A Complete Summary of

IT Governance

as per references

for

Professional Level

CA BANGLADESH | THE INSTITUTE OF CHARTERED ACCOUNTANTS OF BANGLADESH

Prepared by:

MD. SOHEL BEPARY

Rahman Mostafa Alam & Co.
Chartered Accountants

INPACT

Table of Contents

CHAPTER # 01: INFORMATION TECHNOLOGY POLICIES AND LAWS

A. National ICT Policy 2009

Structure and Conventions

The policy document is structured as a hierarchical pyramid with a single vision, 10 broad objectives, 56 strategic themes and 306 action items. The vision and objectives are aligned with the general national goals while the strategic themes are areas within the broad objectives that can readily benefit from the use of ICTs. The action items are generally meant to be implemented either in the

- short term (18 months or less),
- medium term (5 years or less) or
- long term (10 years or less).

However, some action items have been recommended for continuation throughout multiple terms where the scope of the activity gradually expands in the longer terms. Conventional notions of vision, objective, strategic theme, etc. tend to differ greatly from person to person and from discipline to discipline. Thus, for the purpose of this policy proposal, the following definitions have been adopted for a) Vision, b) Objective c) Strategic Theme, d) Action Item, and e) ICTs.

B. Policy Ownership, Monitoring and Review

The ICT Policy must be owned by all stakeholder groups who will continually seek to have the mandates of the policy adhered to in all spheres of national life. The policy must have a Champion in the highest levels of the Government. Accordingly, the following Policy Ownership arrangement is envisaged. The National ICT Policy shall be monitored and coordinated by the Minister in charge of ICT while the associated action programmes will be implemented and/or supported by the Bangladesh Computer Council or its successor organisation; all Government agencies and quasi-state bodies will implement ICT Policy in their respective area. Instruction from National ICT Task Force will be taken for any deviation in implementing the Policy. The action plans under the policy shall be reviewed at least once a year for implementation status checks, necessary reprioritizations and changes in programmes. The strategic themes shall be reviewed every three years along with realignment of specific goals with new developments. The whole policy itself shall be reviewed in totality every six years and long-term goals adjusted according to achievements and failures along the way. With the aims and objectives of the National ICT Policy 2009 materialized, Bangladesh is expected to become a 'knowledge society' within one generation.

Vision

Expand and diversify the use of ICTs to establish a transparent, responsive and accountable government; develop skilled human resources; enhance social equity; ensure cost-effective delivery of citizen-services through public-private partnerships; and support the national goal of becoming a middle-income country within 2021 and join the ranks of the developed countries of the world within thirty years.

Objectives

Social Equity: Ensure social equity, gender parity, equal opportunity and equitable participation in nation-building through access to ICTs for all, including persons with disabilities and special needs

Productivity: Achieve higher productivity across all economic sectors including agriculture and SMME (small, medium and micro enterprises) through the use of ICTs.

Integrity: Achieve transparency, accountability, responsiveness and higher efficiency in the delivery of citizen-services.

Education and Research: Expand the reach and quality of education to all parts of the country using ICTs, ensure computer literacy at all levels of education and public service and facilitate innovation, creation of intellectual property and adoption of ICTs through appropriate research and development.

Employment Generation: Enlarge the pool of world-class ICT professionals to cater to the local and overseas employment opportunities.

Strengthening Exports: Ensure a thriving software, ITES and IT manufacturing industry to meet domestic and global demands and thereby increase foreign exchange earnings, attract foreign direct investments and reduce dependence on imports.

Healthcare: Ensure quality healthcare to all citizens by innovative application of ICTs.

Universal Access: Ensure connectivity to all as a public service obligation (PSO).

Environment, Climate and Disaster Management: Enhance creation and adoption of environment-friendly green technologies, ensure safe disposal of toxic wastes, minimize disaster response times and enable effective climate change management programmes through use of ICTs as Bangladesh is facing the dual scourge of environmental pollution due to rising industrial and consumer wastes and also global-warming-induced climate-change due to excessive carbon emissions of the industrialized countries

Supports to ICTs: Develop appropriate infrastructure including power, and regulatory framework for effective adoption and use of ICTs throughout the country.

E. Strategic Themes

E.1. Social Equity:
1.1 Mainstream social advancement opportunities for disadvantaged groups as an immediate priority to minimize economic disparity and bridge the digital divide for (a) lower income groups, (b) ethnic minorities, (c) women, and (d) persons with disabilities and special needs
1.2 Facilitate citizens' participation in local and national government, and policy making as a broad national agenda
1.3 Provide incentives to the private sector and NGO/CSO/CBOs to generate and share locally relevant and local language digital content and online services
1.4 Develop and preserve content to bolster culture, heritage and religion
1.5 Bring into focus children's issues, including protection of children from harmful digital content

E.2. Productivity:
2.1 Encourage maximum utilization of ICT services nationwide to boost productivity of small, medium and micro enterprises and agriculture sector, and focus on innovation and competitiveness
2.2 Ensure dissemination and utilization of latest know-how and market information to increase production capability and supply chain management of agriculture through ICT applications
2.3 Ensure better monitoring, skills gap determination, appropriate training and modern enterprise operations to enhance productivity of large enterprises by encouraging immediate implementation of end to end applications (ERP)
2.4 Ensure sustainable productivity in the service sector through increased automation of operations and management information systems
2.5 Encourage e-commerce, e-payments, and e-transactions in general bringing in a new dimension of productivity to the economy at the earliest

E.3. Integrity:
3.1 Ensure the use of Bangla in all ICT activities
3.2 Reduce harassment, time and cost of the people and ensure transparency and accountability in government service delivery by monitoring citizens' charter and making results of all services delivery public including services related to justice and law & order
3.3 Establish interconnectivity across government offices for effective data sharing
3.4 Build capacity of public functionaries and foster leadership for electronic service delivery
3.5 Mandate availability of all public information through electronic means and ensure sustainability of ICT-based citizens' services delivery
3.6 Introduce ICT-based monitoring of planning, implementation and effectiveness of development projects

E.4. Education and Research:
4.1 Assess skills of ICT professionals and meet gaps with targeted training programmes to overcome the short-term skills shortage in the ICT industry and adopt continuing education and professional skills assessment and enhancement programmes
4.2 Encourage closer collaboration between academia and industry to align curriculum with market needs
4.3 Establish an ICT Centre of Excellence with necessary long-term funding to teach and conduct research in advanced ICTs
4.4 Extend the reach of ICT literacy throughout the country by incorporating ICT courses in primary and secondary education and technical and vocational education and training (TVET) programmes
4.5 Enhance the quality and reach of education at all levels with a special focus on Mathematics, Science and English
4.6 Ensure ICT Literacy for all in public service

4.7 Boost use of ICT tools in all levels of education including ECDP, mass literacy and lifelong learning
4.8 Ensure access to education and research for people with disabilities and special needs using ICT tools
4.9 Ensure that all universities provide global standard ICT education and introduce Postgraduate Programmes in ICT education to encourage research and innovation

E.5. Employment Generation:
5.1 Provide incentives for investment in local ICT industry
5.2 Build institutional capacity for producing greater number of IT professionals in line with domestic and global demands for knowledge workers
5.3 Standardize skills for local ICT industry
5.4 Facilitate global employment of skilled ICT workforce
5.5 Provide financial assistance to ICT professionals for skills development

E.6. Strengthening Exports:
6.1 Develop strong marketing, promotion and branding for Bangladeshi ICT products and services in global markets
6.2 Ensure access to finance for promising software and ITES companies
6.3 Develop and maintain reliable ICT infrastructure
6.4 Provide incentives to increase export and create industry friendly policy and enabling environment
6.5 Foster innovation through research and development to improve quality, process, technology, domain, value chain and niche markets

E.7. Healthcare:
7.1 Improve management of healthcare delivery system using telemedicine and modern technologies
7.2 Improve community awareness and access to health care facilities for all including difficult to access areas, with a special emphasis on child, maternal and reproduction health
7.3 Ensure Quality Assurance of health care services
7.4 Enhance capacity of National Health Service Delivery System

E.8. Universal Access:
8.1 Extend universal connectivity to all citizens as a public service obligation within 5 years
8.2 Extend internet backbone infrastructure to all district headquarters immediately at the same access cost as in the capital
8.3 Extend Internet and IP telephony services to all parts of the country within 5 years through providing incentives as stipulated in the national telecom policy
8.4 Make IP-based telecommunications ubiquitous and affordable by all through aggressive adoption of NGN and license-free regime

E.9. Environment, Climate and Disaster Management:
9.1 Promote entire environmental preservation including land and water resources by adopting environment-friendly green technologies
9.2 Promote entire environmental protection including land and water resources through the use of ICT tools
9.3 Protect citizens from natural disasters through ICT-based disaster warning and management technologies
9.4 Ensure safe disposal of toxic wastes resulting from use of ICTs
9.5 Promote efficient relief management and post disaster activities monitoring

E.10. Supports to ICTs:
10.1 Ensure reliable and cost-effective power
10.2 Create supportive legal framework for IPR protection, online document sharing, transactions and payments
10.3 Establish a Government Interoperability Framework to be adhered to by all government ICT projects
10.4 Promote the use of cost-effective, open source and open architecture solutions
10.5 Build ICT infrastructure facilities in educational institutions
10.6 Decentralize ICT growth outside the capital
10.7 Improve education quality in IT, Mathematics and English
10.8 Improve Internet availability and reliability

Digital signature" means data in an electronic form, which--

a) is related with any other electronic data directly or logically; and
b) is able to satisfy the following conditions for validating the digital signature--
   (i) affixing with the signatory uniquely;
   (ii) capable to identify the signatory;
   (iii) created in safe manner or using a means under the sole control of the signatory; and
   (iv) related with the attached data in such a manner that is capable to identify any alteration made in the data thereafter.

Sec- 6: **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 information or matter is rendered or made available in an electronic form:
Provided that such information or matter is accessible so as to be usable for a subsequent reference.

Sec- 9: Retention of electronic records.--(1) Where any law provides that any document, record or information shall be retained for any specific period, then such requirement shall be deemed to have been satisfied if such documents, records or information, as the case may be, are retained in the electronic form if the following conditions are satisfied--

a) the information contained therein remains accessible so as to be usable for a subsequent reference;
b) the electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
c) such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained:

Provided that this sub-clause does not apply to any information which is automatically generated solely for the purpose of enabling and electronic record to be dispatched or received.

Sec- 19: Functions of the Controller.--The Controller may perform all or any of the following functions, namely:--

a) exercising supervision over the activities of the Certifying Authorities;
b) laying down the standards to be maintained by the Certifying Authorities;
c) specifying the qualifications and experience which employees of the Certifying Authorities should possess;
d) specifying the conditions subject to which the Certifying Authorities shall conduct their business;
e) specifying the contents of written, printed or visual materials and advertisements that may be used in respect of a Digital Signature Certifying;
f) specifying the form and content of a Digital Signature Certificate;
g) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
h) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them for auditing the Certifying Authorities;
i) facilitatining the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
j) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
k) resolving any conflict of interests between the Certifying Authorities and the subscribers;
l) laying down the duties and responsibilities of the Certifying Authorities;
m) maintaining computer based databases, which--
   i. contain the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations; and
   ii. shall be accessible to the member of the public;
n) perform any other function under this Act or Codes prepared under this Act.

Sec- 30: Access to computers and data.—

(1) Without prejudice to the provisions of section 45 of this Act the Controller or any officer authorized by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act or rules and regulations made there under 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 purpose of sub-section (1) of this section the Controller or any officer authorized by him may, by order, direct any person in charge 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.
(3) If authorization has been given to a person, the authorized person shall oblige to assist as instructed under sub-section (1) of this section.

Sec- 39: Suspension of Digital Signature Certificate.—

1. Subject to the provisions of sub-section (2) of this section, the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate—
   a. on receipt of a request to that effect from the subscriber listed in the Digital Signature certificate or any person duly authorized to act on behalf of that subscriber;
   b. if it is opinion that the Digital Signature Certificate should be suspended in public interest.
2. A Digital Signature Certificate shall not be suspended for a period exceeding 30 (thirty) days without giving the subscriber a notice under sub-section 1 (b) of this section.
3. Certifying Authority can suspend the Digital Signature Certificate, if the Authority is satisfied on the ground that the explanation given by the subscriber in response to the notice of subsection (2) of this section is not acceptable.
4. On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

BREACHING RULES, PREVENTION, PENALTIES ETC.

Sec- 48: Penalty for failure to furnish document, return and report.—If any person fails to submit given document, return and report under the provisions of this Act, or rules and regulations made there under to the Controller or Certifying Authority, the Controller or any officer of the Government authorized by the Government by special order, as the case may be, can fine the person which may extend to **Taka ten thousands** mentioning reasons in written by administrative order.

Sec- 49: Penalty for failure to file return, information, book etc.—If any person fails to deliver any information, books or any other documents under the provisions of this Act, or rules and regulations made there under within stipulated time, the Controller or any officer of the Government authorized by the Government by special order, as the case may be, can fine the person which may extend to **Taka ten thousand** mentioning reasons in written by administrative order.

Sec- 50: Penalty for failure to maintain books of accounts or record.—If any person fails to maintain books of accounts or records which is supposed to be preserved under the provisions of this Act, or rules and regulations made there under, the Controller or any officer of the Government authorized by the Government by special order, as the case may be, can fine the person which may extend to **Taka two lakhs** mentioning reasons in written by administrative order.

Sec- 51: Residuary penalty.—If any person contravenes any rules of this Act for which the provision of penalties has not been fixed separately under the provisions of this Act, or rules and regulations made there under, the Controller or any officer of the Government authorized by the Government by special order, as the case may be, can fine the person for breaching the very rule which may extend to **Taka twenty five thousands** mentioning reasons in written by administrative order.

OFFENCES, INVESTIGATION, ADJUDICATION, PENALTIES ETC

Section- 54 to 57 and 66 has been repealed by Digital Security Act- 2018

58. Punishment for failure to surrender licence.--(1) Where any Certifying Authority fails to surrender a licence under section 34 of this Act, the person in whose favour the licence is issued, the failure of the person shall be an offence.
(2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to six months, or with fine which may extend to Taka ten thousand, or with both.

59. Punishment for failure to comply with order.--(1) Any person who fails to comply with any order made under section 45 of this Act, then this activity of his will be regarded as an offence.

(2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to one year, or with fine which may extend to Taka one lakh, or with both.

60. Punishment for failure to comply with order made by the Controller in emergency --
(1) Any person who fails to comply with any order made under section 46 of this Act, then this activity of his will be regarded as an offence.
(2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to five years, or with fine which may extend to Taka five lakhs, or with both.

61. Punishment for unauthorized access to protected systems.--(1) Any person who secures access or attempts to secure access to protected system in contraventions of section 47 of this Act, then this activity of his will be regarded as an offence.
(2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to Taka ten lakhs, or with both.

62. Punishment for misrepresentation and obscuring information.--Whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate shall be regarded as an offence.
(2) Whoever commits any offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakhs, or with both.

63. Punishment for disclosure of confidentiality and privacy.--Save as otherwise provided by this Act or any other law for the time being in force, no person who, in pursuance of any of the powers conferred under this Act, or rules and regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material shall, without the consent of the person concerned, disclose such electronic record, book, register, correspondence, information, document or other material to any other person shall be regarded as an offence.
(2) Whoever commits any offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakhs, or with both.

64. Punishment for publishing false Digital Signature Certificate.--No person shall publish a Digital Signature Certificate or otherwise make it available to any other person knowing that--
(a) the Certifying Authority listed in the certificate has not issued it; or
(b) the subscriber listed in the certificate has not accepted it; or
(c) the certificate has been revoked or suspended; unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation and by breaching the rules such Digital Signature Certificate is published or
otherwise make it available to others shall be regarded as an offence.
(2) Whoever commits any offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakhs, or with both.

65. Punishment for publishing Digital Signature Certificate for fraudulent purpose etc.-- Whosoever knowingly creates and publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be regarded as an offence.
(2) Whoever commits any offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakh, or with both.

67. Offences committed by companies etc.--If any offence is committed by a company under this Act, then each director, manager, secretary, partner, officer and staff of the company who has directly involvement in committing the said offence shall be guilty of the offence or the contraventions, as the case may be, unless he proves that the offence or contravention was committed without his knowledge or that he exercised sue diligence in order to prevent commission of such offence or contravention.
Explanation.—For the purposes of this section.—
(a) “company” means anybody corporate and includes commercial firm, partnership business, cooperatives, association, organization or other association of individuals; and
(b) “director” in relation to a commercial firm includes a partner or member of Board of Directors.

CHAPTER SIX

Crime and Punishment

17) Punishment for Illegal Entrance in Critical Information Infrastructure, etc.: -

(1) If any person intentionally or knowingly in any Critical information infrastructure-
   a) Illegally enters, or
   b) By means of illegal entrance, harms or destroys or renders inactive the infrastructure or tries to do so,

Then the above activity of that person will be an offense under the Act

(2) If any person of Sub Section (1)- a. Commits any offense within the Clause (a) then, the person will be penalized by imprisonment for a term not exceeding 7(seven) years or by fine not exceeding 25 (twenty five) lacs taka or with both.
   b. Commits any offense within Clause (b) then, the person will be penalized by imprisonment for a term not exceeding 14 (fourteen) years or with fine not exceeding 1 (one) crore taka or with both.

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits the offense then, he will be punished with lifetime imprisonment or with fine not exceeding 5 (five) crore taka or with both

18) Illegal Entrance in computer, digital device, computer system, etc. and punishment:-

(1) If any person willingly-
   a. illegally enters or help to enter in any computer, computer system or computer network, or
   b. illegally enters or helps to enter with the intention of committing a crime then the activity of that person will be a offense under the Act

(2) If any person under Sub Section (1)-
   a. Commits any offense within the Clause (a) then, the person will be penalized with imprisonment for a term not exceeding 6 months or by fine not exceeding3 (three) lacs taka or with both.
   b. Commits any offense within Clause (b) then, the person will be penalized with imprisonment for a term not exceeding 3(three) years or with fine not exceeding 10 (ten) lacs taka or with both.

(3) If an offence within the Sub-Section (1), is committed in case of a secured computer or computer system or computer network then, the person will be penalized by imprisonment for a term not exceeding 3(three) years or by fine not exceeding 10 (ten) lacs taka or with both.

(4) If any person commits the offense within this Section for the second time or recurrently commits it then, he will be penalized with punishment that is two times of the punishment designated for the main offense

19) Damage of Computer, Computer System, etc. and punishment:-

(1) If any person-
   a. Collects any data or data-storage, information or part of it from any computer, computer system, or computer network or collects transferable information or part of it or copy of it stored in the said computer, computer system or computer network, or
   b. Intentionally inserts or tries to insert any virus or malware or any harmful software in any computer or computer system or computer network, or
   c. Intentionally harms or tires to harm the data or data-storage of any computer, computer system, or computer network or harms or tries to harm the Programs protected in a computer, computer system, or computer network or
   d. By any means stops or tries to stop a valid or authorized person to enter any computer, computer system, or computer network, or
   e. Intentionally creates or tries to create spam or undesired emails without the permission of the sender or receiver, for any product or service marketing, or
   f. Interferes unjustly in any computer, computer system or Computer network or by lies and deliberate falsity enjoys the service of an individual or transfers the charge or tries to transfer of such service into the account of another

Then, that person's activity will be a an offense under the Act

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 7(seven) years or fine not exceeding 10 (ten) lacs taka or with both.

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with imprisonment for a term not exceeding 10(ten) years of imprisonment or with fine not exceeding 25 (twenty five) lacs taka or with both.

20) Offenses relating to Computer Source Code Change and Punishment:-

(1) If any person intentionally or knowingly hides or destroys or changes the source code used in any computer, computer system, or computer network or if he tries to hide, destroy or change the source through another person and if that source code is preservable and securable then that act of the said person will be considered an offense under the Act.
(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 3 (three) years or fine not exceeding 3 (three) lacs taka or with both
(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with imprisonment for a term not exceeding 5(five) years or with fine not exceeding 5 (five) lacs taka or with both.

