovered, the security professional can fix it before an attacker finds it.

Browsing

Browsing is a general technique used by intruders to obtain information that they are not authorized to access. This type of attack takes place when an attacker is looking for sensitive data but does not know the format the data is in (word processing document, spreadsheet, database, piece of paper). An example of browsing is when an intruder accesses residual information on storage media. The original user may have deleted the files from a floppy disk, but this only removes the pointers to the files within the file system on that disk. The talented intruder can access this data (residual information) and access information that he is unauthorized to obtain.

Another type of browsing attack is called **shoulder surfing**, where an attacker looks over another's shoulder to see items on that person's monitor or what is being typed in at the keyboard.

Sniffers

A **network sniffer** is a tool that monitors traffic as it traverses a network. Administrators and network engineers often use sniffers to diagnose network problems. Sniffers are also referred to as network analyzers or protocol analyzers. When used as a diagnostic tool, a sniffer enables the administrator to see what type of traffic is being generated, in the hope of getting closer to the root of the network problem. When a sniffer is used as a tool by an attacker, the sniffer can capture usernames, passwords, and confidential information as they travel over the network.

Sniffers have been very successful because a majority of LANs use Ethernet, which is a broadcast technology. Because so much data is continually broadcasted, it is easily available for an attacker who has planted a sniffer on a network segment. However, sniffers are becoming less successful because of the move to switched environments.

Switched environments separate network segments by broadcast and collision domains. If the attacker is not within the broadcast and collision domain of the environment she is interested in sniffing, she will not receive the information she is looking for, because a switch is usually configured so that the required source and destination ports on the switch carry the traffic, meaning the traffic is not blasted for everyone in the vicinity to hear. Switched traffic travels from point A to point B through the switch and does not spill over to every computer on the network, as it does in nonswitched networks.

Loki

A common covert channel in use today is the Loki attack. This attack uses the ICMP protocol for communications purposes. This protocol was not developed to be used in this manner; it is only supposed to send status and error messages. But someone developed a tool (Loki) that allows an attacker to write data right behind the ICMP header. This allows the attacker to communicate with another system through a covert channel. It is usually very successful because most firewalls are configured to allow ICMP traffic in and out of their environments. This channel is covert because it uses something for communication purposes that was not developed for this type of communication functionality. More information on this type of attack can be found at http://xforce.iss.net/xforce/xfdb/1452.

Password Cracking

There are various ways of authenticating a user, most of the time a static password is the method of choice for many companies. The main reason for this choice is that the computing society is used to using static passwords; this is how many systems and applications have their authentication processes coded, and it is an easier technique to maintain and cheaper than other options such as smart cards or biometrics.

However, this static password method is easily cracked when a determined attacker has the right tools. John the Ripper is an example of a sniffer and password cracker that listens for authentication data being passed over network cables. Once the data is captured, the attacker can initiate a dictionary attack using the same tool to try to reveal the captured password. The powerful tools Crack and L0phtcrack are also used to perform dictionary and brute force attacks on the captured password or password file.

A strong password policy is a major countermeasure to password-cracking efforts. The policy should dictate that passwords must be at least eight characters, with upper-and lowercase letters and two special characters (*.,$@). If the passwords are long, contain special characters, and are hard to guess, it will take cracking tools much longer to uncover them. The longer this process takes, the higher the chance of the attacker moving on to an easier victim. Software applications and add-ons are available to ensure that the password that each user chooses meets the company's security policy.

Backdoors

A backdoor is a program that is installed by an attacker to enable her to come back into the computer at a later date without having to supply login credentials or go through any type of authorization process. Access control is thwarted by the attacker because she can later gain access to the compromised computer. The backdoor program actually listens on specific ports for the attacker, and once the attacker accesses those ports, the backdoor program lets her come right in. An attacker can compromise a computer and install the backdoor program or hide the code within a virus or Trojan horse that will install the backdoor when a predefined event takes place. Many times, these backdoors are installed so that the attacker can later control the computer remotely to perform the tasks she is interested in. The tools used for backdoor remote-control actions are Back Orifice, NetBus, and SubSeven.

The following list contains a brief description of a sampling of attack types you should be familiar with:

(1) **Denial-of-service (DoS) attack** An attacker sends multiple service requests to the victim's computer until they eventually overwhelm the system, causing it to freeze, reboot, and ultimately not be able to carry out regular tasks.

(2) **Man-in-the-middle attack** An intruder injects herself into an ongoing dialog between two computers so that she can intercept and read messages being passed back and forth. These attacks can be countered with digital signatures and mutual authentication techniques.

(3) **Mail bombing** This is an attack used to overwhelm mail servers and clients with unrequested e-mails. Using e-mail filtering and properly configuring e-mail relay functionality on mail servers can be used to protect against this type of DoS attack.

(4) **Wardialing** This is a brute force attack in which an attacker has a program that systematically dials a large bank of phone numbers with the goal of finding ones that belong to modems instead of telephones. These modems can provide easy access into an environment. The countermeasures are to not publicize these telephone numbers and to implement tight access control for modems and modem pools.

(5) **Ping of death** This is a type of DoS attack in which oversized ICMP packets are sent to the victim. Systems that are vulnerable to this type of attack do not know how to handle ICMP packets over a specific size and may freeze or reboot. Countermeasures are to patch the systems and implement ingress filtering to detect these types of packets.

(6) **Fake login screens** A fake login screen is created and installed on the victim's system. When the user attempts to log into the system, this fake screen is presented to the user, requesting that he enter his credentials. When he does so, the screen captures the credentials and exits, showing the user the actual login screen for his system. Usually the user just thinks he mistyped his password and attempts to authenticate again without knowing anything malicious just took place. A host-based IDS can be used to detect this type of activity.

(7) **Teardrop** This attack sends malformed fragmented packets to a victim. The victim's system usually cannot reassemble the packets correctly and freezes as a result. Countermeasures to this attack are to patch the system and to use ingress filtering to detect these packet types.

(8) **Traffic analysis** This is a method of uncovering information by watching traffic patterns on a network. For example, heavy traffic between the HR department and headquarters could indicate an upcoming layoff. Traffic padding can be used to counter this kind of attack, in which decoy traffic is sent out over the network to disguise patterns and make it more difficult to uncover patterns.

(9) **Slamming and cramming** Slamming is when a user's service provider has been changed without that user's consent. Cramming is adding on charges that are bogus in nature that the user did not request. Properly monitoring charges on bills is really the only countermeasure to these types of attacks.

Penetration Testing

Penetration testing is the process of simulating attacks on a network and its systems at the request of the owner, senior management. Penetration testing uses a set of procedures and tools designed to test and possibly bypass security controls of a system. Its goal is to measure an organization's level of resistance to an attack and to uncover any weaknesses within the environment. Organizations need to determine the effectiveness of their security measures and not just trust the promises of the security vendors. Good computer security is based on reality, not on some lofty goals of how things are supposed to work.

A penetration test emulates the same methods that attackers would use. Attackers can be clever, creative, and resourceful in their techniques, so penetration attacks should align with the newest hacking techniques along with strong foundational testing methods. The test should look at each and every computer in the environment, because an attacker will not necessarily scan one or two computers only and call it a day. The type of penetration test that should be used depends on the organization, its security objectives, and the management's goals. Some corporations perform periodic penetration tests on themselves using different types of tools or use scanning devices that continually examine the environment for new vulnerabilities in an automated fashion. Other corporations ask a third party to perform the vulnerability and penetration tests to provide a more objective view.

Penetration tests can evaluate web servers, DNS servers, router configurations, workstation vulnerabilities, access to sensitive information, remote dial-in access, open ports, and available services' properties that a real attacker might use to compromise the company's overall security. Some tests can be quite intrusive and disruptive. The timeframe for the tests should be agreed upon so that productivity is not affected and personnel can bring systems back online if necessary.

The result of a penetration test is a report given to management that describes the vulnerabilities that were identified and the severity of those vulnerabilities, along with suggestions on how to deal with them properly. From there, it is up to management to determine how the vulnerabilities are actually dealt with and what countermeasures are implemented.

When performing a penetration test, the team goes through a five-step process:

(1) **Discovery:** footprinting and gathering information about the target

(2) **Enumeration:** performing port scans and resource identification methods

(3) **Vulnerability:** mapping Identifying vulnerabilities in identified systems and resources

(4) **Exploitation:** attempting to gain unauthorized access by exploiting vulnerabilities

(5) **Report to management:** delivering to management documentation of test findings along with suggested countermeasures

The penetration testing team can have varying degrees of knowledge about the penetration target before the tests are actually carried out.

(i) **Zero knowledge** Team does not have much knowledge of target and must start from ground zero

(ii) **Partial knowledge** Team has some information about target

(iii) **Full knowledge** Team has intimate knowledge of target

It is important that the team start off with only basic user-level access, to properly simulate different attacks. The team needs to utilize a variety of different tools and attack methods, and look at all possible vulnerabilities, because this is how actual attackers will function. It is extremely important that the team gets written permission from the right level of management before proceeding with any of these types of activities.

Summary

Operations security involves keeping up with implemented solutions, keeping track of changes, properly maintaining systems, continually enforcing necessary standards, and following through with security practices and tasks. It does not do much good for a company to develop a strong password policy if, after a few months, enforcement gets lax and users can use whatever passwords they want. It is similar to working out and staying physically fit. Just because someone lifts weights and jogs for a week does not mean he can spend the rest of the year eating jelly donuts and expect to stay physically fit. Security requires discipline day in and day out, sticking to a regime, and practicing due care.

CHAPTER 6

PHYSICAL AND ENVIRONMENTAL SECURITY

6.1 INTRODUCTION

Physical security encompasses a different set of threats, vulnerabilities, and risks than the other types of security that have been addressed so far. Physical security mechanisms include site design and layout, environmental components, emergency response readiness, training, access control, intrusion detection, and power and fire protection. Physical security mechanisms protect people, data, equipment, systems, facilities, and a long list of company assets. Physical security has a different set of vulnerabilities, threats, and countermeasures from that of computer and information security. The set for physical security has more to do with physical destruction, intruders, environmental issues, theft, and vandalism. When security professionals look at information security, they think about how someone can enter an environment in an unauthorized manner through a port, modem, or wireless access point. When security professionals look at **physical security**, they are concerned with how people can physically enter an environment and cause an array of damages.

The threats that an organization faces fall into many different categories:

(i) **Natural environmental threats** Floods, earthquakes, storms and tornadoes, fires, extreme temperature conditions, and so forth.

(ii) **Supply system threats** Power distribution outages, communications interruptions, and interruption to other natural energy resources such as water, steam, and gas, and so forth.

(iii) **Manmade threats** Unauthorized access (both internal and external), explosions, damage by angry employees, employee errors and accidents, vandalism, fraud, theft, and so forth.

(iv) **Politically motivated threats** Strikes, riots, civil disobedience, terrorist attacks and bombings, and so forth.

In all situations, the primary consideration, above all else, is that nothing should impede **life safety** goals. Physical security needs to be implemented based on a **layered defense model**, which means that physical controls should work together in a tiered architecture. The concept is that if one layer fails, other layers will protect the valuable asset. Layers would be implemented moving from the perimeter toward the asset. For example, you would have a fence, then your facility walls, then an access control card device, then a guard, then an IDS, and then locked computer cases and safes. This series of layers will protect the company's most sensitive assets, which would be placed in the innermost control zone of the environment. Security needs to protect all the assets of the organization and enhance productivity by providing a secure and predictable environment.