21) Punishment for Any propaganda or campaign against liberation war, Cognition of liberation war, Father of the nation, National Anthem or National Flag: -

(1) If any person by means of digital medium runs any propaganda or campaign or assists in running a propaganda or campaign against the liberation war of Bangladesh, Cognition of liberation war, Father of the Nation, National Anthem or national Flag then, that act of that person will be an offense under the Act.
(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 10 (ten) years or with fine not exceeding 1 (one) crore taka or with both.
(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with life term imprisonment or with fine not exceeding 3 (three) crores or with both

22) Digital or Electronic Forgery:-
(1) If any person commits forgery by means of any digital or electronic medium then that activity of that particular person will be an offense under the Act.
(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 5 (five) years or with a fine not exceeding 5 (five) lacs taka or with both
(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with imprisonment for a term not exceeding 7 (seven) years or with fine not exceeding 10 (ten) lacs taka or with both

Explanation:-
To fulfill the objective of this Act, **"Digital or Electronic Forgery"** means, if any person without authority or in excess of the given authority or by means of unauthorized practice produces input or output of any computer or digital device or changes, erases or hides incorrect data or program, or results in erroneous information, or information system of any computer or digital device, data system and computer or digital network operation

23) Digital or Electronic Fraud:-

(1) If any person commits fraud by means of any digital or electronic medium then that activity of that particular person will be an offense under the Act.
(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 5 (five) years or by fine not exceeding 5 (five) lacs taka or with both
(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with imprisonment for a term not exceeding 7 (seven) years or with fine not exceeding 10 (ten) lacs taka or with both

Explanation:-
To fulfill the objective of this Act**, "Digital or Electric Fraud"** means, if any person intentionally or knowingly or without permission changes any information, deletes, adds new information or creates distortion and reduces the value of that or the utility of any computer program, computer system, computer network, digital

device, digital system, digital network, or of a social communication medium, trying to gain benefit for himself/herself or for others or trying to harm others or to deceive others .

24) Identity Fraud or Being in Disguise:-

(1) If any person intentionally or knowingly uses any computer, computer Program, computer system, computer network, digital device, digital system or digital network-

a. With the intention of deceiving or cheating carries the identity of another person or shows any person's identity as his own, or

b. Intentionally by forgery assuming the identity of a alive or dead person as one's own for the following purpose-

i. To achieve some advantages for oneself or for any other person;

ii. To acquire any property or interest in any property;

iii. To harm a person by using another person's identity in disguise.

Then the Act of the person will be an offense under the Act

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized by imprisonment for a term not exceeding 5 (five) years or fine not exceeding 5 (five) lacs taka or both

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with imprisonment for a term not exceeding 7 (seven) years or with 10 (ten) lacs taka or with both

25) Publishing, sending of offensive, false or fear inducing data-information, etc.:-

(1) If any person in any website or through any digital medium-

a. Intentionally or knowingly sends such information which is offensive or fear inducing, or which despite knowing it as false is sent, published or propagated with the intention to annoy, insult, humiliate or denigrate a person or

b. Publishes or propagates or assists in publishing or propagating any information with the intention of tarnishing the image of the nation or spread confusion or despite knowing it as false, publishes or propagates or assists in publishing or propagates information in its full or in a distorted form for the same intentions

Then, the activity of that person will be an offense under the Act.

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 3(three) years of or fine not exceeding 3(three) lacs taka or with both.

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with imprisonment for a term not exceeding 5(five) years or with fine not exceeding 10 (ten) lacs taka or with both

26) Punishment for Collecting, Using identity Information without Permission, etc :-

(1) If any person without any legal authority collects, sells, takes possession, supplies or uses any person's identity information, then, that activity of that person will be an offense under the Act.

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 5 (five) years or fine not exceeding 5 (five) lacs taka or with both.

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be penalized with imprisonment for a term not exceeding 7 (seven) years or with fine not exceeding 10 (ten) lacs taka or with both.

Explanation:-

To fulfill the objective of this Section, **"Identity Information",** means any external, biological or physical information or any other information which singly or jointly can identify a person or a system, his/her name, address, Date of birth, mother's name , father's name, signature, National identity , birth and death registration number, finger print, passport number , bank account number , driver's license , E-TIN number, Electronic or digital signature , username, Credit or debit card number, voice print , retina image , iris image , DNA profile, Security related questions or any other identification which due to the excellence of technology is easily available.

27) Punishment for committing Cyber-terrorism: -

(1) If any person –

a. With the intention to breach the national security or to endanger the sovereignty of the Nation and to instill terror within the public or a part of them creates obstruction in the authorized access to any computer, computer network or internet network or illegally accesses the said computer, computer

network or internet network or cause the act of obstruction of access or illegal entry through someone, or

b. Creates such pollution within any digital device or inserts malware which causes in the death of a person or results in serious injury to a person or raises a possibility of it, or

c. Damages or destroys the supply of daily necessities of public or adversely affects any critical information infrastructure

d. Intentionally or knowingly enters or penetrates any computer, computer network, internet network, any secured data information or computer database or such secured data information or computer database which can be used to damage friendly relations with another foreign country or can be used for acts against public order or which can be used for the benefit any foreign country or any foreign person or any group.

Then that activity of that person will be considered as cyber security crime.

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 14(fourteen) years or with fine not exceeding 1(one) crore taka or with both.

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with lifetime imprisonment or with fine not exceeding 5(five) crore taka or with both

28) Publication, Broadcast, etc. of such information in any website or in any electronic format that hampers the religious sentiment or values:-

(1) If any person or group intentionally or knowingly with the aim of hurting religious sentiments or values or with the intention to provoke publish or broadcast anything by means of any website or any electronic format which hurts religious sentiment or values then such activity of that person will be considered an offence

(2) If any person commits an offence under sub section (1), the person will be sentenced to a term of imprisonment not exceeding 7 (seven) years or fine not exceeding 10 (ten) lac or both.

(3) If any person commits the offence mentioned in sub-section (1) second time or repeatedly, he will be punished with imprisonment not exceeding 10 (ten) years or fine not exceeding 20 (twenty) lac taka or both

29) To publish, broadcast, etc., defamation information:-

(1) If a person commits an offence of publication or broadcast defamatory information as described in section 499 of the Penal Code (Act XLV of 1860) in any website or in any other electronic format then he will be sentenced to a term of imprisonment not exceeding 3(Three) years or fine not exceeding Tk.5 (Five) lac or both.

(2) If any person commits the offence mentioned in sub-section (1) second time or repeatedly, he he will be sentenced to a term of imprisonment not exceeding 5(Five) years or fine not exceeding Tk.10 (Ten) lac or both

30) E-Transaction without legal authority Offence and Punishment:-

(1) If any person-

a. Does e-transaction through electronic and digital medium of any bank, insurance, or any other financial institution or any mobile money service providing organisation without legal authority, or.

b. Does e-transaction that has been declared illegal by the Government or Bangladesh Bank,.

Then such activity will be considered as an offence.

(2) If any person commits offence mentioned in sub section (1), the person will be penalized with either maximum of 5(five) years of imprisonment or fine of Tk. 5 (five) lac or will be punished with both.

(3) If any person commits the offence mentioned in sub-section (1) for the second time or repeatedly, he will be punished with a maximum of 7(seven) years imprisonment or with maximum fine of Tk. 10 (ten) lac or both.

Explanation:-

To fulfill the objective of this Section, **"E-Transaction", means deposit or withdrawal of fund or direction, order or legally authorized money transaction for withdrawal** through any bank, financial institution or through any digital or electronic medium to a specified account number by a person with the aim of transferring funds.

31) Deterioration of Act-order, etc. and Punishment:-

(1) If any person intentionally publish or broadcast any kind of file in any website or digital format which will create hostility, hatred or adversity among people or destroy any communal harmony or create unrest or disorder or deteriorates or threatens to deteriorate the law and order then that activity of that person will be considered as an offence..
(2) If any person commits any crime mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding to 7(seven) years or fine not exceeding Tk. 5(five) lac or with both.
(3) If any person commits the crime mentioned in sub-section (1) for the second time or recurrently commits it, he will be punished with imprisonment for a term not exceeding 10(ten) years or with fine not exceeding Tk.10 (ten) lac or with both

32) Breaching Government Secret Offence and Punishment:-

(1) If any person commits or aids and abets in committing an offence under Official Secrets Act, 1923 (Act No XIX of 1923) through computer, digital device, computer network, digital network or through any other digital medium then he will be punished to a term of imprisonment not exceeding 14(fourteen) years or with fine not exceeding Tk.25 (Twenty Five) Lac or with both.

(2) If any person commits the offence mentioned in sub-section (1) for the second time or recurrently commits it, he will be punished with life imprisonment or with fine not exceeding Tk. 1(one) crore or with both.

33) Illegal Transferring, Saving etc. of Data-Information, Punishment:-

(1) If any person enters any computer or digital system illegally and does any addition or subtraction, transfer or with the aim of transfer save or aid in saving any data-information belonging to government, semi-government, autonomous or statutory organization or any financial or commercial organisation , then the activity of that person will be considered an offence.
(2) If any person commits an offence mentioned in sub section (1), he will be sentenced to a term of imprisonment not exceeding 5(Five) years or with fine not exceeding Tk.10 (Ten) lac or with both.
(3) If any person commits the offence mentioned in sub-section (1) second time or recurrently commits it then, he will be sentenced to a term of imprisonment not exceeding 7(Seven) years or with fine not exceeding Tk.15 (Fifteen) lac or with both.

34) Hacking Related Offence and Punishment:-

(1) If a person commits hacking then it will be considered an offence. and for this, he will be sentenced to a term of imprisonment not exceeding 14(Fourteen) years or with fine not exceeding Tk.1 (One) Crore or with both.
(2) If any person commits the offence mentioned in sub-section (1) second time or repeatedly then, he will be penalized with life imprisonment or with fine not exceeding Tk.5 (Five) Crore or both
Explanation:
In this section “Hacking” means-
a. To destroy, change, format, cancel any information of the computer data storage or to reduce the value or suitability of it or damaging it in any other way, or
b. Without ownership or possession illegally entering and damaging any computer, server, computer network, or any electric system

35) Aiding in Commission of Offence and its Punishment:-

(1) If any person aids in committing any offence under this Act then such act of that person will be considered an offence.
(2) In case of aiding of an offence, the punishment will be the same as that of the original offence.

36) Offence Committed by Company:-

(1) In case of a company committing an offence under this Act, all such owner, chief executive, director, manager, secretary, shareholder or any other officer or employee or representative of the company

having direct connection with the offence will be considered as the offender unless he can prove that the offence took place without his knowledge or he took all possible steps to stop the commission of the offence

(2) If the company mentioned under subsection (1) is a company having corporate legal personality, then apart from the people mentioned, the company can also be charged and found guilty under the same proceedings, but only the monetary punishment can be imposed on the company as per the relevant provisions

Explanation:

In this Section-

a. The word "Company" includes any commercial institution, business partnership, society, association or organization;

b. In case of commercial organization meaning of "Director "will be regarded as including its shareholder or member of board of directors.

37) The power to give order of compensation:

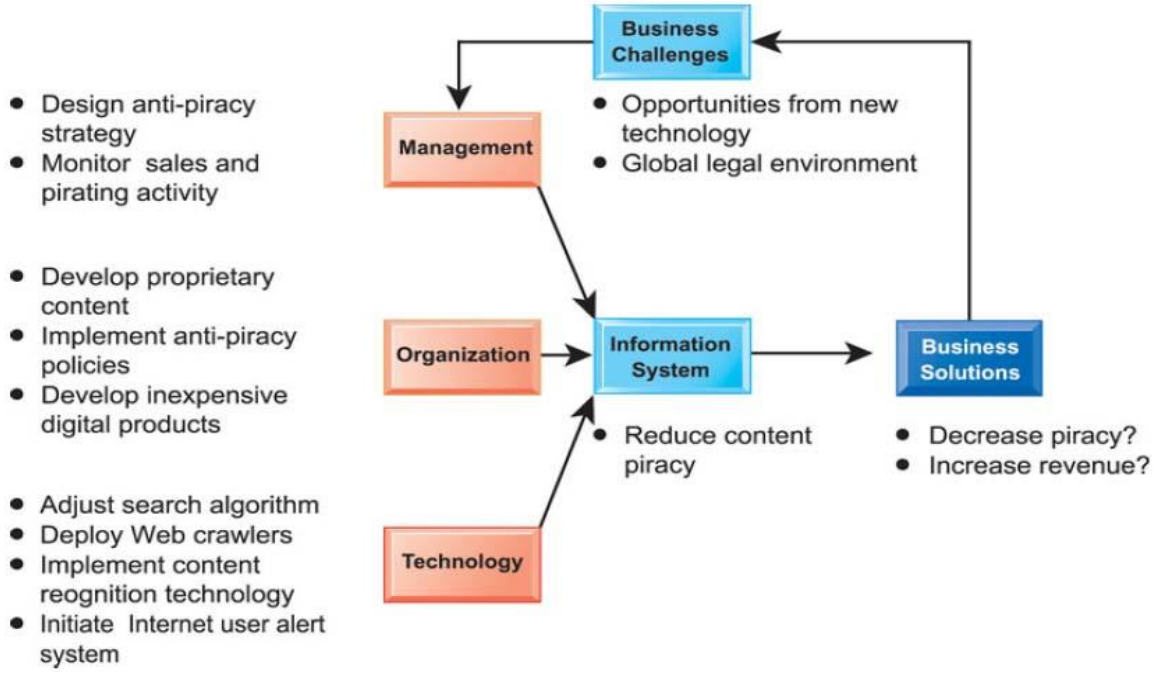
If a person cause financial damage to another person under Section 22 digital or electronic forgery, under Section 23 digital or electric fraud and under Section 24 identification fraud or by means of disguise, the tribunal, may order him to compensate the affected person by giving money equivalent to the damage caused or a suitable amount after considering the damage caused

38) No Responsibility for the service provider:

(1) Any service provider will not be responsible under this Act or any rules enacted under this Act for facilitating access to data-information, if he succeeds in proving that, the offence or breach was committed without his knowledge or he took all possible steps to stop the commission of the offence.

C. Ethical and Social Issues in Information Systems

1. What ethical, social, and political issues are raised by information systems?
2. What specific principles for conduct can be used to guide ethical decisions?
3. Why do contemporary information systems technology and the Internet pose challenges to the protection of individual privacy and intellectual property?
4. How have information systems affected laws for establishing accountability, liability, and the quality of everyday life?



WHAT ETHICAL, SOCIAL, AND POLITICAL ISSUES ARE RAISED BY INFORMATION SYSTEMS?

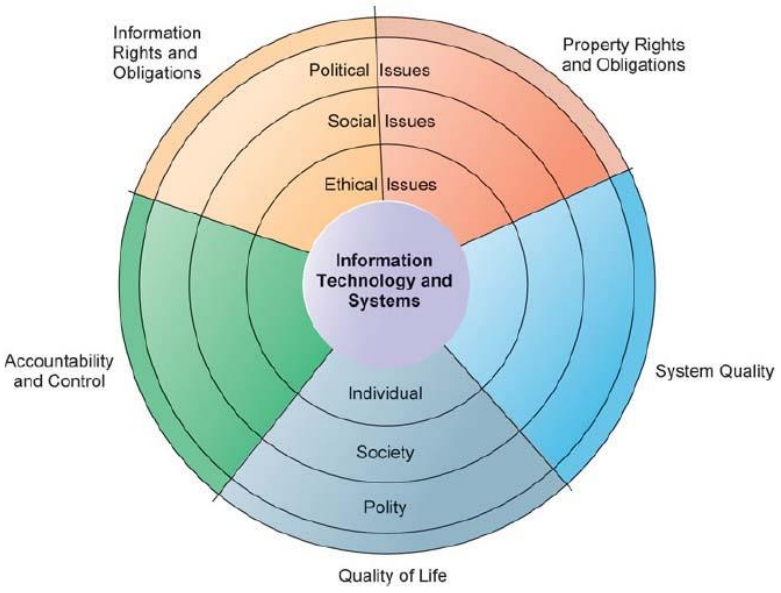
Ethics refers to the principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviors. Information systems raise new ethical questions for both individuals and societies because they create opportunities for intense social change, and thus threaten existing distributions of power, money, rights, and obligations. Like other technologies, such as steam engines, electricity, the telephone, and the radio, information technology can be used to achieve social progress, but it can also be used to commit crimes and threaten cherished social values. The development of information technology will produce benefits for many and costs for others. Ethical issues in information systems have been given new urgency by the rise of the Internet and electronic commerce. Internet and digital firm technologies make it easier than ever to assemble, integrate, and distribute information, unleashing new concerns about the appropriate use of customer information, the protection of personal privacy, and the protection of intellectual property.

Other pressing ethical issues raised by information systems include establishing accountability for the consequences of information systems, setting standards to safeguard system quality that protects the safety of the individual and society, and preserving values and institutions considered essential to the quality of life in an information society. When using information systems, it is essential to ask, "What is the ethical and socially responsible course of action?"

A MODEL FOR THINKING ABOUT ETHICAL, SOCIAL, AND POLITICAL ISSUES

Ethical, social, and political issues are closely linked. The ethical dilemma you may face as a manager of information systems typically is reflected in social and political debate. One way to think about these relationships is shown in Figure 4.1. Imagine society as a more or less calm pond on a summer day, a delicate ecosystem in partial equilibrium with individuals and with social and political institutions. Individuals know how to act in this pond because social institutions (family, education, organizations) have developed well-honed rules of behavior, and these are supported by laws developed in the political sector that prescribe behavior and promise sanctions for violations. Now toss a rock into the center of the pond. What happens? Ripples of course.

FIGURE 4.1 THE RELATIONSHIP BETWEEN ETHICAL, SOCIAL, AND POLITICAL ISSUES IN AN INFORMATION SOCIETY



The introduction of new information technology has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels. These issues have five moral dimensions: information rights and obligations, property rights and obligations, system quality, quality of life, and accountability and control.

The introduction of new information technology has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels. These issues have five moral

dimensions: information rights and obligations, property rights and obligations, system quality, quality of life, and accountability and control.

FIVE MORAL DIMENSIONS OF THE INFORMATION AGE

The major ethical, social, and political issues raised by information systems include the following moral dimensions:

- **Information rights and obligations.** What **information rights** do individuals and organizations possess with respect to themselves? What can they protect?
- **Property rights and obligations.** How will traditional intellectual property rights be protected in a digital society in which tracing and accounting for ownership are difficult and ignoring such property rights is so easy?
- **Accountability and control.** Who can and will be held accountable and liable for the harm done to individual and collective information and property rights?
- **System quality.** What standards of data and system quality should we demand to protect individual rights and the safety of society?
- **Quality of life.** What values should be preserved in an information- and knowledge-based society? Which institutions should we protect from violation? Which cultural values and practices are supported by the new information technology?

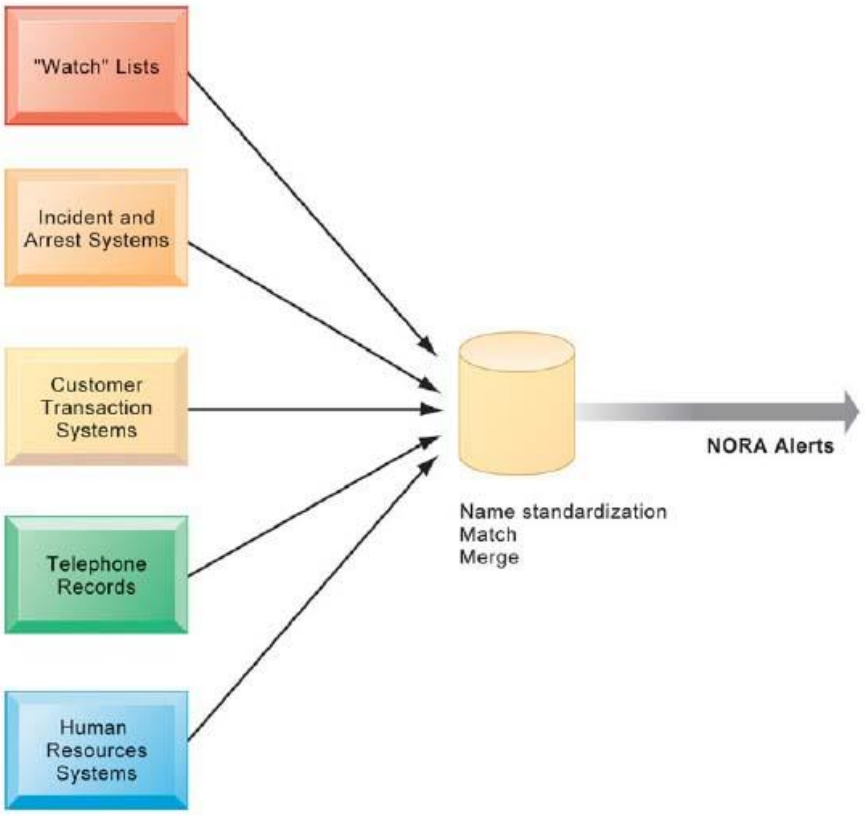
KEY TECHNOLOGY TRENDS THAT RAISE ETHICALISSUES

TABLE 4.2 TECHNOLOGY TRENDS THAT RAISE ETHICAL ISSUES

TREND	IMPACT
Computing power doubles every 18 months	More organizations depend on computer systems for critical operations.
Data storage costs rapidly decline	Organizations can easily maintain detailed databases on individuals.
Data analysis advances	Companies can analyze vast quantities of data gathered on individuals to develop detailed profiles of individual behavior.
Networking advances	The cost of moving data and making it accessible from anywhere falls exponentially .
Mobile device growth Impact	Individual cell phones may be tracked without user consent or knowledge.

A new data analysis technology called **non-obvious relationship awareness (NORA)** has given both the government and the private sector even more powerful profiling capabilities. NORA can take information about people from many disparate sources, such as employment applications, telephone records, customer listings, and “wanted” lists, and correlate relationships to find obscure hidden connections that might help identify criminals or terrorists (see Figure 4.2). NORA technology scans data and extracts information as the data are being generated so that it could, for example, instantly discover a man at an airline ticket counter who shares a phone number with a known terrorist before that person boards an airplane. The technology is considered a valuable tool for homeland security but does have privacy implications because it can provide such a detailed picture of the activities and associations of a single individual.

FIGURE 4.2 NONOBVIOUS RELATIONSHIP AWARENESS (NORA)



WHAT SPECIFIC PRINCIPLES FOR CONDUCT CAN BE USED TO GUIDE ETHICAL DECISIONS?

BASIC CONCEPTS: RESPONSIBILITY, ACCOUNTABILITY, AND LIABILITY

Ethical choices are decisions made by individuals who are responsible for the consequences of their actions. **Responsibility** is a key element of ethical action. Responsibility means that you accept the potential costs, duties, and obligations for the decisions you make. **Accountability** is a feature of systems and social institutions: It means that mechanisms are in place to determine who took responsible action, and who is responsible. Systems and institutions in which it is impossible to find out who took what action are inherently incapable of ethical analysis or ethical action. **Liability** extends the concept of responsibility further to the area of laws. Liability is a feature of political systems in which a body of laws is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations. **Due process** is a related feature of law- overned societies and is a process in which laws are known and understood, and there is an ability to appeal to higher authorities to ensure that the laws are applied correctly.

ETHICAL ANALYSIS

When confronted with a situation that seems to present ethical issues, how should you analyze it? The following five-step process should help:

1. **Identify and describe the facts clearly.** Find out who did what to whom, and where, when, and how. In many instances, you will be surprised at the errors in the initially reported facts, and often you will find that simply getting the facts straight helps define the solution. It also helps to get the opposing parties involved in an ethical dilemma to agree on the facts.
2. **Define the conflict or dilemma and identify the higher-order values involved.** Ethical, social, and political issues always reference higher values. The parties to a dispute all claim to be pursuing higher values (e.g., freedom, privacy, protection of property, and the free enterprise system). Typically, an ethical issue involves a dilemma: two diametrically opposed courses of action that support worthwhile values. For example, the chapter-opening case study illustrates two competing values: the need to improve access to digital content and the need to respect the property rights of the owners of that content.
3. **Identify the stakeholders.** Every ethical, social, and political issue has stakeholders: players in the game who have an interest in the outcome, who have invested in the situation, and usually who have

vocal opinions. Find out the identity of these groups and what they want. This will be useful later when designing a solution.

4. **Identify the options that you can reasonably take.** You may find that none of the options satisfy all the interests involved, but that some options do a better job than others. Sometimes arriving at a good or ethical solution may not always be a balancing of consequences to stakeholders.
5. **Identify the potential consequences of your options.** Some options may be ethically correct but disastrous from other points of view. Other options may work in one instance but not in other similar instances. Always ask yourself, "What if I choose this option consistently over time?"

CANDIDATE ETHICAL PRINCIPLES

Once your analysis is complete, what ethical principles or rules should you use to make a decision? What higher-order values should inform your judgment? Although you are the only one who can decide which among many ethical principles you will follow, and how you will prioritize them, it is helpful to consider some ethical principles with deep roots in many cultures that have survived throughout recorded history:

1. Do unto others as you would have them do unto you (the **Golden Rule**). Putting yourself into the place of others, and thinking of yourself as the object of the decision, can help you think about fairness in decision making.
2. If an action is not right for everyone to take, it is not right for anyone (**Immanuel Kant's Categorical Imperative**). Ask yourself, "If everyone did this, could the organization, or society, survive?"
3. If an action cannot be taken repeatedly, it is not right to take at all. This is the slippery-slope rule: An action may bring about a small change now that is acceptable, but if it is repeated, it would bring unacceptable changes in the long run. In the vernacular, it might be stated as "once started down a slippery path, you may not be able to stop."
4. Take the action that achieves the higher or greater value (**Utilitarian Principle**). This rule assumes you can prioritize values in a rank order and understand the consequences of various courses of action.
5. Take the action that produces the least harm or the least potential cost (**Risk version Principle**). Some actions have extremely high failure costs of very low probability (e.g., building a nuclear generating facility in an urban area) or extremely high failure costs of moderate probability (speeding and automobile accidents). Avoid these high-failure-cost actions, paying greater attention to high-failure-cost potential of moderate to high probability.
6. Assume that virtually all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise. (This is the **ethical "no free lunch" rule**.) If something someone else has created is useful to you, it has value, and you should assume the creator wants compensation for this work. Actions that do not easily pass these rules deserve close attention and a great deal of caution. The appearance of unethical behavior

WHY DO CONTEMPORARY INFORMATION SYSTEMS TECHNOLOGY AND THE INTERNET POSE CHALLENGES TO THE PROTECTION OF INDIVIDUAL PRIVACY AND INTELLECTUAL PROPERTY?

INFORMATION RIGHTS: PRIVACY AND FREEDOM IN THE INTERNET AGE

Privacy is the claim of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state. Claims to privacy are also involved at the workplace: Millions of employees are subject to electronic and other forms of high-tech surveillance. Information technology and systems threaten individual claims to privacy by making the invasion of privacy cheap, profitable, and effective.

Fair Information Practices (FIP) is a set of principles governing the collection and use of information about individuals. FIP principles are based on the notion of a mutuality of interest between the record holder and the individual. The individual has an interest in engaging in a transaction, and the record keeper—usually a business or government agency—requires information about the individual to support the transaction. Once information is gathered, the individual maintains an interest in the record, and the record may not be used to support other activities without the individual's consent. In 1998, the FTC restated and extended the original FIP to provide guidelines for protecting online privacy. Table 4.4 describes the FTC's Fair Information Practice principles.

FEDERAL TRADE COMMISSION FAIR INFORMATION PRACTICE PRINCIPLES

1. Notice/awareness (core principle). Web sites must disclose their information practices before collecting data. Includes identification of collector; uses of data; other recipients of data; nature of collection (active/inactive); voluntary or required status; consequences of refusal; and steps taken to protect confidentiality, integrity, and quality of the data.
2. Choice/consent (core principle). There must be a choice regime in place allowing consumers to choose how their information will be used for secondary purposes other than supporting the transaction, including internal use and transfer to third parties.
3. Access/participation. Consumers should be able to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.
4. Security. Data collectors must take responsible steps to assure that consumer information is accurate and secure from unauthorized use.
5. Enforcement. There must be in place a mechanism to enforce FIP principles. This can involve self-regulation, legislation giving consumers legal remedies for violations, or federal statutes and regulations.

Internet Challenges to Privacy

Internet technology has posed new challenges for the protection of individual privacy. Information sent over this vast network of networks may pass through many different computer systems before it reaches its final destination. Each of these systems is capable of monitoring, capturing, and storing communications that pass through it.

Web sites track searches that have been conducted, the Web sites and Web pages visited, the online content a person has accessed, and what items that person has inspected or purchased over the Web. This monitoring and tracking of Web site visitors occurs in the background without the visitor's knowledge. It is conducted not just by individual Web sites but by advertising networks such as Microsoft Advertising, Yahoo, and Google's Double Click that are capable of tracking personal browsing behavior across thousands of Web sites. Both Web site publishers and the advertising industry defend tracking of individuals across the Web because doing so allows more relevant ads to be targeted to users, and it pays for the cost of publishing Web sites. In this sense, it's like broadcast television: advertiser-supported content that is free to the user. The commercial demand for this personal information is virtually insatiable. However, these practices also impinge on individual privacy, as discussed in the Interactive Session on Technology.

Cookies are small text files deposited on a computer hard drive when a user visits Web sites. Cookies identify the visitor's Web browser software and track visits to the Web site. When the visitor returns to a site that has stored a cookie, the Web site software will search the visitor's computer, find the cookie, and know what that person has done in the past. It may also update the cookie, depending on the activity during the visit.

Web beacons, also called Web bugs (or simply "tracking files"), are tiny software programs that keep a record of users' online clickstream and report this data back to whomever owns the tracking file invisibly embedded in e-mail messages and Web pages that are designed to monitor the behavior of the user visiting a Web site or sending e-mail. Web beacons are placed on popular Web sites by third-party firms who pay the Web sites a fee for access to their audience.

Technical Solutions

In addition to legislation, there are a few technologies that can protect user privacy during interactions with Web sites. Many of these tools are used for encrypting e-mail, for making e-mail or surfing activities appear anonymous, for preventing client computers from accepting cookies, or for detecting and eliminating spyware. For the most part, technical solutions have failed to protect users from being tracked as they move from one site to another.

PROPERTY RIGHTS: INTELLECTUAL PROPERTY

Intellectual property is subject to a variety of protections under three different legal traditions: trade secrets, copyright, and patent law.

Trade Secrets

Any intellectual work product—a formula, device, pattern, or compilation of data—used for a business purpose can be classified as a **trade secret**, provided it is not based on information in the public domain. Protections for trade secrets vary from state to state. In general, trade secret laws grant a monopoly on the ideas behind a work product, but it can be a very tenuous monopoly. Software that contains novel or unique elements, procedures, or compilations can be included as a trade secret. Trade secret law protects the actual ideas in a work product, not only their manifestation. To make this claim, the creator or owner must

take care to bind employees and customers with nondisclosure agreements and to prevent the secret from falling into the public domain.
The limitation of trade secret protection is that, although virtually all software programs of any complexity contain unique elements of some sort, it is difficult to prevent the ideas in the work from falling into the public domain when the software is widely distributed.

Copyright
Copyright is a statutory grant that protects creators of intellectual property from having their work copied by others for any purpose during the life of the author plus an additional 70 years after the author's death. For corporate-owned works, copyright protection lasts for 95 years after their initial creation. Congress has extended copyright protection to books, periodicals, lectures, dramas, musical compositions, maps, drawings, artwork of any kind, and motion pictures. The intent behind copyright laws has been to encourage creativity and authorship by ensuring that creative people receive the financial and other benefits of their work. Most industrial nations have their own copyright laws, and there are several international conventions and bilateral agreements through which nations coordinate and enforce their laws.

Patents
A **patent** grants the owner an exclusive monopoly on the ideas behind an invention for 20 years. The congressional intent behind patent law was to ensure that inventors of new machines, devices, or methods receive the full financial and other rewards of their labor and yet make widespread use of the invention possible by providing detailed diagrams for those wishing to use the idea under license from the patent's owner. The granting of a patent is determined by the United States Patent and Trademark Office and relies on court rulings. The key concepts in patent law are originality, novelty, and invention.

Challenges to Intellectual Property Rights
Contemporary information technologies, especially software, pose severe challenges to existing intellectual property regimes and, therefore, create significant ethical, social, and political issues. Digital media differ from books, periodicals, and other media in terms of ease of replication; ease of transmission; ease of alteration; difficulty in classifying a software work as a program, book, or even music; compactness—making theft easy; and difficulties in establishing uniqueness.

The proliferation of electronic networks, including the Internet, has made it even more difficult to protect intellectual property. Before widespread use of networks, copies of software, books, magazine articles, or films had to be stored on physical media, such as paper, computer disks, or videotape, creating some hurdles to distribution. Using networks, information can be more widely reproduced and distributed. The Ninth Annual Global Software Piracy Study conducted by International Data Corporation and the Business Software Alliance reported that the rate of global software piracy climbed to 42 percent in 2013, representing $73 billion in global losses from software piracy. Worldwide, for every $100 worth of legitimate software sold that year, an additional $75 worth was obtained illegally (Business Software Alliance, 2014).

The Internet was designed to transmit information freely around the world, including copyrighted information. With the World Wide Web in particular, you can easily copy and distribute virtually anything to thousands and even millions of people around the world, even if they are using different types of computer systems. Information can be illicitly copied from one place and distributed through other systems and networks even though these parties do not willingly participate in the infringement.

Individuals have been illegally copying and distributing digitized music files on the Internet for several decades. File-sharing services such as Napster, and later Grokster, Kazaa, and Morpheus, Megaupload, The Pirate Bay, sprung up to help users locate and swap digital music and video files, including those protected by copyright. Illegal file sharing became so widespread that it threatened the viability of the music recording industry and, at one point, consumed 20 percent of Internet bandwidth. The recording industry won several legal battles for shutting these services down, but it has not been able to halt illegal file sharing entirely. The motion picture and cable television industries are waging similar battles, as described in the chapter-opening case study. Several European nations have worked with U.S. authorities to shut down illegal sharing sites, with mixed results. In France, illegal downloaders can lose access to the Internet for a year or more.

The Digital Millennium Copyright Act (DMCA) of 1998 also provides some copyright protection. The DMCA implemented a World Intellectual Property Organization Treaty that makes it illegal to circumvent technology-based protections of copyrighted materials. Internet service providers (ISPs) are required to take down sites of copyright infringers they are hosting once the ISPs are notified of the problem.

HOW HAVE INFORMATION SYSTEMS AFFECTED LAWS FOR STABLISHING ACCOUNTABILITY, LIABILITY, AND THE QUALITY OF EVERYDAY LIFE?

COMPUTER-RELATED LIABILITY PROBLEMS

SYSTEM QUALITY: DATA QUALITY AND SYSTEM ERRORS

QUALITY OF LIFE: EQUITY, ACCESS, AND BOUNDARIES

- Balancing Power: Center Versus Periphery
- Rapidity of Change: Reduced Response Time to Competition
- Maintaining Boundaries: Family, Work, and Leisure
- Dependence and Vulnerability
- Computer Crime and Abuse
- Employment: Trickle-Down Technology and
- Reengineering Job Loss
- Equity and Access: Increasing Racial and Social Class Cleavages
- Health Risks: RSI, CVS, and Techno stress

CHAPTER # 02: DECISION SUPPORT SYSTEMS

A. Decision Support in Business

Information, Decisions, and Management

Levels of management decision making still exist, but their size, shape, and participants continue to change as today's fluid organizational structures evolve. Thus, the levels of managerial decision making that must be supported by information technology in a successful organization are:

- **Strategic Management.** Typically, a board of directors and an executive committee of the CEO and top executives develop overall organizational goals, strategies, policies, and objectives as part of a strategic planning process. They also monitor the strategic performance of the organization and its overall direction in the political, economic, and competitive business environment.
- **Tactical Management.** Increasingly, business professionals in self-directed teams as well as business unit managers develop short- and medium-range plans, schedules, and budgets and specify the policies, procedures, and business objectives for their subunits of the company. They also allocate resources and monitor the performance of their organizational subunits, including departments, divisions, process teams, project teams, and other workgroups.
- **Operational Management.** The members of self-directed teams or operating managers develop short-range plans such as weekly production schedules. They direct the use of resources and the performance of tasks according to procedures and within budgets and schedules they establish for the teams and other workgroups of the organization.

Information Quality

What characteristics of information products make them valuable and useful to you? To answer this important question, we must first examine the characteristics or attributes of information quality. Information that is outdated, inaccurate, or hard to understand is not very meaningful, useful, or valuable to you or other business professionals. People need information of high quality, that is, information products whose characteristics, attributes, or qualities make the information more valuable to them. It is useful to think of information as having the three dimensions of time, content, and form. Figure 10.3 summarizes the important attributes of information quality and groups them into these three dimensions.

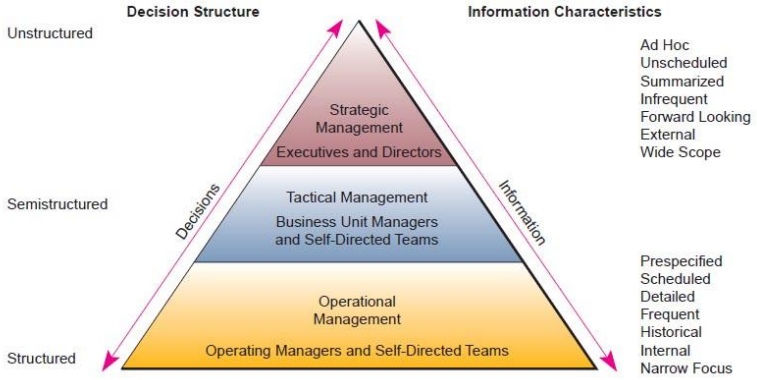
Time Dimension	
Timeliness	Information should be provided when it is needed.
Currency	Information should be up-to-date when it is provided.
Frequency	Information should be provided as often as needed.
Time Period	Information can be provided about past, present, and future time periods.
Content Dimension	
Accuracy	Information should be free from errors.
Relevance	Information should be related to the information needs of a specific recipient for a specific situation.
Completeness	All the information that is needed should be provided.
Conciseness	Only the information that is needed should be provided.
Scope	Information can have a broad or narrow scope, or an internal or external focus.
Performance	Information can reveal performance by measuring activities accomplished, progress made, or resources accumulated.
Form Dimension	
Clarity	Information should be provided in a form that is easy to understand.
Detail	Information can be provided in detail or summary form.
Order	Information can be arranged in a predetermined sequence.
Presentation	Information can be presented in narrative, numeric, graphic, or other forms.
Media	Information can be provided in the form of printed paper documents, video displays, or other media.

Decision Structure

Decisions made at the operational management level tend to be more structured, those at the tactical level are more semi-structured, and those at the strategic management level are more unstructured. Structured decisions involve situations in which the procedures to follow, when a decision is needed, can be specified in advance. The inventory reorder decisions that most businesses face are a typical example.

Unstructured decisions involve decision situations in which it is not possible to specify in advance most of

the decision procedures to follow. Most decisions related to long-term strategy can be thought of as unstructured (e.g., "What product lines should we develop over the next five years?").
Most business decision situations are semi-structured; that is, some decision procedures can be pre-specified but not enough to lead to a definite recommended decision. For example, decisions involved in starting a new line of e-commerce services or making major changes to employee benefits would probably range from unstructured to semi-structured.
Finally, decisions that are unstructured are those for which no procedures or rules exist to guide the decision makers toward the correct decision. In these types of decisions, many sources of information must be accessed, and the decision often rests on experience and "gut feeling." One example of an unstructured decision might be the answer to the question, "What business should we be in 10 years from now?"

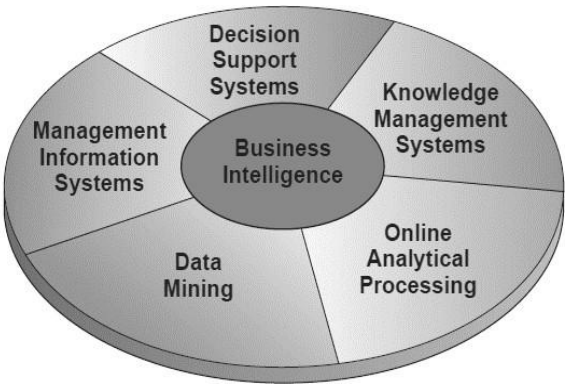


- **Business Intelligence (BI):** refers to all applications and technologies in the organisation that are focused on the gathering and analysis of data and information that can be used to derive strategic business decisions.

Differences between business analytics and business intelligence: Business analytics focuses on developing new insights and understanding of business performance based on data and statistical methods. In contrast, business intelligence traditionally focuses on using a consistent set of metrics to both measure past performance and guide business planning, which is also based on data and statistical methods. Business analytics makes much more extensive use of data, statistical and quantitative analysis, explanatory and predictive modeling, and fact-based management to drive decision making. Analytics may be used as input for human decisions or may drive fully automated decisions. Business intelligence is more associated with querying, reporting, online analytical processing (OLAP), and "alerts." In other words, querying, reporting, OLAP, and alert tools can answer the questions: what happened; how many; how often; where; where exactly is the problem; and what actions are needed. Business analytics, in contrast, can answer the questions: why is this happening; what if these trends continue; what will happen next (that is, predict); and what is the best that can happen (that is, optimize).