6.2 PHYSICAL SECURITY THREATS

The main threats that physical security components combat are theft, interruptions to services, physical damage, compromised system and environment integrity, and unauthorized access. Real loss is determined by the cost to replace the stolen items, the negative effect on productivity, the negative effect on reputation and customer confidence, fees for consultants that may need to be brought in, and the cost to restore lost data and production levels. Many times, companies just perform an inventory of their hardware and provide value estimates that are plugged into risk analysis to determine what the cost to the company would be if the equipment were stolen or destroyed. However, the information held within the equipment may be much more valuable than the equipment itself, and proper recovery mechanisms and procedures also need to be plugged into the risk assessment for a more realistic and fair assessment of cost.

A company may have a need for a safe. Safes are commonly used to store backup data tapes, original contracts, or other types of valuables. The safe should be penetration resistant and/or provide fire protection, depending upon the need. The types of safes that an organization can choose from are:

(i) **Wall safe** Embedded into the wall and easily hidden

(ii) **Floor safe** Embedded into the floor and easily hidden

(iii) **Chests** Stand-alone safes

(iv) **Depositories** Safes with slots, which allow the valuables to be easily slipped in

(v) **Vaults** Safes that are large enough to provide walk-in access

If a safe has a combination lock, it should be changed periodically and only a small subset of people should have access to the combination or key. The safe should be in a visible location, so that anyone who is interacting with the safe can be seen. The goal is to uncover any unauthorized access attempts.

More physical threats:

Fire: A conflagration affects information systems through heat, smoke, or suppression agent (e.g., fire extinguishers and water) damage. This threat category can be minor, major, or catastrophic. Controls can be deployed like smoke detectors near equipment; fire extinguishers near equipment and also train employees in their proper use, conduct regular fire evacuation exercises.

Environmental failure: This type of disaster includes any interruption in the supply of controlled environmental support provided to the operations center. Environmental controls include clean air, air conditioning, humidity, and water. Controls: since humans and computers don't coexist well, try to keep them separate. Many companies are establishing command centers for employees and a "lights-out" environment for the machines. Keep all rooms containing computers at reasonable temperatures (60 to 75ºF or 10 to 25ºC). Keep humidity levels at 20 to 70% and monitor environmental settings.

Earthquake: A violent ground motion results from stresses and movements of the earth's surface. Controls: keep computer systems away from glass and elevated surfaces, in high-risk areas secure the computers with antivibration devices.

Liquid Leakage: A liquid inundation includes burst or leaking pipes and accidental discharge of sprinklers. Controls: keep liquid-proof covers near the equipment and install water detectors on the structural floor near the computer systems.

Lightning: An electrical charge of air can cause either direct lightning strikes to the facility or surges due to strikes to electrical power transmission lines, transformers, and substations. Controls: install surge suppressors, store backups in grounded storage media, install and test Uninterruptible Power Supply (UPS) and diesel generators.

Electrical Interruption: A disruption in the electrical power supply, usually lasting longer than one-half hour, can have serious business impact. Controls: install and test UPS, install line filters to control voltage spikes, and install antistatic carpeting.

The human factor

Recent studies indicate that 72% of all thefts, fraud, sabotage, and accidents are caused by a company's own employees. Another 15 to 20% comes from contractors and consultants who are given access to buildings, systems, and information. Only about 5 to 8% is done by external people, yet the press and management focus mostly on them. The typical computer criminal is a nontechnical authorized user of the system who has been around long enough to locate the control deficiencies.

When implementing control devices, make certain that the controls meet the organization's needs. Include a review of internal access, and be certain that employees meet the standards of due care imposed on external sources.

“Intruders” can include anybody who is not authorized to enter a building, system, or data.

The first defense against intruders is to keep them out of the building or computer room. However, because of cost-cutting measures in the past two decades, very few computer facilities are guarded anymore. With computers everywhere, determining where to install locks is a significant problem.

To gain access to any business environment, everybody should have to pass an authentication and/or authorization test. The three ways of authenticating users involve something:
(i) That the user knows (a password).
(ii) That the user has (a badge, key, card, or token).
(iii) Of their physiognomy (fingerprint, retinal image, voice)

6.3 PHYSICAL SECURITY MEASURES

Administrative Controls

Administrative controls, also known as work strategy controls, are strategies used by admin to limit exposure to a hazard. For example, changes to the work schedule (i.e., when and how the job is performed) can limit the amount of time an employee is exposed to elevated temperatures.

Natural access control

Natural access control is the guidance of people entering and leaving a space by the placement of doors, fences, lighting, and even landscaping. An environment’s space should be divided into zones with different security levels, depending upon who needs to be in that zone and the associated risk. The zones can be labeled as controlled, restricted, public, or sensitive. This is conceptually similar to data classification. In a data classification program, different classifications are created, along with data handling procedures and the level of protection that each classification requires. The same is true of physical zones. Each zone should have a specific protection level that is required of it, which will help dictate the types of controls that should be put into place.

Access control should be in place to control and restrict individuals from going from one security zone to the next. Access control should also be in place for all facility entrances and exits. The security program development team needs to consider other ways in which intruders can gain access to buildings, such as by climbing adjacent trees to access skylights, upper-story windows, and balconies.

The following controls are commonly used for access controls within different organizations:

(i) Limit the number of entry points
(ii) Force all guests to go to a front desk and sign in before entering the environment
(iii) Reduce the number of entry points even further after hours or during the weekend when not as many employees are around
(iv) Have a security guard validate a picture ID before allowing entrance
(v) Require guests to sign in and be escorted
(vi) Encourage employees to question strangers

Access barriers can be naturally created (cliffs, rivers, hills), existing manmade elements (railroad tracks, highways), or artificial forms designed specifically to impede movement (fences, closing streets).

Personnel access controls

Proper identification needs to verify if the person attempting to access a facility or area should actually be allowed in. Identification and authentication can be verified by matching an anatomical attribute (biometric system), by using smart or memory cards (swipe cards), by presenting a photo ID to a security guard, by using a key, or by providing a card and entering a password or PIN.

A common problem with controlling authorized access into a facility or area is called **piggybacking**. This occurs when an individual gains unauthorized access by using someone else's legitimate credentials or access rights. Usually an individual just follows another person closely through a door without providing any credentials. The best preventive measures against piggybacking are to have security guards at access points and to educate employees about good security practices. If a company wants to use a card badge reader, it has several types of systems to choose from. Individuals usually have cards that have embedded magnetic strips that contain access information. These access cards can be used with **user-activated readers**, which just means the user actually has to do something swipe the card or enter a PIN. **System sensing access control readers**, also called **proximity devices or transponders**, recognize the presence of an approaching object within a specific area. This type of system does not require the user to swipe the card through the reader. The reader sends out interrogating signals and obtains the access code from the card without the user having to do anything.

Tokens

A token is an object the user carries to authenticate his or her identity. These devices can be token cards, card readers, or biometric devices. They have the same purpose: to validate the user to the system. The most prevalent form is the card, an electric device that normally contains encoded information about the individual who is authorized to carry it. Tokens are typically used with another type of authentication. Many cipher locks have been replaced with token card access systems.

(i) Challenge-Response Tokens

Challenge-response tokens supply passcodes that are generated using a challenge from the process requesting authentication. Users enter their assigned user IDs and passwords plus a password supplied by the token card. This process requires that the user supply something they possess (the token) and something that they know (the challenge/response process). This process makes passcode sniffing and brute force attacks futile. Challenge-response is an asynchronous process. An alternative to challenge-response is the synchronous token that generates the password without the input of a challenge from the system. It is synchronized with the authenticating computer when the user and token combination is registered on the system.

(ii) Dumb Cards

For many years, photo identification badges have sufficed as a credential for most people. With drivers' licenses, passports, and employee ID badges, the picture, along with the individual's statistics supplies enough information for the authentication process to be completed. Most people flash the badge to the security guard or give a license to a bank teller. Someone visually matches the ID holder's face to the information on the card.

(iii) Smart Cards

The automatic teller machine (ATM) card is an improvement on the "dumb card"; these "smart" cards require the user to enter a personal ID number (PIN) along with the card to gain access. The ATM compares the information encoded on the magnetic stripe with the information entered at the ATM machine.

The smart card contains microchips that consist of a processor, memory used to store programs and data, and some kind of user interface. Sensitive information is kept in a secret read-only area in its memory, which is encoded during manufacturing and is inaccessible to the card's owner. Typically, these cards use some form of cryptography that protects the information. Not all smart cards work with card readers. A user inserts the card into the reader, the system displays a message, and if there is a match, then the user is granted access.

Biometric Devices

Every person has unique physiological, behavioral, and morphological characteristics that can be examined and quantified. Biometrics is the use of these characteristics to provide positive personal identification. Fingerprints and signatures have been used for years to prove an individual's identity, but individuals can be identified in many other ways. Computerized biometrics identification systems examine a particular trait and use that information to decide whether the user may enter a building, unlock a computer, or access system information.

Biometric devices use some type of data input device, such as a video camera, retinal scanner, or microphone, to collect information that is unique to the individual. A digitized representation of a user's biometric characteristic (fingerprint, voice, etc.) is used in the authentication process. This type of authentication is virtually spoof-proof and is never misplaced. The data are relatively static but not necessarily secret. The advantage of this authentication process is that it provides the correct data to the input devices.

(i) Fingerprint Scan

The individual places a finger in or on a reader that scans the finger, digitizes the fingerprint, and compares it against a stored fingerprint image in the file. This method can be used to verify the identity of individuals or compare information against a data base covering many individuals for recognition. Performance:

False rejection rate = 9.4%
False acceptance rate = 0
Average processing time = 7 seconds

(ii) Retinal Scan

This device requires that the user look into an eyepiece that laser-scans the pattern of the blood vessels. The patterns are compared to provide positive identification. It costs approximately Rs. 1,27,200. Performance:

False rejection rate = 1.5%
False acceptance rate = 1.5%
Average processing time = 7 seconds

(iii) Palm Scan

The system scans 10,000 points of information from a 2-inch-square area of the human palm. With the information, the system identifies the person as an impostor or authentic. The typical price is approximately Rs. 1,20,000. Performance:

False rejection rate = 0
False acceptance rate = 0.00025%
Average processing time = 2-3 seconds

(iv) Hand Geometry

This device uses three-dimensional hand geometry measurements to provide identification. The typical price is approximately Rs. 1,03,200. Performance:

False rejection rate = 0.1%
False acceptance rate = 0.1%
Average processing time = 2 to 3 seconds

(v) Facial Recognition

Using a camera mounted at the authentication place (gate, monitor, etc.) the device compares the image of the person seeking entry with the stored image of the authorized user indexed to the system. The typical price is approximately Rs. 1,20,000. Performance:

Average processing time = 2 seconds

(vi) Voice Verification

When a person speaks a specified phrase into a microphone, this device analyzes the voice pattern and compares it against a stored data base. The price can run as high as Rs. 5,76,000 for 3,000 users. Performance:

False rejection rate = 8.2%
False acceptance rate = 0.4%
Average processing time = 2 to 3 seconds (response time is calculated after the password or phrase is actually spoken into the voice verification system).

Physical and Technical Controls

Motion detectors

Surveillance Devices

Installing fences does not provide the necessary level of protection a company needs to protect its facility, equipment, and employees. Areas need to be under surveillance so that improper actions are noticed and taken care of before damage occurs. Surveillance can happen through visual detection or through devices that use sophisticated means of detecting abnormal behavior or unwanted conditions. It is important that every organization have a proper mix of lighting, security personnel, IDSs, and surveillance technologies and techniques.