Figure 10.7 highlights several major information technologies that are being customized, personalized, and Web-enabled to provide key business information and analytical tools for managers, business professionals, and business stakeholders.

FIGURE 10.7
Business intelligence applications are based on personalized and Web-enabled information analysis, knowledge management, and decision support technologies.



Decision Support Systems
Decision support systems are computer-based information systems that provide interactive information support to managers and business professionals during the decision making process. Decision support

systems use (1) analytical models, (2) specialized databases, (3) a decision maker's own insights and judgments, and (4) an interactive, computer-based modeling process to support semi-structured business decisions. For example, Sales managers typically rely on management information systems to produce sales analysis reports. These reports contain sales performance figures by product line, salesperson, sales region, and so on. A decision support system (DSS), however, would also interactively show a sales manager the effects on sales performance of changes in a variety of factors (e.g., promotion expense and salesperson compensation). The DSS could then use several criteria (e.g., expected gross margin and market share) to evaluate and rank alternative combinations of sales performance factors.

DSS Components

Unlike management information systems, decision support systems rely on model bases, as well as databases, as vital system resources. A DSS model base is a software component that consists of models used in computational and analytical routines that mathematically express relationships among variables. For example, a spreadsheet program might contain models that express simple accounting relationships among variables, such as Revenue 2 Expenses 5 Profit. A DSS model base could also include models and analytical techniques used to express much more complex relationships. For example, it might contain linear programming models, multiple regression forecasting models, and capital budgeting present value models. Such models may be stored in the form of spreadsheet models or templates, or statistical and mathematical programs and program modules. In addition, DSS software packages can combine model components to create integrated models that support specific types of decisions.

As businesses become more aware of the power of decision support systems, they are using them in ever-increasing areas of the business.

Management Information Systems

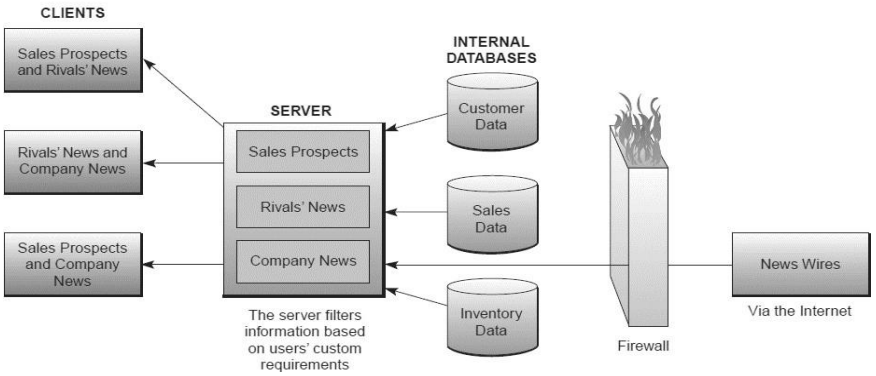
An MIS produces information products that support many of the day-to-day decision-making needs of managers and business professionals. Reports, displays, and responses produced by management information systems provide information that these decision makers have specified in advance as adequately meeting their information needs. Such predefined information products satisfy the information needs of decision makers at the operational and tactical levels of the organization who are faced with more structured types of decision situations. For example, sales managers rely heavily on sales analysis reports to evaluate differences in performance among salespeople who sell the same types of products to the same types of customers. They have a pretty good idea of the kinds of information about sales results (by product line, sales territory, customer, salesperson, and so on) that they need to manage sales performance effectively.

Management Reporting Alternatives

Management information systems provide a variety of information products to managers. Four major reporting alternatives are provided by such systems.

- **Periodic Scheduled Reports.** This traditional form of providing information to managers uses a pre-specified format designed to provide managers with information on a regular basis. Typical examples of such periodic scheduled reports are daily or weekly sales analysis reports and monthly financial statements.
- **Exception Reports. I**n some cases, reports are produced only when exceptional conditions occur. In other cases, reports are produced periodically but contain information only about these exceptional conditions. For example, a credit manager can be provided with a report that contains only information on customers who have exceeded their credit limits. Exception reporting reduces information overload instead of overwhelming decision makers with periodic detailed reports of business activity.
- **Demand Reports and Responses.** Information is available whenever a manager demands it. For example, Web browsers, DBMS query languages, and report generators enable managers at PC workstations to get immediate responses or to find and obtain customized reports as a result of their requests for the information they need. Thus, managers do not have to wait for periodic reports to arrive as scheduled.
- **Push Reporting.** Information is pushed to a manager's networked workstation. Thus, many companies are using Webcasting software to broadcast selectively reports and other information to the networked PCs of managers and specialists over their corporate intranets.

FIGURE 10.10 An example of the components in a marketing intelligence system that uses the Internet and a corporate intranet system to "push" information to employees.



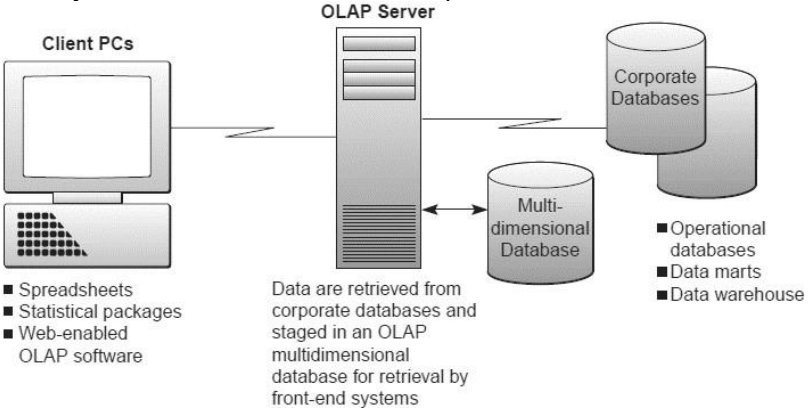
Online Analytical Processing

Online analytical processing (OLAP) enables managers and analysts to interactively examine and manipulate large amounts of detailed and consolidated data from many perspectives. OLAP involves analyzing complex relationships among thousands or even millions of data items stored in data marts, data warehouses, and other multidimensional databases to discover patterns, trends, and exception conditions. An OLAP session takes place online in real time, with rapid responses to a manager's or analyst's queries, so that the analytical or decision-making process is undisturbed.

Online analytical processing involves several basic analytical operations, including consolidation, "drill-down," and "slicing and dicing."

- **Consolidation.** Consolidation involves the aggregation of data, which can involve simple roll-ups or complex groupings involving interrelated data. For example, data about sales offices can be rolled up to the district level, and the district-level data can be rolled up to provide a regional-level perspective.
- **Drill-down.** OLAP can also go in the reverse direction and automatically display detailed data that comprise consolidated data. This process is called drill-down. For example, the sales by individual products or sales reps that make up a region's sales totals could be easily accessed.
- **Slicing and Dicing.** Slicing and dicing refers to the ability to look at the database from different viewpoints. One slice of the sales database might show all sales of a product type within regions. Another slice might show all sales by sales channel within each product type. Slicing and dicing is often performed along a time axis to analyze trends and find time-based patterns in the data.

FIGURE 10.11
Online analytical processing may involve the use of specialized servers and multidimensional databases. OLAP provides fast answers to complex queries posed by managers and analysts using traditional and Web-enabled OLAP software.



Geographic Information and Data Visualization Systems

A geographic information system is a DSS that uses geographic databases to construct and display maps, as well as other graphics displays that support decisions affecting the geographic distribution of people and other resources. Many companies are using GIS technology along with global positioning system (GPS) devices to help them choose new retail store locations, optimize distribution routes, or analyze the demographics of their target audiences.

Data visualization systems represent complex data using interactive, three-dimensional, graphical forms such as charts, graphs, and maps. DVS tools help users interactively sort, subdivide, combine, and organize data while the data are in their graphical form. This assistance helps users discover patterns, links, and anomalies in business or scientific data in an interactive knowledge discovery and decision support process. Business applications like data mining typically use interactive graphs that let users drill down in real time and manipulate the underlying data of a business model to help clarify their meaning for business decision making. Figure 10.14 is an example of airline flight analysis by a data visualization system.

Using Decision Support Systems

A decision support system involves an interactive analytical modeling process. For example, using a DSS software package for decision support may result in a series of displays in response to alternative what-if changes entered by a manager. This differs from the demand responses of management information systems because decision makers are not demanding pre-specified information; rather, they are exploring possible alternatives. Thus, they do not have to specify their information needs in advance. Instead, they use the DSS to find the information they need to help them make a decision. This is the essence of the decision support system concept.

Four basic types of analytical modeling activities are involved in using a decision support system: (1) what-if analysis, (2) sensitivity analysis, (3) goal-seeking analysis, and (4) optimization analysis. Let's briefly look at each type of analytical modeling that can be used for decision support.

What-If Analysis

In what-if analysis, a user makes changes to variables, or relationships among variables, and observes the resulting changes in the values of other variables.

Sensitivity Analysis

Sensitivity analysis is a special case of what-if analysis. Typically, the value of only one variable is changed repeatedly, and the resulting changes on other variables are observed. As such, sensitivity analysis is really a case of what-if analysis that involves repeated changes to only one variable at a time. Some DSS packages automatically make repeated small changes to a variable when asked to perform sensitivity analysis. Typically, decision makers use sensitivity analysis when they are uncertain about the assumptions made in estimating the value of certain key variables.

Goal-Seeking Analysis

Goal-seeking analysis reverses the direction of the analysis done in what-if and sensitivity analyses. Instead of observing how changes in a variable affect other variables, goal-seeking analysis (also called how-can analysis) sets a target value (goal) for a variable and then repeatedly changes other variables until the target value is achieved.

Optimization Analysis

Optimization analysis is a more complex extension of goal-seeking analysis. Instead of setting a specific target value for a variable, the goal is to find the optimum value for one or more target variables, given certain constraints. Then one or more other variables are changed repeatedly, subject to the specified constraints, until you discover the best values for the target variables.

FIGURE 10.16
Activities and examples of the major types of analytical modeling.

Type of Analytical Modeling	Activities and Examples
What-if analysis	Observing how changes to selected variables affect other variables. *Example:* What if we cut advertising by 10 percent? What would happen to sales?
Sensitivity analysis	Observing how repeated changes to a single variable affect other variables. *Example:* Let's cut advertising by $100 repeatedly so we can see its relationship to sales.
Goal-seeking analysis	Making repeated changes to selected variables until a chosen variable reaches a target value. *Example:* Let's try increases in advertising until sales reach $1 million.
Optimization analysis	Finding an optimum value for selected variables, given certain constraints. *Example:* What's the best amount of advertising to have, given our budget and choice of media?

Data Mining for Decision Support

Data mining's main purpose is to provide decision support to managers and business professionals through a process referred to as knowledge discovery. Data mining software analyzes the vast stores of historical business data that have been prepared for analysis in corporate data warehouses and tries to discover patterns, trends, and correlations hidden in the data that can help a company improve its business performance. Data mining software may perform regression, decision tree, neural network, cluster detection, or market basket analysis for a business.

Market basket analysis (MBA) is one of the most common and useful types of data mining for marketing and is a key technique in business analytics. The purpose of market basket analysis is to determine which products customers purchase together with other products. MBA takes its name from the concept of customers throwing all of their purchases into a shopping cart (a market basket) during grocery shopping.

Consider some of the typical applications of MBA:

- **Cross Selling.** Offer the associated items when customer buys any items from your store.
- **Product Placement.** Items that are associated (such as bread and butter, tissues and cold medicine, potato chips and beer) can be put near each other. If the customers see them, it has higher probability that they will purchase them together.
- **Affinity Promotion.** Design the promotional events based on associated products.
- **Survey Analysis.** The fact that both independent and dependent variables of market basket analysis are nominal (categorical) data type makes MBA very useful to analyze questionnaire data.
- **Fraud Detection.** Based on credit card usage data, we may be able to detect certain purchase behaviors that can be associated with fraud.
- **Customer Behavior.** Associating purchase with demographic, and socioeconomic data (such as age, gender, and preference) may produce very useful results for marketing.

Executive Information Systems

Executive information systems (EIS) are information systems that combine many of the features of management information systems and decision support systems. Thus, the first goal of executive information systems was to provide top executives with immediate and easy access to information about a firm's critical success factors (CSFs), that is, key factors that are critical to accomplishing an organization's strategic objectives.

Yet managers, analysts, and other knowledge workers use executive information systems so widely that they are sometimes humorously called "everyone's information systems." More popular alternative names are enterprise information systems (EIS) and executive support systems (ESS).

Features of an EIS

In an EIS, information is presented in forms tailored to the preferences of the executives using the system. Other information presentation methods used by an EIS include exception reporting and trend analysis. The ability to drill down, which allows executives to retrieve displays of related information quickly at lower levels of detail, is another important capability. Executive information systems have spread into the ranks of middle management and business professionals as their feasibility and benefits have been recognized and as less expensive systems for client/server networks and corporate intranets became available. For example, one popular EIS software package reports that only 3 percent of its users are top executives.

Enterprise Portals and Decision Support

Decision support in business is changing, driven by rapid developments in end-user computing and networking; Internet and Web technologies; and Web-enabled business applications. One of the key changes taking place in management information and decision support systems in business is the rapid growth of enterprise information portals.

Enterprise Information Portals

An enterprise information portal (EIP) is a Web-based interface and integration of MIS, DSS, EIS, and other technologies that give all intranet users and selected extranet users access to a variety of internal and external business applications and services. The business benefits of enterprise information portals include providing more specific and selective information to business users, providing easy access to key corporate intranet Web site resources, delivering industry and business news, and providing better access to company data for selected customers, suppliers, or business partners. Enterprise information portals can also help avoid excessive surfing by employees across company and Internet Web sites by making it easier for them to receive or find the information and services they need, thus improving the productivity of a company's workforce.

Knowledge Management Systems

In many organizations, hypermedia databases at corporate intranet Web sites have become the knowledge bases for storage and dissemination of business knowledge. This knowledge frequently takes the form of best practices, policies, and business solutions at the project, team, business unit, and enterprise levels of the company.

For many companies, enterprise information portals are the entry to corporate intranets that serve as their knowledge management systems. That's why such portals are called enterprise knowledge portals by their vendors. Thus, enterprise knowledge portals play an essential role in helping companies use their intranets as knowledge management systems to share and disseminate knowledge in support of business decision making by managers and business professionals.

B. Artificial Intelligence Technologies in Business

An Overview of Artificial Intelligence

Artificial intelligence (AI) is a field of science and technology based on disciplines such as computer science, biology, psychology, linguistics, mathematics, and engineering. The goal of AI is to develop computers that can simulate the ability to think, as well as see, hear, walk, talk, and feel. A major thrust of artificial intelligence is the simulation of computer functions normally associated with human intelligence, such as reasoning, learning, and problem solving.

British AI pioneer Alan Turing in 1950 proposed a test to determine whether machines could think. According to the Turing test, a computer could demonstrate intelligence if a human interviewer, conversing with an unseen human and an unseen computer, could not tell which was which.

One derivative of the Turing test that is providing real value to the online community is a CAPTCHA. A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a type of challenge-response test used in a wide variety of computing applications to determine that the user is really a human and not a computer posing as one. A CAPTCHA is sometimes described as a reverse Turing test because it is administered by a machine and targeted to a human, in contrast to the standard Turing test that is typically administered by a human and targeted to a machine. The process involves one computer (such as a server for a retail Web site) asking a user to complete a simple test that the computer is able to generate and grade. Because other computers are unable to solve the CAPTCHA, any user entering a correct solution is presumed to be human. A common type of CAPTCHA requires that the user type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen.

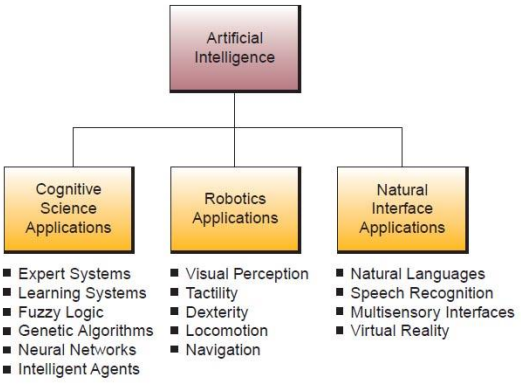
FIGURE 10.24
Some of the attributes of intelligent behavior. AI is attempting to duplicate these capabilities in computer-based systems.

Attributes of Intelligent Behavior
• Think and reason.
• Use reason to solve problems.
• Learn or understand from experience.
• Acquire and apply knowledge.
• Exhibit creativity and imagination.
• Deal with complex or perplexing situations.
• Respond quickly and successfully to new situations.
• Recognize the relative importance of elements in a situation.
• Handle ambiguous, incomplete, or erroneous information.

The Domains of Artificial Intelligence

AI applications can be grouped under three major areas—cognitive science, robotics, and natural interfaces—though these classifications do overlap, and other classifications can be used.

FIGURE 10.26
The major application areas of artificial intelligence. Note that the many applications of AI can be grouped into the three major areas of cognitive science, robotics, and natural interfaces.



Cognitive Science. This area of artificial intelligence is based on research in biology, neurology, psychology, mathematics, and many allied disciplines. It focuses on researching how the human brain works and how humans think and learn. The results of such research in human information processing are the basis for the development of a variety of computer-based applications in artificial intelligence.

Applications in the cognitive science area of AI includes the development of expert systems and other knowledge-based systems that add a knowledge base and some reasoning capability to information systems. Also included are **adaptive learning systems** that can modify their behaviors on the basis of information they acquire as they operate. Chess-playing systems are primitive examples of such applications, though many more applications are being implemented. **Fuzzy logic systems** can process data that are incomplete or ambiguous, that is, fuzzy data. Thus, they can solve semi-structured problems with incomplete knowledge by developing approximate inferences and answers, as humans do. **Neural network** software can learn by processing sample problems and their solutions. As neural nets start to recognize patterns, they can begin to program themselves to solve such problems on their own. **Genetic algorithm** software uses Darwinian (survival of the fittest), randomizing, and other mathematics functions to simulate evolutionary processes that can generate increasingly better solutions to problems. In addition, **intelligent agents** use expert system and other AI technologies to serve as software surrogates for a variety of end-user applications.

Robotics. AI, engineering, and physiology are the basic disciplines of robotics. This technology produces robot machines with computer intelligence and computer controlled, humanlike physical capabilities. This area thus includes applications designed to give robots the powers of sight, or visual perception; touch, or tactile capabilities; dexterity, or skill in handling and manipulation; locomotion, or the physical ability to move over any terrain; and navigation, or the intelligence to find one's way to a destination.

Natural Interfaces. The development of natural interfaces is considered a major area of AI applications and is essential to the natural use of computers by humans. For example, the development of natural languages and speech recognition are major thrusts of this area of AI. Being able to talk to computers and robots in conversational human languages and have them "understand" us as easily as we understand each other is a goal of AI research. This goal involves research and development in linguistics, psychology, computer science, and other disciplines. Other natural interface research applications include the development of multisensory devices that use a variety of body movements to operate computers, which is related to the emerging application area of virtual reality. Virtual reality involves using multisensory human–computer interfaces that enable human users to experience computer- simulated objects, spaces, activities, and "worlds" as if they actually exist.

Expert Systems

An expert system (ES) is a knowledge-based information system that uses its knowledge about a specific, complex application area to act as an expert consultant to end users. Expert systems provide answers to questions in a very specific problem area by making humanlike inferences about knowledge contained in a specialized knowledge base. They must also be able to explain their reasoning process and conclusions to a user, so expert systems can provide decision support to end users in the form of advice from an expert consultant in a specific problem area.

Components of an Expert System

The components of an expert system include a knowledge base and software modules that perform inferences on the knowledge in the knowledge base and communicate answers to a user's questions.

Knowledge Base. The knowledge base of an expert system contains (1) facts about a specific subject area (e.g., John is an analyst) and (2) heuristics (rules of thumb) that express the reasoning procedures of an expert on the subject (e.g., IF John is an analyst, THEN he needs a workstation). There are many ways that such knowledge is represented in expert systems. Examples are rule-based, frame-based, object-based, and case-based methods of knowledge representation. See Figure 10.29.

Software Resources. An expert system software package contains an inference engine and other programs for refining knowledge and communicating with users. The inference engine program processes the knowledge (such as rules and facts) related to a specific problem. It then makes associations and inferences resulting in recommended courses of action for a user.

FIGURE 10.28
A summary of four ways that knowledge can be represented in an expert system's knowledge base.

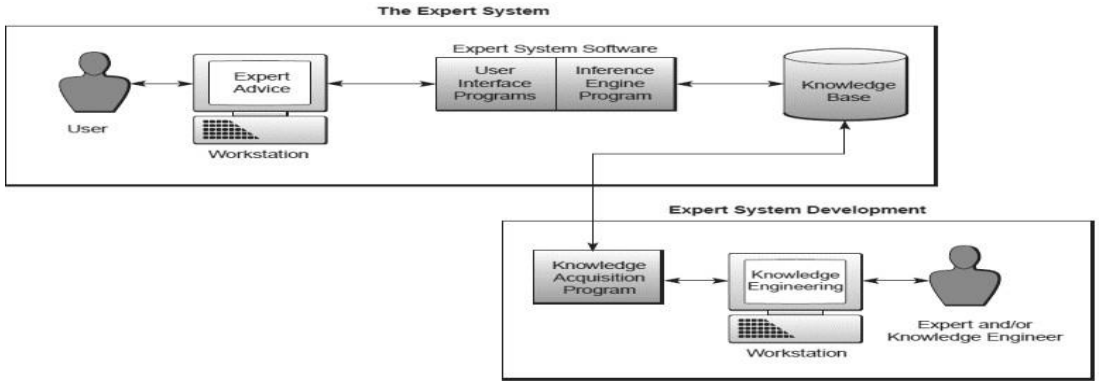
Methods of Knowledge Representation
• **Case-Based Reasoning.** Representing knowledge in an expert system's knowledge base in the form of cases, that is, examples of past performance, occurrences, and experiences.
• **Frame-Based Knowledge.** Knowledge represented in the form of a hierarchy or network of *frames*. A frame is a collection of knowledge about an entity consisting of a complex package of data values describing its attributes.
• **Object-Based Knowledge.** Knowledge represented as a network of objects. An object is a data element that includes both data and the methods or processes that act on those data.
• **Rule-Based Knowledge.** Knowledge represented in the form of rules and statements of fact. Rules are statements that typically take the form of a premise and a conclusion, such as If (condition), Then (conclusion).

Expert System Applications

Using an expert system involves an interactive computer-based session in which the solution to a problem is explored, with the expert system acting as a consultant to an end user. The expert system asks questions of the user, searches its knowledge base for facts and rules or other knowledge, explains its reasoning process when asked, and gives expert advice to the user in the subject area being explored. For example, Figure 10.30 illustrates an expert system application.

Expert systems are being used for many different types of applications, and the variety of applications is expected to continue to increase. You should realize, however, that expert systems typically accomplish one or more generic uses. Figure 10.31 outlines five generic categories of expert system activities, with specific examples of actual expert system applications. As you can see, expert systems are being used in many different fields, including medicine, engineering, the physical sciences, and business. Expert systems now help diagnose illnesses, search for minerals, analyze compounds, recommend repairs, and do financial planning. So from a strategic business standpoint, expert systems can be and are being used to improve every step of the product cycle of a business, from finding customers to shipping products to providing customer service.

FIGURE 10.29 Components of an expert system. The software modules perform inferences on a knowledge base built by an expert and/or knowledge engineer. This provides expert answers to an end user's questions in an interactive process.



Benefits of Expert Systems

An expert system captures the expertise of an expert or group of experts in a computer-based information system. Thus, it can outperform a single human expert in many problem situations. That's because an expert system is faster and more consistent, can have the knowledge of several experts, and does not get tired or distracted by overwork or stress. Expert systems also help preserve and reproduce the knowledge of experts. They allow a company to preserve the expertise of an expert before she leaves the organization. This expertise can then be shared by reproducing the software and knowledge base of the expert system.

Limitations of Expert Systems

The major limitations of expert systems arise from their limited focus, inability to learn, maintenance problems, and developmental cost. Expert systems excel only in solving specific types of problems in a limited domain of knowledge. They fail miserably in solving problems requiring a broad knowledge base and subjective problem solving. They do well with specific types of operational or analytical tasks but falter at subjective managerial decision making. Expert systems may also be difficult and costly to develop and maintain. The costs of knowledge engineers, lost expert time, and hardware and software resources may be too high to offset the benefits expected from some applications.

Application Categories of Expert Systems
• **Decision Management.** Systems that appraise situations or consider alternatives and make recommendations based on criteria supplied during the discovery process: Loan portfolio analysis Employee performance evaluation Insurance underwriting Demographic forecasts
• **Diagnostic/Troubleshooting.** Systems that infer underlying causes from reported symptoms and history: Equipment calibration Help desk operations Software debugging Medical diagnosis
• **Design/Configuration.** Systems that help configure equipment components, given existing constraints: Computer option installation Manufacturability studies Communications networks Optimum assembly plan
• **Selection/Classification.** Systems that help users choose products or processes, often from among large or complex sets of alternatives: Material selection Delinquent account identification Information classification Suspect identification
• **Process Monitoring/Control.** Systems that monitor and control procedures or processes: Machine control (including robotics) Inventory control Production monitoring Chemical testing

Developing Expert Systems

The easiest way to develop an expert system is to use an expert system shell as a developmental tool. An expert system shell is a software package consisting of an expert system without its kernel, that is, its knowledge base. This leaves a shell of software (the inference engine and user interface programs) with generic inferencing and user interface capabilities. Other development tools (e.g., rule editors, user interface generators) are added in making the shell a powerful expert system development tool.

FIGURE 10.32
Criteria for applications that are suitable for expert systems development.

Suitability Criteria for Expert Systems
• **Domain.** The domain, or subject area, of the problem is relatively small and limited to a well-defined problem area.
• **Expertise.** Solutions to the problem require the efforts of an expert. That is, a body of knowledge, techniques, and intuition is needed that only a few people possess.
• **Complexity.** Solution of the problem is a complex task that requires logical inference processing, which would not be handled as well by conventional information processing.
• **Structure.** The solution process must be able to cope with ill-structured, uncertain, missing, and conflicting data, and a problem situation that changes with the passage of time.
• **Availability.** An expert exists who is articulate and cooperative, and who has the support of the management and end users involved in the development of the proposed system.

Knowledge Engineering

A knowledge engineer is a professional who works with experts to capture the knowledge (facts and rules of thumb) they possess. The knowledge engineer then builds the knowledge base (and the rest of the expert system if necessary), using an iterative, prototyping process until the expert system is acceptable. Thus, knowledge engineers perform a role similar to that of systems analysts in conventional information systems development.

Once the decision is made to develop an expert system, a team of one or more domain experts and a knowledge engineer may be formed. Experts skilled in the use of expert system shells could also develop their own expert systems. If a shell is used, facts and rules of thumb about a specific domain can be defined and entered into a knowledge base with the help of a rule editor or other knowledge acquisition tool. A limited working prototype of the knowledge base is then constructed, tested, and evaluated using the inference engine and user interface programs of the shell. The knowledge engineer and domain experts can modify the knowledge base, and then retest the system and evaluate the results. This process is repeated until the knowledge base and the shell result in an acceptable expert system.

Neural Networks

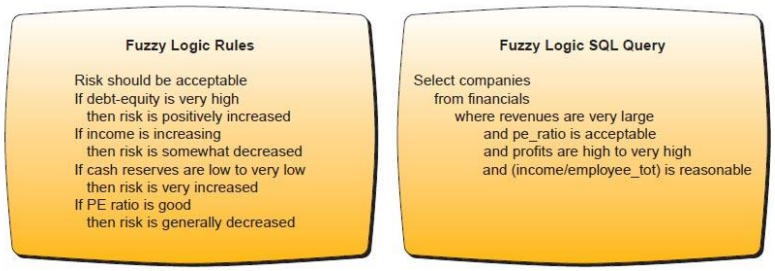
Neural networks are computing systems modeled after the brain's meshlike network of interconnected processing elements, called neurons. Of course, neural networks are a lot simpler in architecture (the human brain is estimated to have more than 100 billion neuron brain cells!). Like the brain, however, the

interconnected processors in a neural network operate in parallel and interact dynamically. This interaction enables the network to "learn" from data it processes. That is, it learns to recognize patterns and relationships in these data. The more data examples it receives as input, the better it can learn to duplicate the results of the examples it processes. Thus, the neural network will change the strengths of the interconnections between the processing elements in response to changing patterns in the data it receives and the results that occur.

Fuzzy Logic Systems

In spite of their funny name, fuzzy logic systems represent a small, but serious, application of AI in business. Fuzzy logic is a method of reasoning that resembles human reasoning, in that it allows for approximate values and inferences (fuzzy logic) and incomplete or ambiguous data (fuzzy data) instead of relying only on crisp data, such as binary (yes/no) choices.

FIGURE 10.35 An example of fuzzy logic rules and a fuzzy logic SQL query in a credit risk analysis application.



Fuzzy Logic in Business

Examples of applications of fuzzy logic are numerous in Japan but rare in the United States. The United States has preferred to use AI solutions like expert systems or neural networks, but Japan has implemented many fuzzy logic applications, especially the use of special- purpose fuzzy logic microprocessor chips, called fuzzy process controllers. Thus, the Japanese ride on subway trains, use elevators, and drive cars that are guided or supported by fuzzy process controllers made by Hitachi and Toshiba.

Genetic Algorithms

The use of genetic algorithms is a growing application of artificial intelligence. Genetic algorithm software uses Darwinian (survival of the fittest), randomizing, and other mathematical functions to simulate an evolutionary process that can yield increasingly better solutions to a problem. Genetic algorithms were first used to simulate millions of years in biological, geological, and ecosystem evolution in just a few minutes on a computer. Genetic algorithm software is being used to model a variety of scientific, technical, and business processes.

Genetic algorithms are especially useful for situations in which thousands of solutions are possible and must be evaluated to produce an optimal solution. Genetic algorithm software uses sets of mathematical process rules (algorithms) that specify how combinations of process components or steps are to be formed. This process may involve trying random process combinations (mutation), combining parts of several good processes (crossover), and selecting good sets of processes and discarding poor ones (selection) to generate increasingly better solutions.

Virtual Reality

Virtual reality (VR) is computer-simulated reality. Virtual reality is a fast-growing area of artificial intelligence that had its origins in efforts to build more natural, realistic, multisensory human–computer interfaces. So virtual reality relies on multisensory input/output devices such as a tracking headset with video goggles and stereo earphones, a data glove or jumpsuit with fiber-optic sensors that track your body movements, and a walker that monitors the movement of your feet. Then you can experience computer-simulated "virtual worlds" three- dimensionally through sight, sound, and touch. Virtual reality is also called tele-presence.

VR Applications

Current applications of virtual reality are wide-ranging and include computer-aided design (CAD), medical diagnostics and treatment, scientific experimentation in many physical and biological sciences, flight simulation for training pilots and astronauts, product demonstrations, employee training, and entertainment, especially 3-D video arcade games. CAD is the most widely used industrial VR application. It enables architects and other designers to design and test electronic 3-D models of products and structures by entering the models themselves and examining, touching, and manipulating sections and parts from all angles. This scientific-visualization capability is also used by pharmaceutical and biotechnology firms to develop and observe the behavior of computerized models of new drugs and materials and by medical

researchers to develop ways for physicians to enter and examine a virtual reality of a patient's body.
The hottest VR application today is Linden Lab's Second Life. Here, users can create avatars to represent them, teleport to any of the thousands of locations in Second Life, build personal domains, "buy" land, and live out their wildest fantasies. Second Life has grown to enormous proportions, although actual statistics regarding size and number of users are constantly in dispute. Today, Second Life is home to individuals, commercial organizations, universities, governments (the Maldives was the first country to open an embassy in Second Life), churches, sports entertainment, art exhibits, live music, and theater. Just about anything goes in Second Life and, as technologies advance, the lines between your first life and your second one may begin to blur—stay tuned.
It is believed by many that virtual reality will lead to a number of important changes in human life and activity. For example:

- Virtual reality will be integrated into daily life and activity and will be used in various human ways.
- Techniques will be developed to influence human behavior, interpersonal communication, and cognition (i.e., virtual genetics).
- As we spend more and more time in virtual space, there will be a gradual "migration to virtual space," resulting in important changes in economics, worldview, and culture.
- The design of virtual environments may be used to extend basic human rights into virtual space, to promote human freedom and well-being or to promote social stability as we move from one stage in sociopolitical development to the next.
- Virtual reality will soon engage all of the senses including smell, taste, and touch.

Intelligent Agents
Intelligent agents are growing in popularity as a way to use artificial intelligence routines in software to help users accomplish many kinds of tasks in e-business and e-commerce. An intelligent agent is a software surrogate for an end user or a process that fulfills a stated need or activity. An intelligent agent uses its built-in and learned knowledge base about a person or process to make decisions and accomplish tasks in a way that fulfills the intentions of a user. Sometimes an intelligent agent is given a graphic representation or persona, such as Einstein for a science advisor, Sherlock Holmes for an information search agent, and so on. Thus, intelligent agents (also called software robots or "bots") are special purpose, knowledge-based information systems that accomplish specific tasks for users.

FIGURE 10.38
Examples of different types of intelligent agents.

Types of Intelligent Agents
User Interface Agents
• **Interface Tutors.** Observe user computer operations, correct user mistakes, and provide hints and advice on efficient software use.
• **Presentation Agents.** Show information in a variety of reporting and presentation forms and media based on user preferences.
• **Network Navigation Agents.** Discover paths to information and provide ways to view information that are preferred by a user.
• **Role-Playing Agents.** Play what-if games and other roles to help users understand information and make better decisions.
Information Management Agents
• **Search Agents.** Help users find files and databases, search for desired information, and suggest and find new types of information products, media, and resources.
• **Information Brokers.** Provide commercial services to discover and develop information resources that fit the business or personal needs of a user.
• **Information Filters.** Receive, find, filter, discard, save, forward, and notify users about products received or desired, including e-mail, voice mail, and all other information media.

C. Understanding Blockchain Technology

Blockchains a network of databases spread across multiple entities that are kept in sync, where there is no single owner or controller of the data. The databases tend to be append-only, that is they can be written to, but historical data can't be altered without broad agreement from the participants of the network. This means that a user or system administrator in one entity can't alter data held on a blockchain without agreement from the other participants.

Purer than golden sources of data- Historically, when multiple parties need to rely on the same data, we have used golden sources of data, held and controlled by trusted third parties. A classic example is the use of a clearing house that is the golden source of data about a trade between two entities. Blockchains can empower groups of parties to agree on events without needing the third party, such is the promise of this new technology.

Benefits of Blockchains

Efficiency- No needs to reconcile data externally Blockchain technology could improve efficiency when financial entities are reconciling trades. A blockchain will mean that the agreed trade data is already in-house, removing the need to reconcile externally, as the blockchain has already done that in real time. The use of blockchains could also help speed up payments between financial entities. As blockchains can store data, they can also include code snippets that automate messages and one-day payments, using the "if-this-then-that" logic. If parties can agree upfront on the payoffs (usually this is agreed in term sheets written in dry legal language) and can encode the payoff terms into the trade details itself, then there can be efficiencies when trade lifecycle events take place, including error reduction and speed increases. These code snippets saved onto blockchains are called "smart contracts".

Transparency- A real time view of the trades With trade data published to a common platform, regulators or other interested parties can plug into this and get a real time view of the trades. This gives regulators oversight into one common source, rather than receiving reports in different formats at different times from each institution. By writing payoff structures onto a common platform in computer code which can be tested against, a smart contract on a blockchain provides for much higher levels of transparency over outcomes.

Resilience- The more the merrier Storing data over a large number of nodes benefits the resilience of the data – the larger the number of blockchain participants, the more robust the data, with longer life. In this respect, a blockchain system is similar to a massively replicated database.

Governance and Trust- Crowd-sourced honesty In a blockchain system, a majority of participants need to agree on data being added before it becomes part of the definitive blockchain. This is very different to central, often secretive ledgers held and controlled centrally. When multiple parties have a say over what data is written, the ability to alter data, or remove dubious data, it creates a more honest system.

Should Banks Be Excited?

Getting on the blockchain bandwagon- If you buy in to the media narrative, it's easy to see why there is so much interest in this space – the promise that for the first time in IT history, you can easily set up a write-only system that creates agreement between disparate entities about events, proven to be tamper-proof, and does not require a third party to host the data.

More and more applications- Initially, blockchains were thought of as a new way to gain efficiency and reduce risk and cost across the entire industry by offering a self-reconciling database for clearing trades. Since then, more applications are under exploration, from asset registration to shared storage of digital documents.

A 21st century central clearing house- The idea is that these processes could be replaced by systems that automatically share and reconcile events in real-time, resulting in all entities working from the same data, reducing cost and risk for the participants, much like using central clearing houses, but replacing the trusted third party with a technological solution where participants remain in control of their own data.

How blockchains can benefit financial services?

- **Current methods are prone to data corruption-** Each of these events are calculated multiple times in multiple systems and recorded in multiple ledgers. The current methods of reconciling separate ledgers are prone to breaks, missing information, and calculation differences. This leads to different versions of the events in different bank systems, increasing risk and associated time wasted investigating the source of these discrepancies.
- **One event, one version-** In a blockchain system, each event exists as one single version of the event stored onto a database and distributed to relevant parties. The blockchain consensus mechanism aligns all the entities to have the same view of the event. This happens without a third party, and it is enabled

by protocols that ensure that each entity independently checks that data conforms to the technical and business rules that they originally agreed upon.

- **Improves current trading-floor and control practices-** What this means for the front office is that it now has the ability to trade with other entities, with the same trade details being guaranteed for both entities. This is an improvement to current trading-floor practices where shorthand, typos, and misunderstandings can lead to trades being booked the wrong way around or with wrong details. In the backoffice, employees are kept busy creating and monitoring control processes, reconciling data between fragile legacy systems internally, and then reconciling the same data externally. For example, maintaining reference data, especially sensitive customer data, is a significant cost and risk to banks.
- **No need for third parties-** Blockchain technologies can negate the need for third parties to be involved in this kind of data management. This can be used for something as trivial as agreeing foreign exchange (FX) settlement holidays (the days on which specific currencies don't settle) through to having an industry view of counterparty data, which can be selectively revealed to trading counterparties.

Withering of trusted third parties in financial sector?

- **Third party risks-** In finance, trusted third parties are relied upon extensively. Entities such as clearing houses, central counterparties, exchanges for equities and futures all exist to reduce risk between financial institutions that may not trust one another fully but need to work together. However, while the problem of "golden source of truth" is solved, adding a third party creates new problems.
- **Technical failure-** The third party becomes a single point of potential failure. Technical failures occur and effects can be significant. For example, in October 2014, the Real Time Gross Settlement payment system in the UK, which is responsible for clearing hundreds of thousands of payment transactions worth £275 billion per day, went offline for ten hours. This led to delayed crucial payments and sparked the need for an independent review.
- **Data concentration attracts attacks-** The third party is at risk, both from external hackers and internal employees. The concentration of valuable data makes the third party an attractive target, both for reselling the data and for causing damage to the systems. Internal employees enjoy privileged access to data and systems. This increases and concentrates risk.
- **Disrupting third parties' monopolies-** Often, industry third parties have a monopoly and industry participants often don't have alternatives. As such, the incumbent industry utilities have no real incentive to offer competitive prices, no real incentive to produce superior customer experience, and no real incentive to innovate. For example SWIFT, an interbank messaging network and standardisation scheme used for sending messages about payments (and more), has such a grip on the banking sector that there is no real competition. Similarly, CLS (a specialist US financial institution) is the de-facto clearing mechanism for FX trades. Many countries use clearing houses for equity transactions. Each of these trusted third parties act as quasi-monopolies for their function.
- **Cross border legal complications-** International third parties add an additional element of legal risk, as they are in a specific jurisdiction that may be different to the jurisdictions where each party to a transaction is located. The government of the third party can subpoena data belonging to the trading counterparts, who are not in a position to keep their data private.
  There are many reasons why giving up trust, power, and control to third parties is undesirable. The potential of consensus distributed ledgers lies in the ability to remove the third party, yet still have participants agree on what the golden source of truth is.

Why You Should Be Excited Too

Bridging trust gaps- We believe that there are several environments where blockchains could solve problems, or at least reduce risk or increase efficiency. Blockchains are the ideal solution for mulitple entities that do not fully trust each other and need to agree on a single version of events, or require a data source that is tamper-proof. Blockchains could also add value where third parties are used either due to a low trust environment (such as escrow services) or as a golden source of truth.