Closed-Circuit TV (CCTV)

A closed-circuit TV (CCTV) is a commonly used monitoring device in most organizations, but before purchasing and implementing a CCTV, you need to consider several items,

(i) Purpose of CCTV Detect, assess, and/or identify intruders
(ii) Type of environment the CCTV camera will work in Internal or external areas
(iii) Field of view that is required Large or small area that needs to be monitored
(iv) Amount of illumination of the environment Lit areas, unlit areas, areas affected by sunlight
(v) Integration with other security controls Guards, IDSs, alarm systems

CCTVs are made up of cameras, transmitters, receivers, a recording system, and a monitor. The camera captures the data and transmits it to a receiver, which allows for the data to be displayed on a monitor. This data is recorded so that it can be reviewed at a later time if needed. A CCTV sends the captured data from the camera's transmitter to the monitor's receiver, usually through a coaxial cable, instead of broadcasting the signals over a public network. This is where the term "closed-circuit" comes in. This circuit should be tamperproof, which means that an intruder cannot manipulate the video feed that the security guards are monitoring.

Intrusion Detection Systems

Surveillance techniques are used to watch for unusual behaviors, whereas intrusion detection devices are used to sense changes that take place in an environment. Both are monitoring methods, but they use different devices and approaches. IDSs are used to detect unauthorized entries and to alert a responsible entity to respond. These systems can monitor entries, doors, windows, devices, or removable coverings of equipment. Many work with magnetic contacts or vibration-detection devices that are sensitive to certain types of changes in the environment. When a change is detected, the IDS device sounds an alarm either in the local area, or in both the local area and to a remote police or guard station.

IDSs can be used to detect changes in the following,

(i) Beams of light
(ii) Sounds and vibrations
(iii) Motion
(iv) Different types of fields (microwave, ultrasonic, electrostatic)
(v) Electrical circuit

IDSs can be used to detect intruders by using electro-mechanical systems (magnetic switches, metallic foil in windows, pressure mats) or volumetric systems. Volumetric systems are more sensitive because they detect changes in subtle environmental characteristics, such as vibration, microwaves, ultrasonic frequencies, infrared values, and photoelectric changes.

Electro-mechanical systems work by detecting a change or break in a circuit. The electrical circuits can be strips of foil embedded or connected to windows. If the window breaks, the foil strip breaks, which sounds an alarm.

A **photoelectric system (or photometric system)** detects the change in a light beam and thus can be used only in windowless rooms. These systems work like photoelectric smoke detectors, which emit a beam that hits the receiver. If this beam of light is interrupted, an alarm sounds.

A **passive infrared system (PIR)** identifies the changes of heat waves in an area it is configured to monitor. If the particles' temperature within the air rise, it could be an indication of the presence of an intruder, so an alarm is sounded.

An **acoustical detection system** uses microphones that are installed on floors, walls, or ceilings. The goal is to detect any sound that is made during a forced entry. Although these systems are easily installed, they are very sensitive and cannot be used in areas that can be affected by the sounds of storms or traffic. **Vibration sensors** are very similar and are also implemented to detect forced entry. Financial institutions may choose to implement these types of sensors on exterior walls, where bank robbers may attempt to drive a vehicle through. They are also commonly used around the ceiling and flooring of vaults to detect someone trying to make an unauthorized bank withdrawal.

Wave-pattern motion detectors range in the frequency of waves that they monitor. The different frequencies are microwave, ultrasonic, and low frequency. All of these devices generate a wave pattern that is sent over a sensitive area and reflected back to a receiver. If the pattern is returned undisturbed, the device does nothing. If the pattern returns altered, because something in the room is moving, then an alarm sounds.

A **proximity detector or capacitance detector**, emits a measurable magnetic field. The detector monitors this magnetic field, and an alarm sounds if the field is disrupted. Capacitance change in an electrostatic field can be used to catch a bad guy, but first you need to understand what capacitance change means. An electrostatic IDS creates an electrostatic magnetic field, which is just an electric field associated with static electric charges. All objects have a static electric charge. All objects are made up of many subatomic particles, and when everything is stable and static, these particles make up one holistic electric charge. This means that there is a balance between the electric capacitance and inductance. Now if an intruder enters the area, his subatomic particles will mess up this lovely balance in the electrostatic field, causing a capacitance change, and an alarm will sound. So if you want to rob a company that uses these types of detectors, leave the subatomic particles that make up your body at home. The type of motion detector that a company chooses to implement, its power capacity, and its configurations dictate the number of detectors needed to cover a sensitive area. Also, the size and shape of the room and the items within the room may cause barriers, in which case more detectors would be needed to provide the necessary level of coverage.

IDSs are support mechanisms that are intended to detect and announce an attempted intrusion. They will not prevent or apprehend intruders, so they should be seen as an aid to the organization's security forces.

Perimeter Security

Perimeter security deals with facility access controls,

Facility access control

Access control needs to be enforced through physical and technical components when it comes to physical security. Physical access controls use mechanisms to identify individuals who are attempting to enter a facility or area. They make sure that the right individuals get in and the wrong individuals stay out, and provide an audit trail of these actions. Having personnel within sensitive areas is one of the best security controls because they can personally detect suspicious behavior. However, they need to be trained on what activity is considered suspicious and how to report such activity.

Access control points can be identified and classified as external, main, and secondary entrances. Personnel should enter and exit through a specific entry, deliveries should be made to a different entry, and sensitive areas should be restricted. Figure illustrates the different types of access control points into a facility.

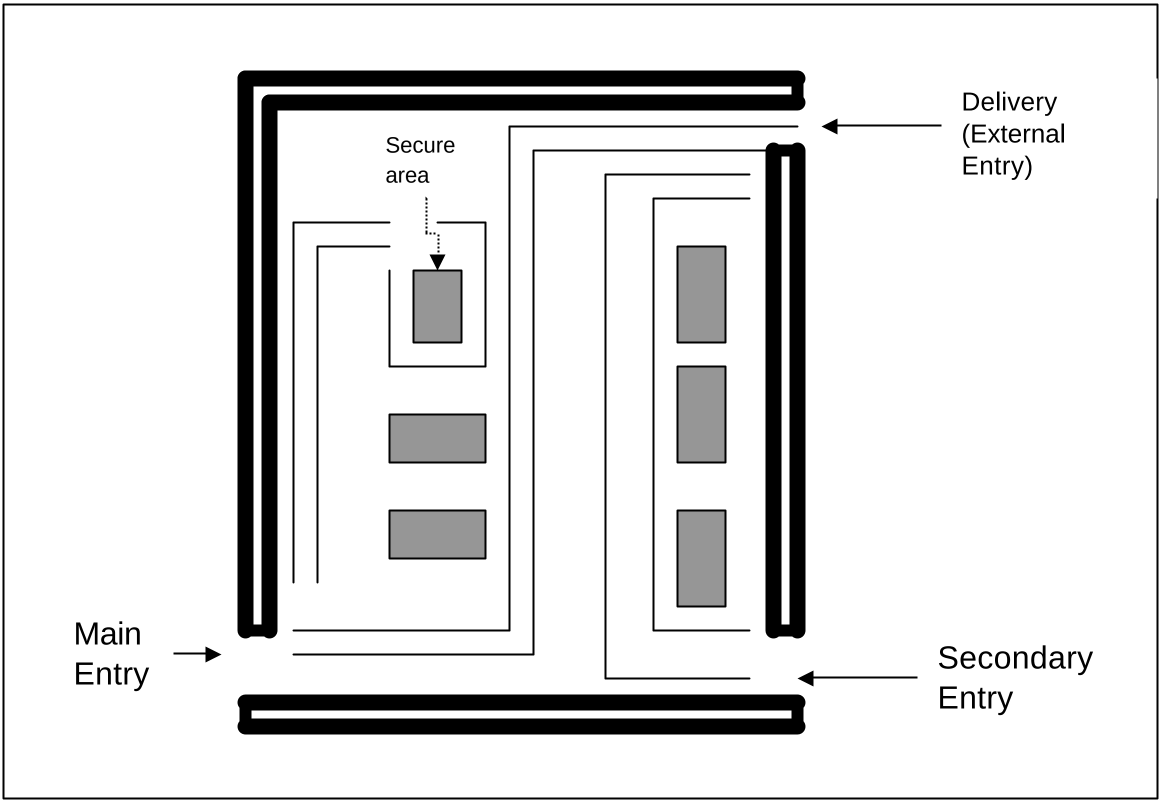


Figure: Access control points should be identified, marked, and monitored properly[6].

Locks

Locks are inexpensive access control mechanisms that are widely accepted and used. Locks are considered delaying devices to intruders. The longer it takes to break or pick a lock, the longer a security guard or police officer has to arrive on the scene if the intruder has been detected. Almost any type of a door can be equipped with a lock, but keys can be easily lost and duplicated, and locks can be picked or broken. If a company depends solely on a lock-and-key mechanism for protection, an individual who has the key can come and go as he likes without control and can remove items from the premises without detection. Locks should be used as part of the protection scheme, but should not be the sole protection scheme. Locks vary in functionality. Locks come in all types and sizes. It is important to have the right type of lock so that it provides the correct level of protection.

[6] All in one CISSP by Shon Harris

Mechanical Locks There are two main types of mechanical locks, the warded lock and the tumbler lock. The **warded lock** is the basic padlock, as shown in figure below.

`

Warded lock[7]

It has a spring-loaded bolt with a notch cut in it. The key fits into this notch and slides the bolt from the locked to the unlocked position. The lock has wards in it, which are metal projections around the keyhole.

The **tumbler lock** has more pieces and parts than a ward lock. The tumbler lock has more pieces and parts than a ward lock. the key fits into a cylinder, which raises the lock metal pieces to the correct height so that the bolt can slide to the locked or unlocked position. Once all of the metal pieces are at the correct level, then the internal bolt can be turned. The correct key has the correct size and sequences of notches to move these metal pieces into their correct position. The three types of tumbler locks are the pin tumbler, wafer tumbler, and lever tumbler. The **pin tumbler lock**, is the most commonly used tumbler lock. The key has to have just the right grooves to put all the spring-loaded pins in the right position so that the lock can be locked or unlocked.

Wafer tumbler locks (also called disc tumbler locks) are the small, round locks that you usually see on file cabinets. They use flat discs (wafers) instead of pins inside the locks. They often are used as car and desk locks. This type of lock does not provide much protection because it can be easily circumvented.

Combination locks, of course, require the correct combination of numbers to unlock them. These locks have internal wheels that have to line up properly before being unlocked. A user spins the lock interface left and right by so many clicks, which lines up the internal wheels. Once the correct turns have taken

[7] All in one CISSP by Shon Harris

place, all the wheels are in the right position for the lock to release and open the door.

Cipher locks, also known as programmable locks, are keyless and use keypads to control access into an area or facility. The lock requires a specific combination to be entered into the keypad and possibly a swipe card. They cost more than traditional locks. Compared to traditional locks, cipher locks can provide a much higher level of security and control of who can access a facility.

Electronic combination lock[8]

The following are some functionalities commonly available on many cipher combination locks that improve the performance of access control and provide for increased security levels:

(i) **Door delay** If a door is held open for a given time, an alarm will trigger to alert personnel of suspicious activity.

(ii) **Key override** A specific combination can be programmed to be used in emergency situations to override normal procedures or for supervisory overrides.

(iii) **Master keying** Enables supervisory personnel to change access codes and other features of the cipher lock.

Hostage alarm If an individual is under duress and/or held hostage, a combination he enters can communicate this situation to the guard station and/or police station.

[8] All in CISSP by Shon Harris

Environmental Issues

Improper environmental controls can cause damage to services, hardware, and lives. Interruption of some services can cause unpredicted and unfortunate results. Power, heating, ventilation, air-conditioning, and air-quality controls can be complex and contain many variables. They all need to be operating properly and be monitored regularly.

Most electronic equipment must operate in a climate-controlled atmosphere. Although it is important to keep the atmosphere at a proper working temperature, it is important to understand that the components within the equipment can suffer from overheating even in a climate-controlled atmosphere if the internal computer fans are not cleaned or are blocked. When devices are overheated, the components can expand and contract, which causes components to change their electronic characteristics, reducing their effectiveness or damaging the system overall.

In more humid climates, or during the summer, more humidity is in the air, which can also affect components. Particles of silver can begin to move away from connectors onto copper circuits, which cement the connectors into their sockets. This can adversely affect the electrical efficiency of the connection. A **hygrometer** is usually used to monitor humidity. It can be manually read, or an automatic alarm can be set up to go off if the humidity passes a set threshold. Lower temperatures can cause mechanisms to slow or stop, and higher temperatures can cause devices to use too much fan power and eventually shut down.

Ventilation

Air ventilation has several requirements that must be met to ensure a safe and comfortable environment. A closed-loop recirculating air-conditioning system should be installed to maintain air quality. “Closed-loop” means that the air within the building is reused after it has been properly filtered, instead of bringing outside air in. The assessment team needs to understand the various types of contaminants, how they can enter an environment, the damage they could cause, and the steps to ensure that a facility is protected from dangerous substances or high levels of average contaminants. Airborne material and particle concentrations must be monitored for inappropriate levels. Dust can affect a device’s functionality by clogging up the fan that is supposed to be cooling the device. Excessive concentrations of certain gases can accelerate corrosion and cause performance issues or failure of electronic devices. Although most disk drives are hermetically sealed, other storage devices can be affected by airborne contaminants. Air-quality devices and ventilation systems deal with these issues.

Fire Prevention, Detection and Suppression

Fire prevention includes training employees on how to react properly when faced with a fire, supplying the right equipment and ensuring that it is in working order, making sure there is an easily reachable fire suppression supply, and storing combustible elements in the proper manner. Fire prevention may also include using proper noncombustible construction materials and designing the facility with containment measures that provide barriers to minimize the spread of fire and smoke.

Fire detection response systems come in many different forms. Manual detection response systems are the red pull boxes that you see on many walls in many buildings. Automatic detection response systems have sensors that react when they detect the presence of fire or smoke.

Fire suppression is the use of a suppression agent to put out a fire. Fire suppression can take place manually through handheld portable exstinguishers, or automatically through automated systems such as sprinkler systems, or halon or CO2 discharge systems.

Fire protection processes should consist of implementing early smoke or fire detection devices and shutting down systems until the source of the heat is eliminated. A warning signal may be sounded by a smoke or fire detector before the suppression agent is released, so that if it is a false alarm or a small fire that can be handled without the automated suppression system, someone has time to shut down the suppression system. Table shows four types of fire and their suppression methods

Fire Class	**Type of Fire**	**Elements of Fire**	**Suppression Method**
A	Common combustibles	Wood products, paper, and laminates	Water, foam
B	Liquid	Petroleum products and coolants	Gas, CO2, foam, dry powders

Fire Class	**Type of Fire**	**Elements of Fire**	**Suppression Method**
C	Electrical	Electrical equipment and wires	Gas, CO2, dry powders
D	Combustible metals	Magnesium, sodium, potassium	Dry powder

Halon: Halon is a gas that was widely used in the past to suppress fires because it interferes with the chemical combustion of the elements within a fire. It mixes quickly with the air and does not cause harm to computer systems and other data processing devices. It was used mainly in data centers and server rooms. It was discovered that halon has chemicals (chlorofluorocarbons) that deplete the ozone and that concentrations greater than 10 percent are dangerous to people. Halon used on extremely hot fires degrades into toxic chemicals, which is even more dangerous to humans. Some really smart people figured that the ozone was important to keep around, which caused halon to be federally restricted, and no companies are allowed to purchase and install new halon extinguishers. Companies that still have halon systems have been instructed to replace them with nontoxic extinguishers. The following are EPA-approved replacements for halon:

(i) FM-200
(ii) NAF-S-III
(iii) CEA-410
(iv) FE-13
(v) Water
(vi) Inergen
(vii) Argon
(viii) Argonite

Water Sprinklers

Water sprinklers typically are simpler and less expensive than halon and FM-200 systems but can cause water damage. In an electrical fire, the water can increase the intensity of the fire, because it can work as conductor for electricity—only making the situation worse. If water is going to be used in any type of environment with electrical equipment, the electricity must be turned off before the water is released. Sensors should be used to shut down the electric power before water sprinklers activate. Each sprinkler head should activate individually to avoid wide-area damage, and there should be shutoff valves so that the water supply can be stopped if necessary. A company needs to take great care in deciding which suppression agent and system is best for it. Four main types of water sprinkler systems are available: wet pipe, dry pipe, preaction and deluge.

Wet Pipe

Wet pipe systems always contain water in the pipes and are usually discharged by temperature control level sensors. One disadvantage of wet pipe systems is that the water in the pipes may freeze in colder climates. Also, if there is a nozzle or pipe break, it can cause extensive water damage. These types of systems are also called closed head systems.

Dry Pipe In dry pipe systems, the water is not actually held in the pipes. The water is contained in a “holding tank” until it is released. The pipes contain pressurized air, which is reduced when a fire or smoke alarm is activated, allowing the water valve to be opened by the water pressure. Water is not allowed into the pipes that feed the sprinklers until an actual fire is detected. First, a heat or smoke sensor is activated; then, the water fills the pipes leading to the sprinkler heads, the fire alarm sounds, the electric power supply is disconnected, and finally water is allowed to flow from the sprinklers. These pipes are best used in colder climates because the pipes will not freeze.

Preaction

Preaction systems are similar to dry pipe systems in that the water is not held in the pipes but is released when the pressurized air within the pipes is reduced. Once this happens, the pipes are filled with water, but it is not released right away. A thermal-fusible link on the sprinkler head has to melt before the water is released. The purpose of combining these two techniques is to give people more time to respond to false alarms or to small fires that can be handled by other means. Putting out a small fire with a handheld extinguisher is better than losing a lot of electrical equipment to water damage. These systems are usually used only in data processing environments rather than the whole building, because of the higher cost of these types of systems.

Deluge A deluge system has its sprinkler heads wide open to allow a larger volume of water to be released in a shorter period. Because the water being released is in such large volume, these systems are usually not used in data processing environments.

External Boundary Protection Mechanisms

Following control types are used in ensuring this mechanism:

Physical barriers Fences, gates, walls, doors, windows, protected vents, vehicular barriers

Fencing

Fencing can be quite an effective physical barrier. Although the presence of a fence may only delay dedicated intruders in their access attempts, it can work as a psychological deterrent by telling the world that your company is serious about protecting itself. Fencing can provide crowd control and helps control access to entrances and facilities. However, fencing can be costly and unsightly. Fences come in varying heights, and each height provides a different level of security,

(i) Fences three to four feet high only deter casual trespassers.
(ii) Fences six to seven feet high are considered too high to climb easily.
(iii) Fences eight feet high (possibly with strands of barbed or razor wire at the top)

Bollards

Bollards usually look like small concrete pillars outside a building. Sometimes companies try to dress them up by putting flowers or lights in them to soften the look of a protected building. They are placed by the sides of buildings that have the most immediate threat of someone driving a vehicle through the exterior wall. They are usually placed between the facility and a parking lot and/or between the facility and a road that runs close to an exterior wall. Within the United States after September 11, 2001, many military and government institutions, which did not have bollards, hauled in huge boulders to surround and protect sensitive buildings. They provided the same type of protection that bollards would provide. These were not overly attractive but provided the sense that the government was serious about protecting those facilities.

6.4 MICROCOMPUTER PHYSICAL SECURITY

Today’s portable computing environment can take on a variety of forms: from remote connectivity to the home office to remote computing on a standalone microcomputer with desktop capabilities and storage. Both of these portable computing methods have environment-specific threats as well as common threats that require specific protective measures.

Portable Computing Threats

Portable computing is inherently risky. Just the fact that company data or remote access is being used outside the normal physical protections of the office introduces the risk of exposure, loss, theft, or data destruction more readily than if the data or access methods were always used in the office environment.

Data Disclosure

Simple techniques as observing a user's remote access to the home can disclose a company's dial-up access phone number, user account, password, or log-on procedures; this can create a significant threat to any organization that allows remote dial-up access to its networks or systems from off-site. Dial-up access is becoming more vulnerable to data disclosure because remote users can now use cellular communications to perform dial-up access from laptop computers. The concern in a wireless data communication link is the threat of unauthorized data interception, especially if the wireless connection is the user's sole method of communication to the organization's computing resources. All of these remote connectivity methods introduce the threat of data exposure.

Data Loss and Destruction

Security controls must also provide protection against the loss and destruction of data. Such loss can result from user error (e.g., laptop computers may be forgotten in a cab or restaurant) or other cause (e.g., lost baggage). Other forms of data loss include outright theft of disks, copying of hard disk data, or loss of the entire unit. In today's competitive business world, it is not uncommon to hear of rival businesses or governments using intelligence-gathering techniques to gain an edge over their rivals.

Threats to Data Integrity

Data integrity in a portable computing environment can be affected by direct or indirect threats, such as virus attacks. Direct attacks can occur from an unauthorized user changing data while outside the main facility on a portable user's system or disk. Data corruption or destruction due to a virus is far more likely in a portable environment because the user is operating outside the physical protection of the office.

Protection Strategies

After the decision has been made to allow portable computing with certain use restrictions, the challenge is to establish sound policies and protection strategies against the known threats of this computing environment.

User Validation Protection

The protection strategy should reflect the types of portable computing to be supported. If remote access to the company's host computers and networks is part of the portable computing capabilities, then strict attention should be paid to implementing a high-level remote access validation architecture. This may include use of random password generation devices, challenge/response authentication techniques, time-synchronized password generation, and biometric user identification methods. Remote access users are registered with a specific device; when accessing the system, they are sent a random challenge number. Users must decrypt this challenge using the token's algorithm and provide the proper response back to the host system to prove their identity. Another type of high-level validation is biometric identification, such as thumb print scanning on a hardware device at the remote user site, voice verification, and keyboard dynamics, in which the keystroke timing is figured into the algorithm for unique identification. The portable computer user validation from off-site should operate in conjunction with the network security firewall implementation.

Data Disclosure Protection

If standalone computers are used in a portable or mobile mode outside of the company facility, consideration should be given to requiring some form of password user identification on the individual unit itself. Various software products can be used to provide workstation-level security. Other techniques for controlling access to portables include physical security devices on portable computers. Physical security locks for portables are a common option. One workstation security software product includes a physical disk lock that inserts into the diskette drive and locks to prevent disk boot-ups that might attempt to override hard-disk-resident software protections. If the primary objective is protection of data during remote transmission, then a strategy mandating encryption of the file before it is transmitted should be put in place. Portable computer hardware is also available that can provide complete encryption of all data and processes on a portable computer. The encryption technology is built into the system itself, though this adds to the expense of each unit.