How implementation of a blockchain can improve trust between stakeholders

Doing away with paper- Another place to look is where paper documentation is prevalent. Paper documents have historically been used in place of trust – instead of trusting the word of the merchant, you trust the paper certificate of authenticity. However, the world has evolved and paper certificates are easy to replicate or forge – easier than digitally signed digital documents. Blockchains can provide for digital records with guaranteed authenticity and uneditable audit records.

Technology trumps trust- Where digital records are held centrally by a single entity, there may be a place for blockchains – if trust in the entity is low or if the entity needs to demonstrate that the data is tamper-proof. This is because having the data on a blockchain demonstrates mathematically and systemically what an auditor had to accept on trust previously.

The promise of the technology is to replace the need to trust third parties with live, append-only databases with some level of compute logic, self-reconciled, and independently validated across multiple data centres and owners, containing uneditable, time-stamped records of the network-agreed truth.

Transaction ledgers

Exist only in ether impedes adoption- Bitcoin is a digital token whose ownership can be passed from user to user. This token has no real-life tangible representation, and as such is referred to as an 'on-chain' asset. That means, it exists on its blockchain, and owning the token reflects nothing else except that you own the token.

Opportunities in digitizing real assets- 'Off-chain' assets, by contrast, are real-world items (such as gold, shares, currency) that are digitally represented on a ledger by a token or tokens issued by an issuer. The issuer will safe- keep the real-world item and issue tokens on a ledger against them. The token represents a title deed for that asset and can be passed from user to user.

Event recording

Beyond ledgers any event can be "blockchained"- Moving away from the term 'ledger', with its financial connotations, events can also be recorded. An event could take the form of any sort of data and can be recorded in plain view or encrypted. Events in financial services could be anything from messages between entities to documents, meeting minutes to shareholder votes, counterparty data (e.g. mapping of legal entities to nostro accounts) to industry-agreed FX settlement holidays. The protection gained from using a blockchain is that the data cannot be edited once written, and has a trusted timestamp, without relying on an independent trusted third party.

Understanding the Technology

In its simplest form, a blockchain acts like a shared, replicated, append-only database where write access is shared among participants, but validation is performed by all participants. Taking the elements common to most blockchain systems, there is:

- A data store, usually containing financial transactions, but could contain any type of data
- Data replication across a number of systems in real-time
- Peer-to-peer network topology instead of hierarchical client-server models Usage of cryptography and digital signatures to prove identity, authenticity and enforce read/write access rights
- Mechanisms that make it hard to change historical records, and make it easy to detect when someone attempts to do so

How It Works?

Be part of the blockchain system network- To be a part of a blockchain system, participating entities will each install and run some software that connects their computer or server to other participants in the

network. By running this software, the participants act as individual validators, called network nodes.

- When a node connects to the network for the first time, it will download a full copy of the blockchain database onto its computer or server.
- The network of nodes manages the database, also known as the blockchain. The nodes are entry points for new data, as well as the validation and propagation of new data that have been submitted to the blockchain.
- But in a distributed system with no golden source of truth, how does the network come to consensus, or agree on what data to write on the blockchain? How do you resolve a situation where equivalent people can say conflicting things, but there is no boss to arbitrate?
- The answer – using protocols. In a blockchain system there will be protocol, i.e. pre-agreed rules for technical and business validity of data to be written, and a rule to determine how consensus is achieved.
- A block is created by grouping similar transactions together. These blocks are added in chronological order, in a way that resembles a chain, hence the name blockchain. The nodes then store these new blocks on the local blockchain database on their computer or server.

What about conflicting data entries?
One node may receive two pieces of mutually conflicting data. For example A is, "I sell all my shares to Alice," and B is, "I sell all my shares to Bob." Each node will have to keep one and reject one as they cannot both logically coexist.
An intuitive solution is for nodes to act on time priority, keeping the first and rejecting the second. However different nodes may hear the messages in different orders. The messages will propagate and some proportion of the network will believe A has happened (and B hasn't) and the rest of the network will believe B has happened (and A hasn't). The network is in an unstable state.
How is this resolved? Each node is working on its own version of the truth. Whichever node gets to add the next block will propagate its version of events, and all nodes will read this and act on the new 'truth'.

What about conflicting blocks?
Across a network, there is a possibility that two different blocks are added at the same time by different nodes, creating a fork in the chain. In this case, there is a 'consensus rule' that helps nodes figure out which is the block they should believe. In bitcoin, the rule is called the 'longest chain rule' – each node acknowledges the legitimacy of both contender blocks and the situation resolves when the next block is built on one of the contenders. The longer chain becomes part of the de-facto blockchain.

Public Versus Private Blockchains
Bitcoin blockchain is the grandfather of public blockchains- One of the breakthroughs of bitcoin was the ability to maintain a consensus view of transactions in a system, where anyone can create and send transactions, and anyone can write blocks of transactions to the ledger – all without needing the permission of higher authority. The bitcoin blockchain is the grandfather of public, or 'permissionless' blockchains – anyone can write data to it just by running some free software, and without signing up.
Conversely, private blockchains limit the participants using traditional methods, such as private networks with firewalls and IP whitelisting. A private blockchain can be set up so that known entities can add data to the blockchain, without letting external entities read or write access.
In finance and trade, in general, we have a set of known entities who are trying to legitimately do business with each other and who don't have a problem with revealing their identity. The issue before blockchains is that they may struggle to reach a common understanding of events. To solve that, they have always used third parties, such as banks and escrow services, which then involve a high amount of risk, or avoid the situation altogether.

Smoother information flows- So what is the difference between a private blockchain and existing third party systems? Blockchains can replace the need for data to flow from institutions to the third party and back. Instead, data flows between known institutions and comes to a consensus within a short period of time. This means that all parties can work from a single, known state of events. Encryption keeps private data private and digital signatures ensure authenticity, data integrity, and non-repudiation. Blockchains can solve the problem of needing to trust third parties.

Difference between public and private blockchains

Public blockchain, e.g. Bitcoin	Private blockchain
Anyone can write	Limited set of known entities can write
Anyone can read	Read-access is configurable

From Bitcoin to Blockchains: A Brief History

The first widely known and discussed blockchain was The Bitcoin Blockchain, and it serves as the de-facto example of how blockchain systems can work. The Bitcoin Blockchain is a database file that sits on thousands of computers worldwide, where the individual copies are kept aligned through the rules of the Bitcoin protocol. The Bitcoin Blockchain file (actually it is a series of files, because large files are difficult to manage) contains a list of every single bitcoin transaction that has ever happened: it is the ledger of record for Bitcoin and has been growing since January 2009.

The Bitcoin Blockchain is an open or 'permissionless' database. That is, should you wish to write entries to the database you may do so without signing up, logging in or asking permission from anyone in charge. In practice, this is done by downloading some open-source software and running it. By doing so, your computer will connect over the Internet to other computers running similar software. The software lets you start sending and receiving bitcoin transaction data with neighbours, and allow you to add data to the bitcoin blockchain, by playing a computationally intensive lottery known as 'mining'.

By studying The Bitcoin Blockchain file it is easy to see which bitcoin account has how many bitcoins and which accounts are sending bitcoins to whom. This transparency is needed so that the validators of the transactions determine whether a transaction is legitimate or not. For example, a bitcoin transaction that pays someone using bitcoins that don't exist would not be considered valid.

Other Blockchains

Ripple- Aims to dematerialise currencies and assets- Ripple sits somewhere between the public and private platforms and has a heavy reliance on validating nodes controlled by Ripple Inc. It aims to dematerialise currencies and assets by having customers park real-world assets with guardians called 'Ripple Gateways' who would issue tokens against the assets, just as goldsmiths issued receipts against gold deposits. The tokens can be sent between anyone with a Ripple account, traded for other tokens, and finally redeemed by sending them back to the guardian in return for the real-world item.

NXT- Uses 'proof-of-stake' as a block-adding mechanism- NXT is a public platform whose genesis block was created in November 2013. It works with a slightly different block-adding mechanism to bitcoin called 'proof-of-stake' instead of bitcoin's energy-intensive 'proof-of-work'. 'Proof-of-stake' distributes mining rewards in proportion to the balance of your account, as opposed to in proportion to how much electric power you are expending. The NXT platform includes more functionality than just sending tokens around (to date it has messaging, new token creation, new asset creation, a decentralised exchange, and a marketplace).

Ethereum- Its network acts as one giant consensus computing machine- Ethereum is a public platform and takes distributed computing one step further. The Ethereum network acts as one giant consensus computing machine instead of just a giant consensus database. The computations it is capable of are 'Turing-complete' meaning that it can calculate anything that any other computer can calculate, just a lot more slowly.

Ethereum's genesis block launched in July 2015 and the platform is currently one of the leading platforms for permissionless smart contracts.

When Blockchains Can be Used

lockchains have yet to find their niche for single entities where data governance is under one structure as general databases perform adequately. However, we see a role for blockchains when there are concerns around rogue employees, more secure logging (for any application), and also where regulators want to "plug in" to institutions to validate and see transactions in real time.

For example, currently system administrators with the right level of access can alter a database, and then modify log files to remove all traces of their activities. In the case of a distributed database running with nodes in separate data centres, a system administrator would need to have access to each of the data centres to make a change to an organisation's blockchain – a significantly harder task.

Improve National and Corporate Governance

Blockchain systems have a lot more potential between entities, i.e. where entities need to work with other entities to achieve a common goal. This is due to governance: Within an entity, bosses and the traditional hierarchy can mandate a golden source of truth and resolve conflict. However where entities interact, there needs to be another method for conflict resolution. The potential for blockchains to add value is higher if used collaboratively across an industry or a workflow.

It can protect the interests of entities within a nation if used appropriately, for example in invoice financing – if banks within a country can share data (without necessarily revealing the data to each other) about invoices that have been factored, then certain double invoicing scams can be avoided. Looking further afield, if an invoice can be issued on a blockchain by the issuer and signed, then you have a guaranteed unique digital record of the invoice that cannot be copied and cannot be financed more than once.

As Singapore looks to build a smart nation, blockchains can replace centralised registries with decentralised ledgers. With political will, Singapore can lead the way in creating trusted, tamper-proof repositories. Share registries, property, assets, insurance, and national identity can all be stored in secure blockchains, allowing for easier verification of "the truth", reduce settlement times when assets change hands, and by using smart contracts, even automated title transfers could be done when specific parameters are met. Digital identities can be used across systems without systems necessarily touching or interacting. One blockchain for identity, that is validated against when needed, and with the user in control of which data is shared with the merchant.

One of the most exciting advances would be for a national currency stored on a blockchain, enabling seamless payments that are much more secure and privacy-aware than credit cards. Disassociating the transmission of personally identifying information with the transmission of the payment would be a huge improvement over traditional systems.

Additionally, with smart contracts, logic can be written into accounts enabling payments to occur automatically when triggered by events. No longer will we need to rely on operations departments to follow straightforward "if this, then that" rules, and no longer will we need to chase down people who renege on a financial commitment. A smart nation would have front doors that unlock only if the rent has been paid, and have assets that automatically settle according to digital wills, reducing the need for costly probate.

Helps Facilitate Intra Asia Trade and Capital Flows

Spur regional trade- While attempts have been made to increase trade within the region, one of the biggest drags to success is low levels of trust in both businesses and political regimes. In Asia, this lack of trust has led to maintaining supply chains with known entities, where changes to the status quo are limited due to the risk of using new suppliers. New business relationships are slow to establish and often based on family ties and introductions by mutual trusted parties. By establishing digital credibility on an open system that is known to be fair and not under the influence of any politician, perhaps this can provide the lubrication that businesses need to open up.

Promote cross border investments and financing- Another example is in lending. Currently, the region has a huge amount of value tied up in assets such as buildings, plant, machinery, etc. If these assets could be recorded and verified on an independent ledger, outside the control of any specific third party or government, then loans can be made against the assets, releasing financing where previously it was impossible. In the initial stages, a blockchain could record ownership and changes of ownership of assets, but in the future, the financing leg could also live on a blockchain.

Hurdles for Adoption

- **Total transparency a double-edged sword-** Are we ready for blockchains? Often within organisations, whether businesses or governments, the ability to tweak historical data is a comfort blanket that may not be happily or easily forgone. Total transparency is somewhat of a double-edged sword. The demand for change here will come either from the grassroots demanding that certain data go on a blockchain and form a record which cannot be subsequently edited, or from regulators and policymakers mandating such change.
- **Requires a lot of coordination-** Having said that, blockchains are not just about transparency. Blockchains can also be used in industry platforms for the sharing of data that is helpful to the industry as a whole. In this case, a majority of players in an industry needs to come together and agree on what such a platform would look like, who would pay for it, and what value each participant would get from it. This isn't something that can be done overnight, and it is not a cheap exercise.
- **Costly to switch technologies-** Switching technologies also cost money. In any bank there are legacy systems that are old and inadequate, yet the cost/benefit of replacing the system doesn't make sense. Blockchain solutions will need to have a clear business case before being adopted outside of pet projects.

- **Regulatory clarity over data sovereignty-** Regulatory clarity of on- and off-chain assets is something that is often discussed, in the context of bitcoins and the issues of data governance of a share certificate on a blockchain. What is often neglected is regulatory clarity over data sovereignty. In an industry blockchain, the same data is copied over many data centres, often in different countries. A lot of the data are encrypted so that only the intended recipient can see it.
- **New-ness of blockchain technology-** Finally, the technology needs to clearly prove itself before conservative businesses take the plunge. We are still in the early stages as the technology is still immature and hasn't yet been proven at scale. In many of the situations outlined, data volume, transfer speed, and consensus speed will need to be increased significantly for this technology to prove useful given bitcoin is adding just up to 1 megabyte of data every ten minutes.

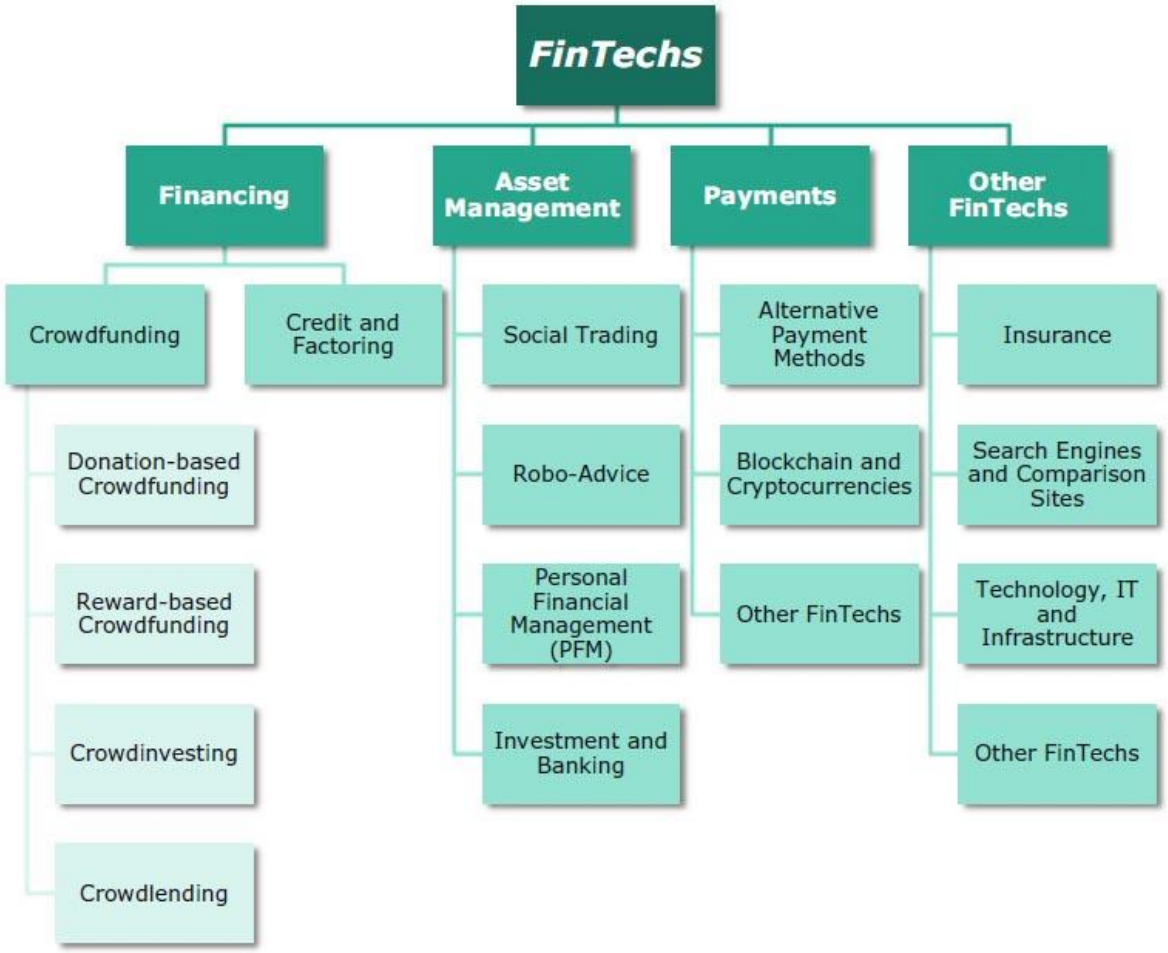
D. Understanding Fintech Technologies

Definition of FinTech

The term "FinTech," which is the short form of the phrase financial technology, denotes companies or representatives of companies that combine financial services with modern, innovative technologies.1 As a rule, new participants in the market offer Internet-based and application-oriented products. FinTechs generally aim to attract customers with products and services that are more user-friendly, efficient, transparent, and automated than those currently available. Traditional banks have not yet exhausted the possibilities for improvements along these lines (EBF 2015; Mackenzie 2015).

In addition to offering products and services in the banking sector, there are also FinTechs that distribute insurance and other financial instruments or provide third party services. In a generous sense of the term, "FinTech" encompasses companies that simply provide the technology (such as software solutions) to financial service providers. However, such companies are not dealt with in detail in this study.

Segments of the FinTech Industry



Companies in the FinTech industry can be divided into four major segments in accordance with their distinctive business models.

i. Financing;
ii. Asset Management;
iii. Payments;
iv. Other FinTechs.

1. **Financing:** The finance sector includes a FinTech segment that makes financing available for both private individuals and for businesses. This segment can be further divided into FinTechs whose offerings are based on the participation of a large number of contributors (the crowdfunding subsegment) and those that offer factoring services or credit without the participation of the crowd (the credit and factoring subsegment).

- **Crowdfunding** describes a form of financing in which a large number of contributors (often called "backers") provide the financial resources to achieve a common goal. In the place of a traditional bank, a crowdfunding portal acts as an intermediary.

  Crowdfunding portals can be **subdivided into four further sub-segments** on the basis of the kind of consideration given to investors for their investments.

While investors participating in **donation-based crowdfunding** receive no remuneration for their contributions (though they may derive indirect personal benefits through the act of donation; Andreoni 1989).

In reward-based crowdfunding they receive some form of non-monetary consideration. Such consideration can take the form of the right to pre-order a product or some other form of prestige, such as having the investor's name included in the credits of a funded film (Bradford 2012). Generally, there are no costs to individuals for initiating projects in the reward-based and donation based crowdfunding subsegments. Some portals charge a fee of between 5% and 11% of the total amount of funding in the case of a successful campaign. Other portals gain revenue through voluntary donations from investors and the initiators of the projects.

In the third subsegment, **crowdinvesting,** investors receive a share of equity, debt or hybrid ownership. The contracts used in crowdinvesting often simulate certain aspects of equity participation using a mezzanine instrument (Kl€ohn et al. 2016a). As a rule, crowdinvesting portals profit from the fees they receive from successfully financed companies. In Germany, this fee is 8% of the financed amount on average (Hornuf and Schwienbacher 2014). Recently crowdinvesting portals have also gained revenue from the future success of financed companies by requiring investors to deduct a certain share of a company's potential profits, its enterprise value and exit proceeds (carried interest) (Kl€ohn et al. 2016a). Generally speaking, portals handle relatively small sums in crowdinvesting campaigns. Kl€ohn et al. (2016b) show that by the middle of 2015 amounts of more than 1 million EUR had been collected from only five of the 174 crowdinvesting campaigns that had taken place in Germany by that date. However, these five successful campaigns correspond to 29% of the total volume of financing from successful campaigns.

The fourth subsegment, **crowdlending,** contains platforms that enable private individuals and businesses to secure loans from the crowd. In return for the provision of the loan, investors receive a pre-determined interest rate (Bradford 2012). In Germany, the market leaders in the crowdlending industry are financed by two types of fees. On the one hand, borrowers are charged a fee that depends on their creditworthiness and the duration of the loan. On the other hand, lenders are required to pay a certain percentage of the amount invested (often 1%) or one percentage point of the interest rate.