Virus protection in a portable environment

All portable or off-site computers targeted to process company data must have some consistent form of virus protection. This is a very important consideration when negotiating a site license for virus software. What should be negotiated is not a site license per se, but rather a use license for company's users, wherever they may process company data. The license should include employees' home computers and as well as company-owned portables. If this concept isn't acceptable to a virus software vendor, then procedures must be established in which all data that have left the company and may have been processed on a nonvirus-protected computer must be scanned before it can reenter the company's internal computing environment. This can be facilitated by issuing special color-coded diskettes for storing data that are used on portables or users' home computers. By providing the portable computer users with these disks for storage and transfer of their data and mandating the scanning of these disks and data on a regular basis on-site, the threat of externally contracted computer viruses can be greatly reduced.

Controlling Data Dissemination

Accumulation of data on portable computers creates the potential for its disclosure. This is easily addressed by implementing a variety of procedures intended to provide checks against this accumulation of data on shared portable computers. A user procedure should be mandated to remove and delete all data files from the hard disk of the portable computer before returning it to the company loan pool. The hardware loaning organization should also be required to check disk contents for user files before reissuing the system.

Theft Protection

The threat of theft can be in the form of illicit copying of files from a user's computer when unattended, such as checked baggage or when left in a hotel room. The simplest method is to never store data on the hard disk and to secure the data on physically secured diskettes. Another method is to never leave the portable in an operational mode when unattended. The batteries and power supply can be removed and locked up separately so that the system itself is not functional and thus information stored on the hard disk is protected from theft. These measures can help protect against the loss of data, which might go unnoticed. To protect against physical theft, something as simple as a cable ski lock on the unit can be an effective protection mechanism.

User Education

The selection of portable computing protection strategies must be clearly communicated to portable computer users by means of a thorough user education process. Education should be mandatory and recurring to assure the most current procedures, tools, and information are provided to portable users. In the area of remote access to on-site company resources, such contact should be initiated when remote users register in the remote access authentication system.

For the use of shared company portable computers, this should be incorporated with the computer check-out process; portable computer use procedures can be distributed when systems are checked out and agreed to by prospective users. With respect to the use of noncompany computers in a portable mode, the best method of accountability is a general user notice that security guidelines apply to this mode of computing. This notification could be referenced in an employee nondisclosure agreement, in which employees are notified of their responsibility to protect company data, on-site or off-site. In addition to registering all portable users, there should be a process to revalidate users in order to maintain their authorized use of portable computing resources on a regular basis. The registration process and procedures should be part of overall user education on the risks of portable computing, protection mechanisms, and user responsibilities for supporting these procedures.

Summary

Every organization should develop, implement, and maintain a physical security program that contains the following control categories: deterrence, delay, detection, assessment, and response. It is up to the organization to determine its acceptable risk level and the specific controls that are required to fulfill the responsibility of each category. Physical security is not often thought about when people think of organizational security and company asset protection, but real threats and risks need to be addressed and planned for. Who cares if a hacker can get through an open port on the web server if the building is in flames!.

The use of portable computing presents very specific data security threats. For every potential threat, some countermeasure should be implemented to ensure the company's proprietary information is protected. This involves identifying the potential threats and implementing the level of protection needed to minimize these threats. By providing a reasonably secure portable computing environment, users can enjoy the benefits of portable computing and the organization can remain competitive in the commercial marketplace.

CHAPTER 7

SECURITY MANAGEMENT PRACTICES & RISK ANALYSIS

7.1 INTRODUCTION

The information security management system (ISMS) is a management system in order to protect the information of an organization. It works on PDCA (Plan, Do Check, and Act) model, which is to establish, implement and operate, monitor and review, maintain and improve the ISMS. Managing the security can be difficult task to understand for the most of information security professionals. It is a median between understanding what should be protected and why those protections are important. Using basic principles and risk analysis as a tool, policies can be created to implement a security management system.

This management system should also understand how standards and guidelines also play a important role in creating procedures. While doing this, role of every user and responsibility associated with him should be accounted for understanding how to protect the organization's information assets.

Data always play an important role for the information assets of an organization, which cannot be minimized. Data is lifeblood for the organizations, but it is the asset that is the most vulnerable. Protecting this asset means understanding various mechanisms to make it less vulnerable as well as to protect critical assets fully.

7.2 OBJECTIVES OF SECURITY MANAGEMENT PRACTICES

The objective of security control policy is to reduce vulnerabilities to a tolerable level and to minimize the effects of threats. To achieve this, the organization must determine the impact that a threat might have on an organization and the likelihood that the loss could occur. The process that analyzes the various threats scenarios and produces a representative value for the estimated potential loss is constituted in the Risk Assessment.

A policy is one of those terms that can mean several things. For example, there are security policies on firewalls, which refer to the access control and routing list information. Standards, procedures, and guidelines are also referred to as policies in the larger sense of an information security policy.

A good well-written policy is more than an exercise created on white paper; it is an essential and fundamental element of sound security practice. A policy for example, can literally be a lifesaver during a disaster or might be a requirement of governmental or regulatory function. A policy can also provide protection from liability due to an employee's actions, or it can control access trade secrets

The four main objectives of security management practices are
(i) Policy
(ii) Standard
(iii) Baseline
(iv) Guideline
(v) Procedure

Information Security Policies

Information Security policies are the plans that states the objective of the procedures. Policies are different from guidelines and or standards; it describes the security in general terms, not specifics. Procedures are not the parts of policies. Procedures are implementation details; a policy is a statement of the goals to be achieved by procedures. General terms are used to describe security policies so that the policy does not get in the way of the implementation. For example, if the policy specifies a single vendor's solution for a single sign up, it will limit the company's ability to use an upgrade or a new product. Although the policy documents might require the documentation of the implementation, these implementation notes should not be part of the policy.

Specifications

Policies do not discuss the implementation process of the security; accurately defining what is to be protected ensures that proper control is implemented. It is the policies, which describes what is being protected and what limitations should be put on those controls.

How to write Policies

The objective of policies must be determined before to write the policy documents. In any case, the first step is to determine what is being protected and why it is being protected. Policies can be written to affect hardware, software, access, human resource, networks, telecommunications, enforcement, and so on. Before we begin the writing process, it should be given a consideration that which systems and processes are important to the company's mission. This will help to determine what and how many policies are necessary to complete the mission.

Defining the policies need to be written

Information security policies do not have to be a single document. This should be divided into parts. By doing so they are easier to understand, easier to distribute and easier to provide individual training because each policy has its own section. Smaller sections are also easier to modify and update. How many policies should be written? It is ok to have a policy for email that is separate from one for Internet usage. It is not a problem to have a policy for antivirus protection and a separate policy for Internet usage.

Identify what is to be protected

Computers are the means for processing the company's intellectual property that the disks are for storing that property, and that the networks are for allowing that information to flow through the various business processes. The following is an example of what can be inventoried:

(i) Human Resource Assets
(ii) Software Assets
(iii) Physical Assets
(iv) Paper Assets
(v) Electronic Assets
(vi) Service Assets

It is important to have a complete inventory of the information assets supporting the business processes. The best way to create this list is to perform a risk assessment inventory. There should be a list of documentation on programs, hardware, systems, local administrative processes, and other documentation that describes any aspect of the technical business process. These documents can contain information regarding how the business works and can show areas that can be attacked. The business processes can be affected by industrial espionage as well as hackers and disgruntled employees.

The most important and expensive of all resources are the human resources who operate and maintain the items inventoried. Performing an inventory of the people involved with the operations and use of the systems, data, and non computer resources provides insight into which policies are necessary.

Creating an inventory of people can be as simple as creating a typical organizational chart of the company. This can be burdensome however, if thousand of people are being included or even a few hundred, people in one document. Moreover, organizational charts are notoriously rigid and do not assume change or growth. The inventory, then, could include the type of job performed by a department, along with the level of those employees' access to the enterprise's data.

Identify from whom it is protected

Defining access control policy is an exercise in understanding how each system and network component is accessed. A network might have a system to support network-based authentication and another supporting intranet-like services, but are all the systems accessed like this? How is data accessed amongst systems? By understanding how information resources are accessed, you should be able to identify on whom your policies should concentrate.

Some considerations for data access are:

a. Authorized and unauthorized access to resources and information
b. Unintended or unauthorized disclosure of information
c. Enforcement procedures

Primarily, the focus should be on who can access resources and under what conditions. This is the type of information that can be provided during a risk assessment of the assets. The risk assessment then determines which considerations are possible for each asset. From that list, policies can then be written to justify their use.

Setting Standards

When creating policies for an established organization, there is an existing process for maintaining the security of the assets. These policies are used as drivers for the policies. For other policies in which there are no technology drivers, standards can be used to establish the analysts' mandatory mechanisms for implementing the policy.
Regardless of how the standards are established, by setting standards, policies that are difficult to implement or that affect the entire organization are guaranteed to work in your environment. Even for small organizations, if the access policies require one-time-use passwords, the standard for using a particular token device can make interoperability a relative certainty.

Creating Baselines

Baselines are used to create a minimum level of security necessary to meet policy requirements. Baselines can be configurations, architectures, or procedures that might or might not reflect the business process but that can be adapted to meet those requirements. One can use these baselines as an abstraction to develop standards.

Most baselines are specific to the system or configuration they represent, such as a configuration that allows only Web services through a firewall. However, like most baselines, this represents a minimum standard that can be changed if the business process requires it. One example is to change the configuration to allow a VPN client to access network resources.

Guidelines

Standards and baselines describe specific products, configurations, or other mechanisms to secure the systems. Sometimes security cannot be described as a standard or set as a baseline, but some guidance is necessary. These are areas where recommendations are created as guidelines to the user community as a reference to proper security. For example, your policy might require a risk analysis every year. Rather than require specific procedures to perform this audit, a guideline can specify the methodology that is to be used, leaving the audit team to work with management to fill in the details.

Setting and Implementing Procedures

Procedures describe exactly how to use the standards and guidelines to implement the countermeasures that support the policy. These procedures can be used to describe everything from the configuration of operating systems, databases, and network hardware to how to add new users, systems, and software.

Procedures are written to support the implementation of the policies. Because policies change between organizations, defining which procedures must be written is impossible. For example, if your organization does not perform software development, procedures for testing and quality assurance are unnecessary. However, some types of procedures might be common amongst networked systems, including

a. **Auditing**: These procedures can include what to audit, how to maintain audit logs, and the goals of what is being audited.

b. **Administrative**: These procedures can be used to have a separation of duties among the people charged with operating and monitoring the systems. These procedures are where you can show that database administrators should not be watching the firewall logs.

c. **Access control**: Access control policy should be clearly defined for the all employees. Access control includes both physical and logical access. Access controls rules should be clearly documented.

d. **Configuration**: These procedures cover the firewalls, routers, switches, and operating systems.

e. **Incident response**: These procedures cover everything from detection to how to respond to the incident. These procedures should discuss how to involve management in the response as well as when to involve law enforcement. If any disaster takes place this should be reported to management immediately.

f. **Physical and environmental**: These procedures cover not only the air conditioning and other environmental controls in rooms where servers and other equipment are stored, but also the protection of Ethernet cables to prevent them from being tapped. Also this should include the physical entry control of the personals.