In addition there is the credit and factoring subsegment. FinTech businesses in this subsegment, generally in cooperation with a partner bank (or else a number of partner banks), extend credit to private individuals and businesses without recourse to the crowd. Loans are sometimes given over short-term periods of a few days or weeks via mobile phone. In addition, these FinTechs offer innovative factoring solutions, such as selling claims online or offering factoring solutions without a minimum requirement. As a rule, companies in the credit and factoring subsegment automate many of their processes, thereby enabling cost-effective, fast and efficient services.

The asset management segment includes FinTechs that offer advice, disposal and management of assets, and aggregated indicators of personal wealth. **This segment is also divided into further subsegments.**

Social trading is a form of investment in which investors (or "followers") can observe, discuss, and copy the investment strategies or portfolios of other members of a social network (Liu et al. 2014; Pentland 2013). Individual investors are supposed to benefit from the collective wisdom of a large number of traders. Depending on the business model of a social trading platform, users can be charged for spreads, order costs, or percentages of the amount invested.
In addition, innovative software solutions and computer systems play an important role in the business models of many FinTechs in the asset management segment.

The robo-advice subsegement refers to portfolio management systems that provide algorithm-based and largely automated investment advice, sometimes also making investment decisions (ESA 2015). Robo advisers' algorithms are generally based on passive investing and diversification strategies (Sironi 2016). They consider the investor's risk tolerance, the preferred duration of the investment, as well as other goals (Fein 2015). The German Federal Financial Supervisory Authority (Bundesanstalt f€ur Finanzdienstleistungsaufsicht—BaFin) (BaFin 2016a, b) also distinguishes between "automated investment advice," in which a one-off investment recommendation is given, and "automated financial portfolio management," which is characterized by ongoing recommendations. Since these two services often overlap, they are conflated in this study. Robo-advice providers are often financed by a fee withheld from investors that is proportionate to the sum of their investment. A performance-dependent fee is also charged.

The personal financial management (PFM) subsegment includes FinTech companies that offer private financial planning, in particular the administration and presentation of financial data using software or app-based services. PFMs enable clients to visualize the assets they have deposited with different financial institutions as well as loans borrowed from different lenders in one application. The app or software often requires a one-off or annual fee from users. In order to integrate the accounts of different providers into a PFM system, PFMs interface with the portals of financial institutions, which are frequently open-access, using application programming interface (API) technology (Glushko et al. 1999; Dapp 2015; Nienaber 2016). In many PFM systems, however, manual entry of the account data is also required.

There are also FinTech companies that offer innovative concepts for advising or managing assets that cannot be included in the social trading, robo-advice or PFM subsegments. These may be organized into two main groups. First, there is onlinebased asset management, in which human investment advisors actively interact with customers, though as with robo-advice they also automate or partially automate many processes. Secondly, there are deposit brokers, which arrange daily or fixed-term deposits in other EU countries and offer the opening of accounts as well as management on a German website. As a result of the EU-wide deposit guarantee scheme (Directive 2014/49/EU), using this business model it is possible to exploit interest rates from different countries. **These FinTechs are included in the investment and banking subsegment.** Also included in this subsegment are FinTechs that offer traditional banking products, such as a cash account with certain IT functionalities. By making efficient use of technologies and by abandoning cumbersome branch networks, these FinTechs can offer traditional banking products more costeffectively and quickly, as well as more user-friendly functionalities.

The payments segment is an umbrella term that applies to FinTechs whose applications and services concern national and international payment transactions. Under this umbrella is included the **blockchain and cryptocurrency subsegment,** which includes FinTechs that offer virtual currencies (cryptocurrency) as an alternative to typical fiat money. As with legal means of payment, it is possible to save, use, and exchange cryptocurrencies (BaFin 2016c). Banks are not needed to serve as intermediaries. One of the best-known cryptocurrencies is Bitcoin. Bitcoin, which has undergone large fluctuations in value in the past, has not yet been able to establish itself as a serious competitor with official currencies issued by central banks. There are more than 700 other virtual currencies that have not yet reached the level of market capitalization of Bitcoin (CoinMarketCap 2016a). As with most other digital payment systems, a blockchain is used to secure Bitcoin's transactions. With this technology, all transactions are registered and stored on a variety of servers. This makes it very difficult to falsify the information (Grinberg 2011; B€ohme et al. 2015). Even companies that do not themselves offer cryptocurrencies, but solely blockchain technology for financial services, are included in the **blockchain and cryptocurrency subsegment.**

FinTechs that offer alternative payment methods are included in the **alternative payment methods** subsegment. Companies that offer mobile payment solutions belong to this subsegment. In the scholarly literature, the term "mobile payment" generally encompasses various functionalities that are handled via mobile phones (see Mallat 2007; Mallat et al. 2004; Merritt 2010). This includes the use of the mobile phone to make payments or bank transfers. Companies that offer eWallets or cyberwallets are also included in the alternative payment methods subsegment. An eWallet is a system in which both digital currencies and

payment information for various payment systems can be stored. The payment information can then be used during the payment process without re-entering it using a mobile phone or the Internet. This enables very fast and user-friendly transactions (Mjølsnes and Rong 2003; Mallat 2007). Other innovative solutions for bank transfers or other payment methods are also included in the alternative payment methods subsegment. Some FinTechs in this subsegment, for example, offer the transfer of money between two individuals (peer-to-peer transfer). The money is often transferred in real time and thus is faster than in the traditional banking industry (Merritt 2010).

The other FinTechs segment describes FinTech businesses that cannot be classified by the other three traditional bank functions, i.e. financing, asset management and payment transactions. FinTechs that offer insurance or facilitate its acquisition are included in the insurance subsegment. These FinTechs are often also called InsurTechs. Among other things, they offer peer-to-peer-insurance, wherein a group of policyholders come together and assume collective liability in the case of damages. If no loss occurs within the group, there is partial reimbursement of the insurance premium (Wolff-Marting 2014). Furthermore, FinTechs of the search engines and comparison sites subsegment, which enable the Internet-based search and comparison of financial products or financial services, are included in other FinTechs. FinTechs that provide technical solutions for financial services providers are included in the Technology, IT and Infrastructure subsegment.

CHAPTER # 03: IT GOVERNANCE, ORGANISATION AND STRATEGY

A. IT Governance

What is IT governance?
Essentially, IT governance provides a structure for aligning IT strategy with business strategy. By following a formal framework, organizations can produce measurable results toward achieving their strategies and goals. A formal program also takes stakeholders' interests into account, as well as the needs of staff and the processes they follow. In the big picture, IT governance is an integral part of overall enterprise governance.

What's the relationship between IT governance and GRC (governance, risk and compliance)?
According to Calatayud, IT governance and GRC are practically the same thing. "While GRC is the parent program, what determines which framework is used is often the placement of the CISO and the scope of the security program. For example, when a CISO reports to the CIO, the scope of GRC is often IT focused. When security reports outside of IT, GRC can cover more business risks beyond IT."

Why do organizations implement IT governance infrastructures?
Organizations today are subject to many regulations governing the protection of confidential information, financial accountability, data retention and disaster recovery, among others. They're also under pressure from shareholders, stakeholders and customers.
To ensure they meet internal and external requirements, many organizations implement a formal IT governance program that provides a framework of best practices and controls.

What kind of organization uses IT governance?
Both public- and private-sector organizations need a way to ensure that their IT functions support business strategies and objectives. And a formal IT governance program should be on the radar of any organization in any industry that needs to comply with regulations related to financial and technological accountability. However, implementing a comprehensive IT governance program requires a lot of time and effort. Where very small entities might practice only essential IT governance methods, the goal of larger and more regulated organizations should be a full-fledged IT governance program.

How do you implement an IT governance program?
The easiest way is to start with a framework that's been created by industry experts and used by thousands of organizations. Many frameworks include implementation guides to help organizations phase in an IT governance program with fewer speedbumps.

CIO Leadership Live with Douglas Blackwell, CIO at Horizon Blue Cross Blue...

The most commonly used frameworks are:

COBIT: Published by ISACA, COBIT is a comprehensive framework of "globally accepted practices, analytical tools and models" (PDF) designed for governance and management of enterprise IT. With its roots in IT auditing, ISACA expanded COBIT's scope over the years to fully support IT governance. The latest version is COBIT 5, which is widely used by organizations focused on risk management and mitigation.

ITIL: Formerly an acronym for Information Technology Infrastructure Library, ITIL focuses on IT service management. It aims to ensure that IT services support core processes of the business. ITIL comprises five sets of management best practices for service strategy, design, transition (such as change management), operation and continual service improvement.

COSO: This model for evaluating internal controls is from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO's focus is less IT-specific than the other frameworks, concentrating more on business aspects like enterprise risk management (ERM) and fraud deterrence.

CMMI: The Capability Maturity Model Integration method, developed by the Software Engineering Institute, is an approach to performance improvement. CMMI uses a scale of 1 to 5 to gauge an organization's performance, quality and profitability maturity level. According to Calatayud, "allowing for mixed mode and objective measurements to be inserted is critical in measuring risks that are qualitative in nature."

FAIR: Factor Analysis of Information Risk (FAIR) is a relatively new model that helps organizations quantify risk. The focus is on cyber security and operational risk, with the goal of making more well-informed decisions. Although it's newer than other frameworks mentioned here, Calatayud points out that it's already gained a lot of traction with Fortune 500 companies.

How do I choose which framework to use?
Most IT governance frameworks are designed to help you determine how your IT department is functioning overall, what key metrics management needs and what return IT is giving back to the business from its investments.
Where COBIT and COSO are used mainly for risk, ITIL helps to streamline service and operations. Although CMMI was originally intended for software engineering, it now involves processes in hardware development, service delivery and purchasing. As previously mentioned, FAIR is squarely for assessing operational and cyber security risks.
When reviewing frameworks, consider your corporate culture. Does a particular framework or model seem like a natural fit for your organization? Does it resonate with your stakeholders? That framework is probably the best choice.
But you don't have to choose only one framework. For example, COBIT and ITIL complement one another in that COBIT often explains why something is done or needed where ITIL provides the "how." Some organizations have used COBIT and COSO, along with the ISO 27001 standard (for managing information security).

How do you ensure a smooth implementation and positive results?
One of the most important paths to success is with executive buy-in. Calatayud recommends forming a risk management committee with top-level sponsorships and business representation. "To ensure it's an effective program, it needs to be supported by a broad set of line of business leaders." He also recommends sharing results with the board or audit committee to "develop real attention when items begin to get ignored." As with any significant project, you should always keep communication lines open between various parties, measure and monitor the progress of the implementation, and seek outside help if needed.

B. IT Organisations and Strategy

Which features of organizations do managers need to know about to build and use information systems successfully?

Information systems and organizations influence one another. Information systems are built by managers to serve the interests of the business firm. At the same time, the organization must be aware of and open to the influences of information systems to benefit from new technologies.
The interaction between information technology and organizations is complex and is influenced by many mediating factors, including the organization's structure, business processes, politics, culture, surrounding environment, and management decisions.

FIGURE 3.1 THE TWO-WAY RELATIONSHIP BETWEEN ORGANIZATIONS AND INFORMATION TECHNOLOGY

This complex two-way relationship is mediated by many factors, not the least of which are the decisions made—or not made—by managers. Other factors mediating the relationship include the organizational culture, structure, politics, business processes, and environment.

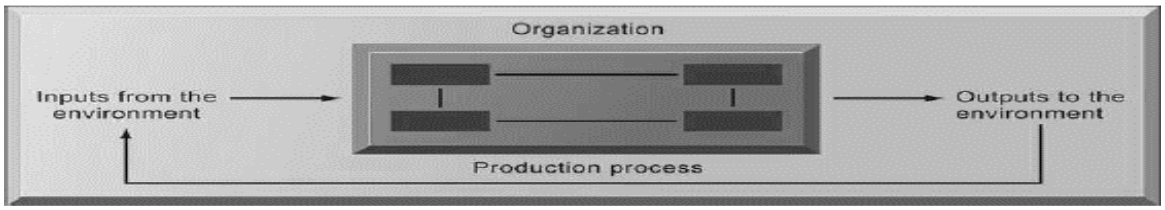
What Is An Organization?

Technical View
An **organization** is a stable, formal social structure that takes resources from the environment and processes them to produce outputs. This technical definition focuses on three elements of an organization. Capital and

labor are primary production factors provided by the environment. The organization (the firm) transforms these inputs into products and services in a production function. The products and services are consumed by environments in return for supply inputs.

Organizations are formal legal entities with internal rules and procedures that must abide by laws.
How do these definitions of organizations relate to information systems technology? A technical view of organizations encourages us to focus on how inputs are combined to create outputs when technology changes are introduced into the company.

FIGURE 3.2 THE TECHNICAL MICROECONOMIC DEFINITION OF THE ORGANIZATION



In the microeconomic definition of organizations, capital and labor (the primary production factors provided by the environment) are transformed by the firm through the production process into products and services (outputs to the environment). The products and services are consumed by the environment, which supplies additional capital and labor as inputs in the feedback loop.

Features of Organizations these are the features:

Routines and Business Processes
All organizations, including business firms, become very efficient over time because individuals in the firm develop **routines** for producing goods and services. Routines— sometimes called standard operating procedures—are precise rules, procedures, and practices that have been developed to cope with virtually all expected situations. As employees learn these routines, they become highly productive and efficient, and the firm is able to reduce its costs over time as efficiency increases.
Business processes are collections of such routines. A business firm, in turn, is a collection of business processes.

Organizational Politics
People in organizations occupy different positions with different specialties, concerns, and perspectives. As a result, they naturally have divergent viewpoints about how resources, rewards, and punishments should be distributed. These differences matter to both managers and employees, and they result in political struggle for resources, competition, and conflict within every organization.
Political resistance is one of the great difficulties of bringing about organizational change— especially the development of new information systems. Managers who know how to work with the politics of an organization will be more successful than less-skilled managers in implementing new information systems.

Organizational Culture
All organizations have bedrock, unassailable, unquestioned (by the members) assumptions that define their goals and products. Organizational culture encompasses this set of assumptions about what products the organization should produce, how it should produce them, where, and for whom. Generally, these cultural assumptions are taken totally for granted and are rarely publicly announced or discussed. Business processes—the actual way business firms produce value—are usually ensconced in the organization's culture.

Organizational Environments
Organizations reside in environments from which they draw resources and to which they supply goods and services. Organizations and environments have a reciprocal relationship. On the one hand, organizations are open to, and dependent on, the social and physical environment that surrounds them. Without financial and human resources—people willing to work reliably and consistently for a set wage or revenue from customers—organizations could not exist. Organizations must respond to legislative and other requirements imposed by government, as well as the actions of customers and competitors.

Organizational Structure
All organizations have a structure or shape. Mintzberg's classification identifies five basic kinds of organizational structure (Mintzberg,1979). The kind of information systems you find in a business firm—and the nature of problems with these systems—often reflects the type of organizational structure.

For instance, in a professional bureaucracy such as a hospital, it is not unusual to find parallel patient record systems operated by the administration, another by doctors, and another by other professional staff such as nurses and social workers. In huge multidivisional firms operating in hundreds of locations, you will often find there is not a single integrating information system, but instead each locale or each division has its set of information systems.

Other Organizational Features

Organizations have different goals (coercive goals (e.g., prisons); utilitarian goals (e.g., businesses) normative goals (universities, religious groups) and use different means to achieve them.

Organizations also serve different groups or have different constituencies, some primarily benefiting their members, others benefiting clients, stockholders, or the public.

The nature of leadership differs greatly from one organization to another—some organizations may be more democratic or authoritarian than others.

Another way organizations differ is by the tasks they perform and the technology they use. Some organizations perform primarily routine tasks that can be reduced to formal rules that require little judgment (such as manufacturing auto parts), whereas others (such as consulting firms) work primarily with non-routine tasks.

TABLE 3.2 ORGANIZATIONAL STRUCTURES

ORGANIZATIONAL TYPE	DESCRIPTION	EXAMPLES
Entrepreneurial structure	Young, small firm in a fast-changing environment. It has a simple structure and is managed by an entrepreneur serving as its single chief executive officer.	Small start-up business
Machine bureaucracy	Large bureaucracy existing in a slowly changing environment, producing standard products. It is dominated by a centralized management team and centralized decision making.	Midsize manufacturing firm
Divisionalized bureaucracy	Combination of multiple machine bureaucracies, each producing a different product or service, all topped by one central headquarters.	Fortune 500 firms, such as General Motors
Professional bureaucracy	Knowledge-based organization where goods and services depend on the expertise and knowledge of professionals. Dominated by department heads with weak centralized authority.	Law firms, school systems, hospitals
Adhocracy	Task force organization that must respond to rapidly changing environments. Consists of large groups of specialists organized into short-lived multidisciplinary teams and has weak central management.	Consulting firms, such as the Rand Corporation

What is the impact of information systems on organizations?

Economic Impacts

IT changes both the relative costs of capital and the costs of information. Information systems technology can be viewed as a factor of production that can be substituted for traditional capital and labor. As the cost of information technology decreases, it is substituted for labor, which historically has been a rising cost. As the cost of information technology decreases, it also substitutes for other forms of capital such as buildings and machinery, which remain relatively expensive. Information technology helps firms contract in size because it can reduce transaction costs. As transaction costs decrease, firm size (the number of employees) should shrink. Information technology, especially the use of networks, can help firms lower the cost of market participation. Information technology also can reduce internal management costs.

Organizational and Behavioral Impacts

Theories based in the sociology of complex organizations also provide some understanding about how and why firms change with the implementation of new IT applications.

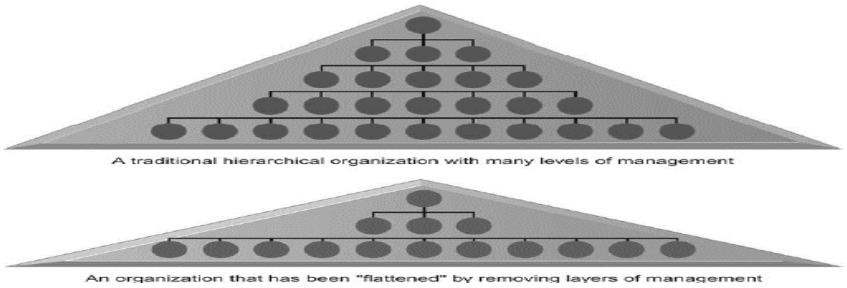
IT Flattens Organizations

Large, bureaucratic organizations, which primarily developed before the computer age, are often inefficient, slow to change, and less competitive than newly created organizations. Some of these large organizations have downsized, reducing the number of employees and the number of levels in their organizational hierarchies.

Behavioral researchers have theorized that information technology facilitates flattening of hierarchies by broadening the distribution of information to empower lower-level employees and increase management

efficiency. IT pushes decision-making rights lower in the organization because lower-level employees receive the information they need to make decisions without supervision.
Managers now receive so much more accurate information on time, they become much faster at making decisions, so fewer managers are required. Management costs decline as a percentage of revenues, and the hierarchy becomes much more efficient.

FIGURE 3.6 FLATTENING ORGANIZATIONS



Information systems can reduce the number of levels in an organization by providing managers with information to supervise larger numbers of workers and by giving lower-level employees more decision-making authority.

Postindustrial Organizations
Postindustrial theories based more on history and sociology than economics also support the notion that IT should flatten hierarchies. In postindustrial societies, authority increasingly relies on knowledge and competence, and not merely on formal positions. Hence, the shape of organizations flattens because professional workers tend to be self-managing, and decision making should become more decentralized as knowledge and information become more widespread throughout the firm (Drucker, 1988).

Understanding Organizational Resistance to Change
Organizational resistance to change is so powerful, many information technology investments flounder and do not increase productivity. There are several ways to visualize organizational resistance. Research on organizational resistance to innovation suggests that four factors are paramount: the nature of the IT innovation, the organization's structure, the culture of people in the organization, and the tasks impacted by the innovation.

The Internet and Organizations

The Internet, especially the World Wide Web, has an important impact on the relationships between many firms and external entities, and even on the organization of business processes inside a firm. The Internet increases the accessibility, storage, and distribution of information and knowledge for organizations. In essence, the Internet is capable of dramatically lowering the transaction and agency costs facing most organizations. Businesses are rapidly rebuilding some of their key business processes based on Internet technology and making this technology a key component of their IT infrastructures. If prior networking is any guide, one result will be simpler business processes, fewer employees, and much flatter organizations than in the past.