7.3 PRINCIPAL OF RISK MANAGEMENT

Introduction

In this information age, information is the most valuable asset for every organization as today everything is moving from paper to digital format. In this modern era the whole business activities are being made through the transmission of information. Thus information of the organizations are under threat from various sources, these can be internal, external, and accidental or malicious. ISMS is a systematic approach to manage the commercially sensitive information of the organization. It covers all aspects of an IT system.

Risk management is the process which involves identifying, controlling and minimizing or eliminating the security risks. A responsible organization will assess the risk to its identified information assets, make decisions about which risks are intolerable and therefore need to be controlled, and manage the residual risks through carefully considered policies, procedure and controls. An organization must fully understand the security risks, it faces in order to determine the appropriate management action and to implement controls selected to protect against these risks.

Approaches to Risk Assessment

It is up to the organization to select the appropriate approach for the risk assessment, so this section describes the different options for an organization-wide risk approach for risk assessment.

The different approaches vary in the time and effort involved and the depth of detailed explored. Despite of the fact that the organization is free to choose the risk assessment approach. It needs to be ensured that the risk assessment method(s) applied are suitable and detailed enough for the organization’s business and security requirements.

If for example an organization or the ISMS and its assets have at most low to medium security requirements, a Basic Risk Assessment Approach might be sufficient. If the security requirements are higher, requiring more detailed and special assessment, then a Detailed Risk Assessment Approach may be necessary. In any case it should be ensured that the chosen approach fulfils all criteria, namely:

(i) Identify the assets and owners of these assets.

(ii) Identifying the threats and vulnerabilities, and any other applicable security requirements.

(iii) Identifying the impacts of losses of confidentiality. Integrity and availability might have on the assets.

(iv) Based on this information, assessing the harm and the likely hood of risks occurring, and the estimating the levels of risk.

(v) Identifying the most appropriate risk treatment option.

(vi) Select control objectives and controls to reduce the risks to an acceptable level.

Risk assessments, whether they pertain to information security or other types of risk, are a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk. For example, bank officials have conducted risk assessments to manage the risk of default associated with their loan portfolios and nuclear power plant engineers have conducted such assessments to manage risks to public health and safety. As reliance on computer systems and electronic data has grown, information security risk has joined the array of risks that governments and businesses must manage.

Regardless of the types of risk being considered, all risk assessments generally include the following elements:

(i) Identifying threats that could harm and, thus, adversely affect critical operations and assets. Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters.

(ii) Estimating the likelihood that such threats will materialize based on historical information and judgment of knowledgeable individuals.

(iii) Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize in order to determine which operations and assets are the most important.

(iv) Estimating, for the most critical and sensitive assets and operations, the potential losses or damage that could occur if a threat materializes, including recovery costs.

(v) Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organizational policies and procedures as well as technical or physical controls.

(vi) Documenting the results and developing an action plan.

Models and Methods for Assessing Risk

There are various models and methods for assessing risk, and the extent of an analysis and the resources expended can vary depending on the scope of the assessment and the availability of reliable data on risk factors. In addition, the availability of data can affect the extent to which risk assessment results can be reliably quantified.

(1) Qualitative Risk Analysis

Qualitative risk analysis is the process of performing a qualitative analysis of identified risks. This process is intended to prioritize risks according to their potential effect on project objectives. Qualitative risk analysis is one way of determining the importance of addressing specific risks and guides risk response measures. The time-criticality of risk-related actions may magnify the importance of a risk. An evaluation of the quality of the available information also helps modify the assessment of the risk. Qualitative risk Analysis requires that the probability and impact of the risks be estimated using qualitative analysis methods and tools. Using these tools helps correct biases that are often present in a project plan. Qualitative risk analysis should be revisited during the project's life cycle to stay current with changes in project risks.

(2) Quantitative Risk Analysis

The quantitative risk analysis process aims to analyze numerically the probability of each risk and of its impact on project objectives, as well as the extent of overall project risk. This process uses techniques such as Monte Carlo simulation and decision analysis to:

(i) Determine the probability of not achieving a specific project objective.
(ii) Quantify the risk exposure for the project and determine the size of cost and schedule contingency reserves that may be needed.
(iii) Identify risks requiring the most attention by quantifying their relative contribution to project risk.
(iv) Identify realistic and achievable cost, schedule or scope targets.

Quantitative risk analysis generally follows qualitative risk analysis. It requires risk identification. The qualitative and quantitative risk analysis processes can be performed separately or together. Considerations of time and budget availability, and the need for qualitative or quantitative statements about risk and impacts will determine which method(s) to use.

A **QUANTITATIVE APPROACH** generally estimates the monetary cost of risk and risk reduction techniques based on:

(i) the likelihood that a damaging event will occur,
(ii) the costs of potential losses and
(iii) the costs of mitigating actions that could be taken.

When reliable data on likelihood and costs are not available**; a *QUALITATIVE APPROACH* can be taken by defining risk in more subjective and general terms such as high, medium and low**. In this regard, qualitative assessments depend more on the expertise, experience, and judgment of those conducting the assessment. It is also possible to use a combination of quantitative and qualitative methods.

The Basic approach involves the selection of asset of security controls based on a simple and straightforward application of the processes.

This approach enables an organization to establish its ISMS by achieving a basic level of protection, based on the identification and assessment of the basic and essential needs requirements of the organization. The basic level of security achieved, using this straightforward and easy to use approach may be suitable for far apart of an organization with low security requirements, or in some cases, even for the whole organization if its security requirements are sufficiently low.

A typical example of the use of this approach might be part of an organization whose business operations are not very complex and whose dependency on information processing and e-working is not that extensive. This might also be the case with some business, however, there may be businesses whose business environment is more complex and they are dependent on extensive use of commercially sensitive information. This is basic risk assessment approach involves the following activities taking into account the security requirements from all sources.

Risk Assessment and Management Tasks Basic Assessment Activities

(i) Asset identification and valuation.
(ii) List those assets those associated with the business environment, operation and information being assessed within the scope of the ISMS, and identify their values, using a simple valuation scale.
(iii) Identification and Assessment of Security requirements
(iv) The security requirements should be identified (this can be supported by the use of checklists of generalized or commonly known threats and vulnerabilities),all identified security requirements should be valued, using a simple valuation scale
(v) Risk calculation. Calculate the risks, based on the information on assets and security requirements, using simple calculation scheme.

(vi) Identification & evaluation of the risk

(vii) Treatment options

(viii) Identify suitable risk treatment action for each of the identified risks, document the results for the risk treatment plan.

(ix) Selection of security controls and risk

(x) Reduction and Acceptance

Using list of generalized or commonly known threats and vulnerabilities can help to guide and direct the thinking process behind the assessment activities. An approach could involve, for example, two levels of security requirements (e.g. high & low), and evaluation of assets using a predefined scale e.g. values- Very High, Low, Medium Value and low or by using numbers 1to 9.

The risk measures can be used to decide what risks should be dealt with first and need the most attention, what the appropriate risk treatment options might be. For those risks where the option of risk reductions chosen, an acceptable level of risks needs to be identified that is suitable to the business and security requirements for the ISMS considered.

There are a number of **advantages** with the Basic Risk assessment approach, such as:

(i) Minimum of resources is needed for risk assessment, and their time and effort spent on control selection is reduced.

(ii) Normally, no significant resources are needed to identify appropriate controls

(iii) The same or similar controls can be adopted for several assets without great effort.

(iv) If a large number of an organization's assets operate in a common environment, and if the business and security requirements are comparable, there controls may offer a const-effective solution.

The **disadvantage**s of this approach include:

(i) If the security level is set too high, there might be too expensive or too restrictive controls selected for some assets, and if the level is too low, the security implemented might be not be sufficient for some assets.

(ii) There might be difficulties in managing security relevant changes (as required in the 'check' and the 'Act' part of the PDCA model). For instance, if changes to the overall ISMS business occur, it might be difficult to assess whether the original controls are still sufficient.

Detailed risk assessment

This approach involves conducting detailed risk assessment, which include the detailed identification and valuation of assets, and identification and assessment of the levels of security requirements. This information is used to assess the risks and is subsequently used for the identification and selection of security controls.

The selection of these controls is justified by the identified risks to the assets, and it is ensured that the risks are reduced to the acceptable level, if this risk treatment option was chosen.

Detailed risk assessment can be a very resource intensive process, and therefore needs careful establishment of boundaries of the business environment, operations, information and assets within the scope of the ISMS to be assessed. It is also an approach that requires constant management attention.

According to the risks assessed, controls can be selected from ISO/IEC:17799 in relation to those control objectives that should be satisfied. This overall approach is different from the Basic Risk assessment approach that much more detailed analysis of the assets and the security requirements is carried out.

Risk Assessment and Management Tasks

(i) Asset identification and valuation

Identify and list all those assets associated with the business environment, operations and information within the scope of the ISMS, define a value scale and for each asset assign values from this scale (one value for each: confidentiality, integrity and availability, and any other value, if applicable).

(ii) Security Requirements Identification

Identify all security requirements (threats and vulnerabilities, legal and business requirements) associated with the list of assets within the scope of the ISMS.

(iii) Security requirements Assessment

Identify an appropriate valuation scale for the security requirements, and assign the appropriate value for each of the identified security requirements.

(iv) Calculation of risks:

Calculate the risk (based on the assets and security requirement's and their values resulting from the above assessment) by a method appropriate for the security requirements of the ISMS considered.

(v) Risk Formulae

Threats X Vulnerability X asset value = total risk
(Threats X Vulnerability X asset value) X controls gap = residual risk

Identification and Evaluation of Options

Treatment of Risks

Identify a suitable risk treatment action for each of the identified risks. Evaluate that the identified option is realistic, suitable and in line with all business and security requirements, and document the results for the risk treatment plan.

Selection of Security Controls, Reducing the Risks and Risk Acceptance

Determine their acceptable level of risk for their risk assessment methodology chosen, and ensure that this level of acceptable risk is appropriate for the business and security requirements of the ISMS considered. For those risks where their option of risk reduction was chosen, select, suitable control objectives and controls from ISO 27001 that will reduce these risks to an acceptable level.

Assess how much the controls selected reduce the identified risk

For each of those risks that cannot be reduced to the acceptable level, identify additional action to deal with it (either management approval to accept the risk for business reasons or to reduce it further).

The advantages of this approach are:

(i) An accurate and detailed view of the security risks is obtained leading to the identification of security levels which reflect the organization's security requirements of the assets and their ISMS.

(ii) The management of security relevant changes (as required in the 'Check' and the 'Act' part of the PDCA model) will benefit from the additional information obtained from a detailed risk assessment.

The disadvantage of this approach is:

It takes a considerable amount of time, effort and expertise to get viable results.

Combined Approach

This approach involves first identifying those assets within the scope of the ISMS which are potentially at high risk or critical to business operations. Based on these results, the assets with in the scope of the ISMS are categorized into, those which required a Detailed Risk Assessment approach to achieve appropriate protection and those for which the Basic Risk Assessment is sufficient.

This approach is a combination of the advantages of the approaches described earlier above. Consequently, it provides a good balance between minimizing the time and effort spent in identifying controls, while still ensuring that all of an organization's assets are assessed and protected appropriately.

In addition to having the combined **advantages** of the two approaches it also has the advantage that:

- Resources and money can be applied where they will be most beneficial, and an organization's information systems, which are likely to be high risk, can be addressed early.

The **Disadvantage** of this approach is:

- This may lead to inaccurate results if the identification of those information systems at high risk is incorrect, i.e. if systems for which a Detailed Risk Assessment is needed have been considered by only by a Basic Assessment approach.

Selections of a Suitable Risk Assessment/Management Approach

Selection Factors: As explained in the previous clauses of this section, there are different overall, organization-wide, approaches an organization can take to risk assessment. The previous clauses have indicated some of the advantages and disadvantages of these approaches.

Which approach is suitable for an organization is dependent on a number of factors, including:

(i) their business environment and the kind of business conducted

(ii) the dependency on information processing and applications supporting their business

(iii) the complexity of the business and supporting systems, applications and services

(iv) the number of trading partners and external business and contractual relationships.

These factors should be generally common to all business, therefore when selecting an appropriate organization-wide, approach an organization needs to consider these factors tighter with the advantages and disadvantages of the approaches. It is up to the organization to make the decision of which approach to take, as long as the criteria set out in ISO 27001 are satisfied.

As a rule of thumb the more important and essential is to the organization and for its business, and the more there is to loose, the more time and more resources be devoted to the security.

Risk Assessment and Businesses

There is no general rule that says which approach to risk assessment is suitable to each business since this decision is based on the business and information security requirements, and not necessarily on the organization. The following are some notes for business based on some general ideas of how business might relate to the factors given in above.

It is certainly the case that the less complex the business operations are and the fewer systems there are, the simpler the information security requirements might be, and this situation probably holds true for the majority of business.

However, there is some business whose business requirements could be quite involved. One business might be a supplier to many other organizations and there may be a contractual agreement to implement a range of ISO27001controls.

A business's dependency on the use of information processing and computing systems may be very high and their business may be highly reliant on the use of such systems. For examples, a company might use such systems to produce information products for the entertainment industry where the content and design has a high market value in terms of intellectual property.

A business needs to balance what resources it would need to devote to risk assessment in accordance with once of the three approaches and the implementation of security controls to meet its own security requirements and those of its customers. As a minimum an SME will need to implement some security controls, what ever their business is, and the basic Risk Assessment approach will enable them to establish what this should be. Certainly there is a need to have some from of security policy in place, to have some forms of access control and to be compliant with statutory and regulatory requirements. In addition, there may be a need to give special treatment to some specific requirements resulting from its business relationships, using some or all of a Detailed Risk Assessment approach, as described earlier.

Identify and Classify the Assets

We identified critical business processes and the IT systems, which support these critical business processes. Each IT system in turn comprises of various information assets, which are created by the organization to perform the business functions. These information assets utilize other critical components like software, hardware, physical and infrastructure facilities to perform designated task in an efficient and secure manner. Identification of all such information assets and critical components and maintaining an up-to-date record is essential to know what we intend to protect. Once we have this inventory, next step is to devise a scheme for classifying the assets, based on their criticality towards confidentiality, integrity and availability of information. This classification is necessary to implement various protection measures.

The assets are grouped under the following categories:

Information assets

(i) These are the assets, which have been created by the efforts of an organization and would be most difficult to replace. Examples are databases, documentations, procedures, plans, drawings, diagrams etc. These in turn will be stored on various types of media like paper, magnetic tapes, magnetic disc drives, optical discs and many other media which are becoming more and more compact in size and larger in capacity.

(ii) These critical assets should be carefully protected throughout their life, but their death should be final and irrevocable if the authorities order deletion. Removal or movement of a critical information asset needs to be thoroughly controlled. An information asset could be temporarily transformed from the data element in a database to an attachment of an email stored on the hard disk, to a printed copy of the email and finally as a fax document. The protection as well as deletion schemes should protect or delete the critical asset in all its forms, simultaneously and entirely.

Software assets

Application software, system software, development tools and utilities are part of these assets. Application software, which has been developed in-house or customized, would be difficult to replace compared to the off-the-shelf software. Depending on the assessment done during Step 1 we should be able to identify the critical software assets, which will require a higher level of protection.

Physical Assets

All the hardware devices, communication devices, magnetic media, technical infrastructure devices like power supplies, air conditioning units etc. are part of these assets. Storage medium, by itself, may not be a high-cost item but if it contains vital, critical information or software assets, its security rating will go up.

Services

Computing and communication services, general utilities like heating, lighting, power, air-conditioning etc. Step 2 will provide a detailed scope for ISMS, which will define the areas that are critical for the business, and dependence on these services make them critical too.

Asset Identification

An identification scheme should uniquely identify each of the above listed assets. This could be part of an organization-wide asset tracking system, to avoid duplication of the effort.

Following information should be compiled for the organization:

(i) List of information systems included in the ISMS
(ii) List of assets and their owners
(iii) Replacement value of these assets
(iv) Location of the assets
(v) Classification of these assets as per the scheme described below

Asset Classification

Individual information assets will have to be classified based on the C, I, A classification of the individual IT systems.

Example: Human Resources System

Confidentiality: Very high, the employee data should be maintained at highest confidentiality level.
Integrity: Medium, the data is verified at various stages and any changes to it would be detected.
Availability: Low, the system is not required on-line. A delay of up to one day in getting requisite information is acceptable.

Information access classification

Based on the C, I, A classification done for the IT systems in, each of the IT system will have appropriate access classification. Most business organization follows a four level classification for providing access to the information systems

Unclassified

Considered publicly accessible. There are no requirements for access control or confidentiality.
Shared: Resources that are shared within groups or with people outside of your organization.
Company Only: Access to be restricted to your internal employees only.
Confidential: Access to be restricted to a specific list of people.

Identify and Assess the Risk

We should have a comprehensive list of all the critical assets whose failure could impact a business. We will also have the C, I, A rating for each of these assets which will help us in identifying suitable protection measures, commensurate with the C, I, A ratings of individual assets. We should now proceed to identify and assess risks to these assets.

Perform a threat analysis

Every asset is exposed to numerous threats. These threats are broadly classified in three categories:

(i) Natural Threats
These are Acts of God like floods, earthquakes, tornados, landslides, avalanches, electrical storms and other such events.

(ii) Environmental Threats
Long term power failure, pollution, chemicals, liquid leakage etc.

(iii) Human Threats
Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, and unauthorized access to confidential information).

Make a comprehensive list of all the threats, which are likely to occur this list will have to be made, based on interviews, past records and experience of similar industries as well as organizations located in similar geographical areas and subjected to similar environment.

Perform a vulnerability analysis

Vulnerability is a weakness in the design of a system, which could be exploited by a threat. Discovering such vulnerabilities is the objective of this analysis. Following methods could discover the vulnerabilities.

Design documentation review

Do a complete design review beginning with the design specifications. You may discover that security was not a part of the specifications and hence was not implemented in the design.

This is because majority of the present-day Information Systems have evolved from a central configuration to a networked one, and this evolution has thrown new challenges to the security professionals. Information Security is only an afterthought of these systems.

Review incident logs

The historical incident logs, where available, will give a good insight into the vulnerabilities of a system.

Physical inspection of the premises

This is essential when identifying vulnerabilities. The premises could be exposed to natural and environmental threats.

Tools based security testing

Various vulnerability assessment tools could be used to identify weaknesses, which are usually exploited by a hacker. This means that the same tools that are used by a hacker to break into a system should be used to test the strength of the system. Use of these security-testing tools could sometimes threaten the security. Hence prior written permission must be obtained before applying the tools.

Social engineering

An attack based on deceiving users or administrators at the target site. Social engineering is one of the most effective techniques used by a human attacker. Similar technique should be employed to test the vulnerabilities, which are usually present because of the lack of the security awareness. Similar to the use of security testing tools, social engineering should be used only with prior written permission.

Use of risk analysis tools

Various commercial risk analysis tools are available to aid an organization in evaluating the level of security. These have large databases of questions, which help in analyzing the risks. Examples of such tools are Cobra and CRAMM

Assign overall vulnerability ratings

Based on the threat and vulnerability analysis, each threat and vulnerability could be assigned specific rating based on what is the severity of the vulnerability and what is the resultant exposure.

Asset risk evaluation

Now that we have a comprehensive list of risks, threats and vulnerabilities rating as per the severity and exposure rating, next step is to evaluate the level of risk that the organization is exposed to:

There are two factors that need to be considered.

Probability signifies the confidence level that a threat will be successful, in view of the current level of controls. Probability is directly related to the overall vulnerability rating calculated in the previous step and could be expressed as a percentage.

Consequences of a successful threat attempt are based on the business risk evaluation. These should preferably be expressed as monetary figures.

Level of risk is the product of probability and consequence. This gives an absolute value if consequences are expressed in monetary terms or relative value if the consequences are shown as a relative number. Whatever is the measure used, the level of risk could be used for prioritizing the security implementation efforts.

Plan for Risk Management

Options for risk management are based on cost benefit analysis of various options available to handle the risk. These are:

Transfer the risk: For example, take a fire insurance policy and transfer the risk for fire to an insurance company.

Avoidance of the risk: For example, if there is an old server, which is malfunctioning, replacing it will avoid all the associated risk.

Acceptance of the risk: You are aware of the risk but the solution to avoid the risk is too costly. You decide to live with the risk and face the consequences.

Risk reduction: You decide to take the bull by the horn and plan to identify the security measures, which will reduce the risk to an acceptable level.

Following steps could be followed to select appropriate controls:

(1) **Define security policies:** This should be the beginning point for risk reduction. Security policy statement described in Step 2 was to demonstrate the management's commitment towards information security. Detailed security policy statements define the operational level commitment to tackle each of the security risks identified during the threat and risk assessment. For example, if electronic mail is recognized as a business critical function, every risk to electronic mail system as well as the threats that could be carried out by using electronic mail system will be addressed by an 'Electronic mail security policy document'. This policy should cover the organization's concern, approach to tackle the security issue and compliance requirements.

(2) **Define procedures:** Procedures define details regarding implementation of the security policy. These will provide details like responsibilities of various groups, actions to be taken for preventing, detecting, correcting and reporting security lapses.

(3) **Define standards:** Organization may decide adhering to some international standards in the area of information security. For example, for email security, the organization may select S/MIME as the standard for secure email exchange.

(4) **Identify security products:** Security policy cannot be implemented just by having well defined administrative procedures. It may be necessary to select some products to implement some of the clauses of security policy. For example E-mail security policy may state that the user should not use profane, obscene language in the email. Only a device like content filter could detect violation of this policy by users.

(5) **Cost vs. benefit:** Finally, selection of the control depends on cost vs. benefit analysis. We should check whether cost of implementation of control is more than the risk we are attempting to reduce. For example, if we have to select the access control device for a location, we have a bewildering range of controls, ranging from simple swipe card system to biometric devices like retina scanners. Selection will be based on the C, I, A rating of the objects we are trying to protect and the business impact of the security compromise. We have to take a judicious decision and select the control whose cost is less than the risk it is attempting to reduce.

Implement Risk Mitigation strategy

Implementation or risk mitigation strategy involves converting all the risk management plans into actions. As an outcome of the previous step you should have following items ready for implementation:

(i) Detailed Security Policies
(ii) Procedures and guidelines
(iii) New security products
(iv) Improvements for existing devices

(i) Detailed Security policies

These could be addressing a number of security concerns. Typically an organization will have following policies:

Essential Policies:
Natural and Environmental Threats: - Disaster recovery plan - Backup and recovery plan - Wide area network recovery plan

Human Threats:
Password Security & Controls-Internet access and security-Punitive Actions-Email security

Technical controls -Program Change Controls -Version Controls -Application Software Security -Database Security -Network & Telecommunication Security -Operating Systems Security -Firewall Security -Incident Response and Management -Data Classification -Web server Security -Intranet Security -Virus Protection -E-commerce Security -Data encryption Administrative Controls - Third Party Security -Tele-working security

(ii) Procedures and guidelines

Each of the above policies will be supported by appropriate procedures, instructions and guidelines based on selected standards and products. The procedures should be detailed and unambiguous enough for every person to follow.

(iii) New security products

You would have acquired a range of new security products. Installing, configuring and integrating them with the existing security architecture will be a daunting task.

(iv) Improvements for existing devices

Finally, you would also have acquired or downloaded new versions of software, new patches and service packs to enhance the security of your current devices.

Project planning

Implementing the security policies by deploying appropriate procedures and products will be major task. This needs to be done by creating teams with specific and time-bound responsibilities. This will involve coordination with the end-users of systems as well as suppliers of products. If the vulnerability assessment has indicated numerous holes in the current implementation of operating systems, relevant patches will have to be implemented after appropriate testing.

Testing the new security measures

Repeat all the steps described in Step 6 namely:
(i) Perform a vulnerability analysis
(ii) Assign overall vulnerability ratings
(iii) Asset/ risk evaluation
(iv) Prepare a new current state assessment and gap analysis table

We should be able to see a substantial improvement in all the ratings as well as reduction in Security gaps.

Confirm the change in risk levels

You will have to ensure that the risk levels have really changed due to the new security measures. Doing peer review of each team's work by another team can achieve this. You could also invite other competent individuals and groups like external consultants as well as vendors.

Write the Statement of Applicability

So far we took the risk management approach for identifying and mitigating the risks. Now we should start checking our selection of controls against the controls defined by ISO 27001. As explained, these controls are described in very general terms and no specific interpretation has been provided. There is no 'how to implement a control' defined anywhere. Entire emphasis is on selection of appropriate controls based on the risk assessment.

To identify if we have missed any of these controls, carry out the following exercise:

Mapping the implemented controls against ISO 27001control objectives and controls:

Map the implemented controls against the ISO 27001controls:
Make a table of all the controls and map the controls implemented against relevant ISO 27001 control objectives and controls. One implemented control may address more than one ISO 27001 control.

Identify the gaps:

If there are some gaps, find out, whether these are unintentional omissions or there are no requirements of controls. Recheck the evaluation of risks and threats performed by you. Validate the business risk analysis performed earlier. Prepare justification for any gaps in the table. You may be able to justify a gap if the risk assessment has not shown requirement for a particular control.

Reasons for exclusion:

Explain the controls implemented and reason for exclusion, if any, in the appropriate column. Also give the risk reference, which will support your statement. Organizations, various security risks and threats and finally consequences of not abiding by the security procedures. Following steps should be taken:

Design security training programs .These programs should be designed for all levels. Broadly these will be:
(i) Top management Security Awareness program
(ii) End user Security Awareness program
(iii) IT Department Security Management program

The training programs should be relevant to the organization's security requirements, and as such, should be based on the security policy and risk assessment performed for the organization.

Annual calendar:

You may have to prepare an annual schedule for these programs and ensure that all the users are trained.

Creating Security awareness:

To ensure that information security measures do not become routine stuff and get ignored, create slogans, posters, newsletters and competitions to keep the interest in security topics alive. Also, give publicity to relevant security incidents. There will be increased awareness if the hypothetical threats really materialized.

Monitor and Review the ISMS performance

Implementation of information security management system is not a one-time job. It needs to be constantly monitored and reviewed.

Create the following mechanism for effectively monitoring and reviewing the ISMS performance:

Reporting system

ISO 27001 has defined a specific control objective: responding to security incidents and malfunctions. This involves the following measures:

(i) Reporting security incidents
(ii) Reporting security weaknesses - Reporting software malfunctions
(iii) Operator logs
(iv) Fault logs

Each of these controls will generate huge amount of information. Ensure that this information is properly recorded and stored for any analysis

Review mechanism

The incident reports will be of no use if they are not reviewed regularly. The formation of security organization should include assigning specific responsibilities to teams or individuals to periodically review the logs and reports.

Internal Audit

Periodic audit should be performed to review the performance of various controls and measures defined in ISMS. Internal audit teams or external consultants could perform the audit. The audit findings should be documented and all non-conformities must be corrected and reported within a specific time frame.

Management Review

The Security Steering Committee should conduct management review of the performance of ISMS at least once a year. This review should be based on various reports submitted by incident reporting and review processes and internal audit reports.

Maintain the ISMS and ensure continual Improvement

Implementing ISMS will not ensure sudden improvement in information security stance of the organization. It provides an opportunity to monitor the security in an organized manner and ensure continual improvement. You could ensure that the continual improvement actually takes place by having the following measures in

7.4 BASICS CONCEPTS OF ISO 27001

What is ISO 27001?

It's a International Standard for Information Security Management. It consists of various Specification for information Security Management, Code of Practice for Information Security Management.

ISO 27001, titled "Information Security Management - Specification With Guidance for Use", is the replacement for BS7799-2. It is intended to provide the foundation for third party audit, and is 'harmonized' with other management standards, such as ISO 9001 and ISO 14001.

The basic objective of the standard is to help establish and maintain an effective information management system, using a continual improvement approach. It implements OECD (Organization for Economic Cooperation and Development) principles, governing security of information and network systems.

The Contents of the Standard

The broad content is of course similar to the old BS7799. Included is:

(i) Cross reference with ISO 17799 controls
(ii) Use of PDCA
(iii) Information Management System
(iv) Terms and definitions

ISO 27001 Certification

As with BS7799-2, a robust audit and certification scheme supports the standard. For those already certified against BS7799, accredited certification bodies will establish transitional arrangements.

The ISO 27000 Series

The final version of ISO 27001 was published in October 2005 to a great fanfare. It should be noted, however, that this is in fact only the first of a series of standards to support information security. Having stated this, it may well be the most important, at least from a 'top down' perspective, as it defines the information security management system.

ISO Domains

ISO has 11 domains.

(I) Security policy
(II) Organization of information security
(III) Asset management
(IV) Human resources security
(V) Physical and environmental security
(VI) Communications and operations management
(VII) Access control
(VIII) Information systems acquisition, development and maintenance
(IX) Information security incident management
(X) Business continuity management
(XI) Compliance

(I) Security policy

Information security policy

(i) information security policy document
(ii) review of the information security policy

(II) Organization of information security

Internal Organization

(i) management commitment to information security
(ii) information security co-ordination
(iii) allocation of information security responsibilities
(iv) confidentiality agreements
(v) contact with authorities
(vi) contact with special interest groups
(vii) independent review of information security

External Parties

(i) identification of risks related to external parties
(ii) addressing security when dealing with customers
(iii) addressing security in third party agreements

(III) Asset management

Responsibility for Assets

(i) inventory of assets
(ii) ownership of assets
(iii) acceptable use of assets

Information Classification

(i) classification guidelines
(ii) information labeling and handling

(IV) Human resources security

Prior to Employment

(i) roles and responsibilities
(ii) screening
(ii) terms and conditions of employment

During Employment

(i) management responsibilities
(ii) information security awareness, education, and training
(iii) disciplinary process

Termination or Change of Employment

(i) termination responsibilities
(ii) return of assets
(iii) removal of access rights

(V) Physical and environmental security

Secure Areas

(i) physical security perimeter
(ii) physical entry controls
(iii) securing offices, rooms, and facilities
(iv) protecting against external and environmental threats
(v) working in secure areas
(vi)) public access, delivery, and loading areas

Equipment Security

(i) equipment siting and protection
(ii) supporting utilities
(iii) cabling security
(iv) equipment maintenance
(v) security of equipment off-premises
(vi) secure disposal or re-use of equipment
(vii) removal of property

(VI) Communications and operations management

Operational Procedures And Responsibilities

(i) documented operating procedures
(ii) change management
(iii) segregation of duties
(iv) separation of development, test, and operational facilities

Third Party Service Delivery Management

(i) service delivery
(ii) monitoring and review of third party services
(iii) managing changes to third party services

System Planning and Acceptance

(i) capacity management
(ii) system acceptance

Protection against Malicious and Mobile Code

(i) controls against malicious code
(ii) controls against mobile code

Back-Up

(i) information back-up

Network Security Management

(i) network con 45
(ii) security of network services

Media Handling

(i) management of removable media
(ii) disposal of media
(iii) information handling procedures
(iv) security of system documentation

Exchange Of Information

(i) information exchange policies and procedures
(ii) exchange agreements
(iii) physical media in transit
(iv) electronic messaging
(v) business information systems

Electronic Commerce Services

(i) electronic commerce
(ii) on-line transactions
(iii) publicly available information

Monitoring

(i) audit logging
(ii) monitoring system use
(iii) protection of log information
(iv) administrator and operator logs
(v) fault logging
(vi) clock synchronization

(VII) Access control

Business Requirement For Access Control

(i) access control policy

User Access Management

(i) user registration
(ii) privilege management
(iii) user password management
(iii) review of user access rights

User responsibilities

(i) password use
(ii) unattended user equipment
(iii) clear desk and clear screen policy

Network Access Control

(i) policy on use of network services
(ii) user authentication for external connections
(iii) equipment identification in networks
(iv) remote diagnostic and configuration port protection
(v) segregation in networks
(vi) network connection control
(vii) network routing control

Operating System Access Control

(i) secure log-on procedures
(ii) user identification and authentication
(iii) password management system
(iv) use of system utilities
(v) session time-out
(vi) limitation of connection time

Application and Information Access Control

(i) information access restriction
(ii) sensitive system isolation

Mobile Computing and Teleworking

(i) mobile computing and communications

(ii) teleworking

(VIII) Information systems acquisition, development and maintenance

Security Requirements of Information Systems

(i) security requirements analysis and specification

Correct Processing in Applications

(i) input data validation
(ii) control of internal processing
(iii) message integrity
(iv) output data validation

Cryptographic Controls

(i) policy on the use of cryptographic controls
(ii) key management

Security Of System Files

(i) control of operational software
(ii) protection of system test data
(iii) access control to program source code

Security In Development And Support Processes

(i) change control procedures
(ii) technical review of applications after operating system changes
(iii) restrictions on changes to software packages
(iv) information leakage
(v) outsourced software development

Technical Vulnerability Management

(i) control of technical vulnerabilities

(IX) Information security incident management

Reporting Information Security Events And Weaknesses

(i) reporting information security events
(ii) reporting security weaknesses

Management Of Information Security Incidents And Improvements

(i) responsibilities and procedures
(ii) learning from information security incidents
(iii) collection of evidence

(X) Business continuity management

Information Security Aspects Of Business Continuity Management

(i) including information security in the business continuity management process
(ii) business continuity and risk assessment
(iii) developing and implementing continuity plans including information security
(iv) business continuity planning framework
(v) testing, maintaining and re-assessing
(vi) business continuity plan

(XI) Compliance

Compliance With Legal Requirements

(i) identification of applicable legislation
(ii) intellectual property rights (ipr)
(iii) protection of organizational records
(iv) data protection and privacy of personal information
(v) prevention of misuse of information processing facilities
(vi) regulation of cryptographic controls

Compliance With Security Policies And Standards, And Technical Compliance

(i) compliance with security policies and standards
(ii) technical compliance checking

Information Systems Audit Considerations

(i) information systems audit controls
(ii) protection of information systems audit tools