Implications for the Design and Understanding Of Information Systems

To deliver genuine benefits, information systems must be built with a clear understanding of the organization in which they will be used. In our experience, the central organizational factors to consider when planning a new system are the following:

- The environment in which the organization must function
- The structure of the organization: hierarchy, specialization, routines, and business processes
- The organization's culture and politics
- The type of organization and its style of leadership the principal interest groups affected by the system and the attitudes of workers who will be using the system
- The kinds of tasks, decisions, and business processes that the information system is designed to assist

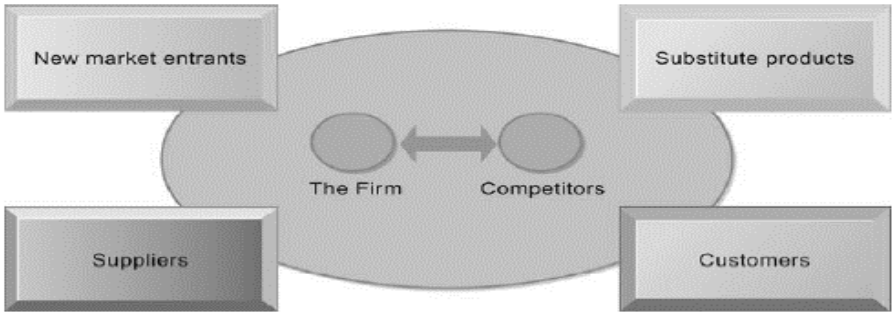
How do porter's competitive forces model, the value chain model, synergies, core competencies, and network economics help companies develop competitive strategies using information systems?
Why do some firms do better than others and how do they achieve competitive advantage? How can you analyze a business and identify its strategic advantages? How can you develop a strategic advantage for your own business? And how do information systems contribute to strategic advantages? One answer to

that question is Michael Porter's competitive forces model.

Porter's Competitive Forces Model

Arguably, the most widely used model for understanding competitive advantage is Michael Porter's **competitive forces model** (see Figure 3.8). This model provides a general view of the firm, its competitors, and the firm's environment. In this model, five competitive forces shape the fate of the firm.

FIGURE 3.8 PORTER'S COMPETITIVE FORCES MODEL



In Porter's competitive forces model, the strategic position of the firm and its strategies are determined not only by competition with its traditional direct competitors but also by four other forces in the industry's environment: new market entrants, substitute products, customers, and suppliers.

Traditional Competitors

All firms share market space with other competitors who are continuously devising new, more efficient ways to produce by introducing new products and services, and attempting to attract customers by developing their brands and imposing switching costs on their customers.

New Market Entrants

In a free economy with mobile labor and financial resources, new companies are always entering the marketplace. In some industries, there are very low barriers to entry, whereas in other industries, entry is very difficult. For instance, it is fairly easy to start a pizza business or just about any small retail business, but it is much more expensive and difficult to enter the computer chip business, which has very high capital costs and requires significant expertise and knowledge that is hard to obtain.

Substitute Products and Services

In just about every industry, there are substitutes that your customers might use if your prices become too high. New technologies create new substitutes all the time. Internet and wireless telephone service can substitute for traditional telephone service. The more substitute products and services in your industry, the less you can control pricing and the lower your profit margins.

Customers

A profitable company depends in large measure on its ability to attract and retain customers (while denying them to competitors), and charge high prices. The power of customers grows if they can easily switch to a competitor's products and services, or if they can force a business and its competitors to compete on price alone in a transparent marketplace where there is little **product differentiation**, and all prices are known instantly (such as on the Internet). For instance, in the used college textbook market on the Internet, students (customers) can find multiple suppliers of just about any current college textbook. In this case, online customers have extraordinary power over used-book firms.

Suppliers

The market power of suppliers can have a significant impact on firm profits, especially when the firm cannot raise prices as fast as can suppliers. The more different suppliers a firm has, the greater control it can exercise over suppliers in terms of price, quality, and delivery schedules. For instance, manufacturers of laptop PCs almost always have multiple competing suppliers of key components, such as keyboards, hard drives, and display screens.

Information System Strategies for Dealing with Competitive Forces

What is a firm to do when it is faced with all these competitive forces? And how can the firm use information systems to counteract some of these forces? How do you prevent substitutes and inhibit new market entrants? There are four generic strategies, each of which often is enabled by using information technology and systems: low-cost leadership, product differentiation, focus on market niche, and strengthening

customer and supplier intimacy.

Low-Cost Leadership
Use information systems to achieve the lowest operational costs and the lowest prices. The classic example is Walmart. By keeping prices low and shelves well stocked using a legendary inventory replenishment system, Walmart became the leading retail business in the United States. Point-of-sale terminals record the bar code of each item passing the checkout counter and send a purchase transaction directly to a central computer at Walmart headquarters. The computer collects the orders from all Walmart stores and transmits them to suppliers. Suppliers can also access Walmart's sales and inventory data using Web technology. Walmart's continuous replenishment system is also an example of an **efficient customer response system**.

Product Differentiation
Use information systems to enable new products and services, or greatly change the customer convenience in using your existing products and services. For instance, Google continuously introduces new and unique search services on its Web site, such as Google Maps. Manufacturers and retailers are using information systems to create products and services that are customized and personalized to fit the precise specifications of individual customers. For example, Nike sells customized sneakers through its NIKEiD program on its Web site.

Focus on Market Niche
Use information systems to enable a specific market focus, and serve this narrow target market better than competitors. Information systems support this strategy by producing and analyzing data for finely tuned sales and marketing techniques. Information systems enable companies to analyze customer buying patterns, tastes, and preferences closely so that they efficiently pitch advertising and marketing campaigns to smaller and smaller target markets.

Strengthen Customer and Supplier Intimacy
Use information systems to tighten linkages with suppliers and develop intimacy with customers. Chrysler Corporation uses information systems to facilitate direct access by suppliers to production schedules, and even permits suppliers to decide how and when to ship supplies to Chrysler factories. This allows suppliers more lead time in producing goods. On the customer side, Amazon keeps track of user preferences for book and CD purchases, and can recommend titles purchased by others to its customers. Strong linkages to customers and suppliers increase **switching costs** (the cost of switching from one product to a competing product), and loyalty to your firm.

TABLE 3.4 FOUR BASIC COMPETITIVE STRATEGIES

STRATEGY	DESCRIPTION	EXAMPLE
Low-cost leadership	Use information systems to produce products and services at a lower price than competitors while enhancing quality and level of service	Walmart
Product differentiation	Use information systems to differentiate products, and enable new services and products	Google, eBay, Apple, Lands' End
Focus on market niche	Use information systems to enable a focused strategy on a single market niche; specialize	Hilton Hotels, Harrah's
Customer and supplier intimacy	Use information systems to develop strong ties and loyalty with customers and suppliers	Chrysler Corporation, Amazon

TABLE 3.5 IMPACT OF THE INTERNET ON COMPETITIVE FORCES AND INDUSTRY STRUCTURE

COMPETITIVE FORCE	IMPACT OF THE INTERNET
Substitute products or services	Enables new substitutes to emerge with new approaches to meeting needs and performing functions
Customers' bargaining power	Availability of global price and product information shifts bargaining power to customers
Suppliers' bargaining power	Procurement over the Internet tends to raise bargaining power over suppliers; suppliers can also benefit from reduced barriers to entry and from the elimination of distributors and other intermediaries standing between them and their users
Threat of new entrants	Internet reduces barriers to entry, such as the need for a sales force, access to channels, and physical assets; it provides a technology for driving business processes that makes other things easier to do
Positioning and rivalry among existing competitors	Widens the geographic market, increasing the number of competitors, and reducing differences among competitors; makes it more difficult to sustain operational advantages; puts pressure to compete on price

THE INTERNET'S IMPACT ON COMPETITIVE ADVANTAGE

Because of the Internet, the traditional competitive forces are still at work, but competitive rivalry has become much more intense (Porter, 2001). Internet technology is based on universal standards that any company can use, making it easy for rivals to compete on price alone and for new competitors to enter the market. Because information is available to everyone, the Internet raises the bargaining power of customers, who can quickly find the lowest-cost provider on the Web. Profits have been dampened. Table 3.5 summarizes some of the potentially negative impacts of the Internet on business firms identified by Porter.

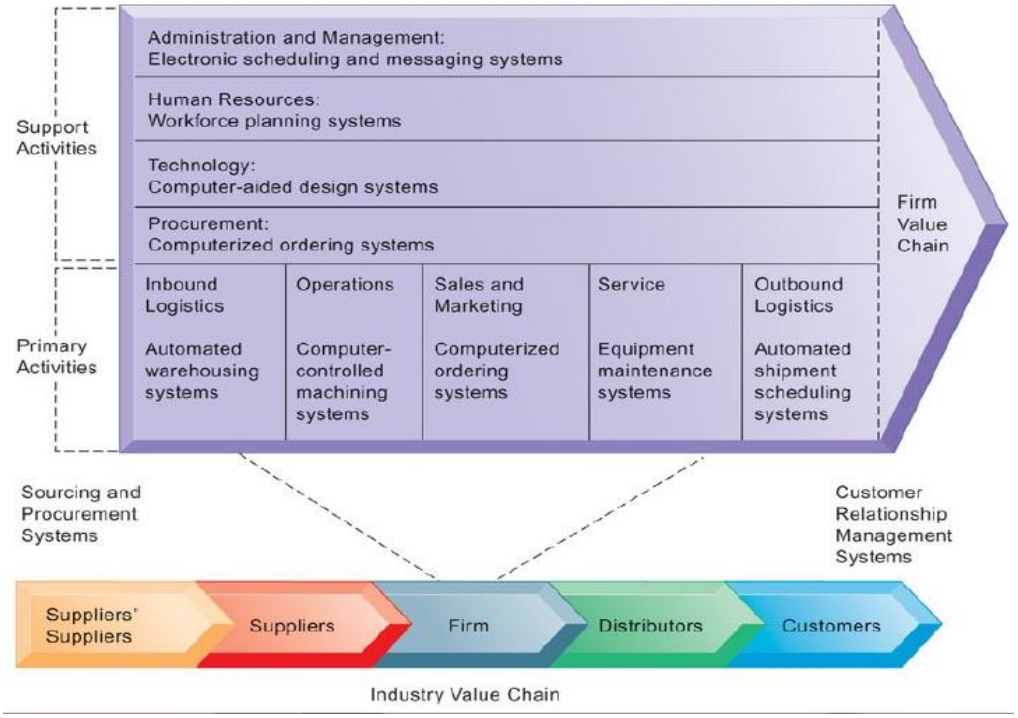
The Internet has nearly destroyed some industries and has severely threatened more. For instance, the printed encyclopedia industry and the travel agency industry have been nearly decimated by the availability of substitutes over the Internet. Likewise, the Internet has had a significant impact on the retail, music, book, retail brokerage, software, telecommunications, and newspaper industries.

However, the Internet has also created entirely new markets, formed the basis for thousands of new products, services, and business models, and provided new opportunities for building brands with very large and loyal customer bases.

THE BUSINESS VALUE CHAIN MODEL

Although the Porter model is very helpful for identifying competitive forces and suggesting generic strategies, it is not very specific about what exactly to do, and it does not provide a methodology to follow for achieving competitive advantages. If your goal is to achieve operational excellence, where do you start? Here's where the business value chain model is helpful.

FIGURE 3.9 THE VALUE CHAIN MODEL



The **value chain model** highlights specific activities in the business where competitive strategies can best be applied (Porter, 1985) and where information systems are most likely to have a strategic impact. This model identifies specific, critical leverage points where a firm can use information technology most effectively to enhance its competitive position. The value chain model views the firm as a series or chain of basic activities that add a margin of value to a firm's products or services. These activities can be categorized as either primary activities or support activities.

Primary activities are most directly related to the production and distribution of the firm's products and services, which create value for the customer. Primary activities include inbound logistics, operations, outbound logistics, sales and marketing, and service. Inbound logistics includes receiving and storing materials for distribution to production. Operations transforms inputs into finished products. Outbound logistics entails storing and distributing finished products. Sales and marketing includes promoting and selling the firm's products. The service activity includes maintenance and repair of the firm's goods and services.

Support activities make the delivery of the primary activities possible and consist of organization infrastructure (administration and management), human resources (employee recruiting, hiring, and training), technology (improving products and the production process), and procurement (purchasing input).

Using the business value chain model will also cause you to consider benchmarking your business processes against your competitors or others in related industries, and identifying industry best practices. **Benchmarking** involves comparing the efficiency and effectiveness of your business processes against strict standards and then measuring performance against those standards. Industry **best practices** are usually identified by consulting companies, research organizations, government agencies, and industry associations as the most successful solutions or problem-solving methods for consistently and effectively achieving a business objective.

Extending the Value Chain: The Value Web

How can information systems be used to achieve strategic advantage at the industry level? By working with other firms, industry participants can use information technology to develop industry-wide standards for exchanging information or business transactions electronically, which force all market participants to subscribe to similar standards. Such efforts increase efficiency, making product substitution less likely and perhaps raising entry costs—thus discouraging new entrants. Also, industry members can build industry-wide, IT-supported consortia, symposia, and communications networks to coordinate activities concerning government agencies, foreign competition, and competing industries.

Internet technology has made it possible to create highly synchronized industry value chains called value webs. A **value web** is a collection of independent firms that use information technology to coordinate their value chains to produce a product or service for a market collectively. It is more customer driven and operates in a less linear fashion than the traditional value chain.

Figure 3.10 shows that this value web synchronizes the business processes of customers, suppliers, and trading partners among different companies in an industry or in related industries. These value webs are flexible and adaptive to changes in supply and demand. Relationships can be bundled or unbundled in response to changing market conditions. Firms will accelerate time to market and to customers by optimizing their value web relationships to make quick decisions on who can deliver the required products or services at the right price and location.

FIGURE 3.10 THE VALUE WEB

Synergies, Core Competencies, And Network-based Strategies
A large corporation is typically a collection of businesses. Often, the firm is organized financially as a collection of strategic business units and the returns to the firm are directly tied to the performance of all the strategic business units. Information systems can improve the overall performance of these business units by promoting synergies and core competencies.

Synergies
The idea of synergies is that when the output of some units can be used as inputs to other units, or two organizations pool markets and expertise, these relationships lower costs and generate profits. One use of information technology in these synergy situations is to tie together the operations of disparate business units so that they can act as a whole. For example, acquiring Countrywide Financial enabled Bank of America to extend its mortgage lending business and to tap into a large pool of new customers who might be interested in its credit card, consumer banking, and other financial products. Information systems would help the merged companies consolidate operations, lower retailing costs, and increase cross- marketing of financial products.

Enhancing Core Competencies
Yet another way to use information systems for competitive advantage is to think about ways that systems can enhance core competencies. A **core competency** is an activity for which a firm is a world-class leader. Core competencies may involve being the world's best miniature parts designer, the best package delivery service, or the best thin-film manufacturer. Any information system that encourages the sharing of knowledge across business units enhances competency. Such systems might encourage or enhance existing competencies and help employees become aware of new external knowledge; such systems might also help a business leverage existing competencies to related markets. For example, Procter & Gamble, a world leader in brand management and consumer product innovation, uses a series of systems to enhance its core competencies. An intranet called Innovation Net helps people working on similar problems share ideas and expertise. Innovation Net connects those working in research and development (R&D), engineering, purchasing, marketing, legal affairs, and business information systems around the world, using a portal to provide browser-based access to documents, reports, charts, videos, and other data from various sources.

Network-Based Strategies
The availability of Internet and networking technology have inspired strategies that take advantage of firms' abilities to create networks or network with each other. Network-based strategies include the use of network economics, a virtual company model, and business ecosystems.

Network Economics. Business models based on a network may help firms strategically by taking advantage of **network economics**. In traditional economics—the economics of factories and agriculture—production experiences diminishing returns. The more any given resource is applied to production, the lower the marginal gain in output, until a point is reached where the additional inputs produce no additional outputs. This is the law of diminishing returns, and it is the foundation for most of modern economics. In some situations, the law of diminishing returns does not work. For instance, in a network, the marginal costs of adding another participant are about zero, whereas the marginal gain is much larger. The larger the number of subscribers in a telephone system or the Internet, the greater the value to all participants because each user can interact with more people. It is not much more expensive to operate a television station with 1,000 subscribers than with 10 million subscribers. The value of a community of people grows with size, whereas the cost of adding new members is inconsequential. From this network economics perspective, information technology can be strategically useful. Internet sites can be used by firms to build communities of users—like- minded customers who want to share their experiences. This builds customer loyalty and enjoyment, and builds unique ties to customers. EBay, the giant online auction site, and iVillage, an online community for women, are examples.

What are the challenges posed by strategic information systems and how should they be addressed?
Strategic information systems often change the organization as well as its products, services, and operating procedures, driving the organization into new behavioral patterns. Successfully using information systems to achieve a competitive advantage is challenging and requires precise coordination of technology, organizations, and management.

Sustaining Competitive Advantage
The competitive advantages that strategic systems confer do not necessarily last long enough to ensure long-term profitability. Because competitors can retaliate and copy strategic systems, competitive advantage

is not always sustainable. Markets, customer expectations, and technology change; globalization has made these changes even more rapid and unpredictable. Classic strategic systems, such as American Airlines's SABRE computerized reservation system, Citibank's ATM system, and FedEx's package tracking system, benefited by being the first in their industries. Then rival systems emerged. Systems originally intended to be strategic frequently become tools for survival.

Aligning IT with Business Objectives

Information technology takes on a life of its own and does not serve management and shareholder interests very well. Instead of business people taking an active role in shaping IT to the enterprise, they ignore it, claim not to understand IT, and tolerate failure in the IT area as just a nuisance to work around. The research on IT and business performance has found that the more successfully a firm can align information technology with its business goals, the more profitable it will be.

Management Checklist: Performing a Strategic Systems Analysis

To align IT with the business and use information systems effectively for competitive advantage, managers need to perform a strategic systems analysis.

To identify the types of systems that provide a strategic advantage to their firms, managers should ask the following questions:

1. **What is the structure of the industry in which the firm is located?**
   - What are some of the competitive forces at work in the industry?
   - Are there new entrants to the industry?
   - What is the relative power of suppliers, customers, and substitute products and services over prices?
   - Is the basis of competition quality, price, or brand?
   - What are the direction and nature of change within the industry?
   - From where are the momentum and change coming?
   - How is the industry currently using information technology?
   - Is the organization behind or ahead of the industry in its application of information systems?
2. **What are the business, firm, and industry value chains for this particular firm?**
   - How is the company creating value for the customer—through lower prices and transaction costs or higher quality?
   - Are there any places in the value chain where the business could create more value for the customer and additional profit for the company?
   - Does the firm understand and manage its business processes using the best practices available
   - Is it taking maximum advantage of supply chain management, customer relationship management, and enterprise systems?
   - Does the firm leverage its core competencies?
   - Is the industry supply chain and customer base changing in ways that benefit or harm the firm?
   - Can the firm benefit from strategic partnerships and value webs?
   - Where in the value chain will information systems provide the greatest value to the firm?
3. **Have we aligned IT with our business strategy and goals?**
   - Have we correctly articulated our business strategy and goals?
   - Is IT improving the right business processes and activities to promote this strategy?
   - Are we using the right metrics to measure progress toward those goals?

Managing Strategic Transitions

Sociotechnical changes (changes in business goals, relationships with customers and suppliers, and business processes) affecting both social and technical elements of the organization, can be considered **strategic transitions**— a movement between levels of sociotechnical systems. Such changes often entail blurring of organizational boundaries, both external and internal. Suppliers and customers must become intimately linked and may share each other's responsibilities. Managers will need to devise new business processes for coordinating their firms' activities with those of customers, suppliers, and other organizations.

CHAPTER # 04: INFORMATION SYSTEMS SECURITY

A. System Vulnerability and Abuse

Why Systems Are Vulnerable

When large amounts of data are stored in electronic form, they are vulnerable to many more kinds of threats than when they existed in manual form. Through communications networks, information systems in different locations are interconnected. The potential for unauthorized access, abuse, or fraud is not limited to a single location but can occur at any access point in the network. Figure 8.1 illustrates the most common threats against contemporary information systems. They can stem from technical, organizational, and environmental factors compounded by poor management decisions. In the multi-tier client/server computing environment illustrated here, vulnerabilities exist at each layer and in the communications between the layers. Users at the client layer can cause harm by introducing errors or by accessing systems without authorization. It is possible to access data flowing over networks, steal valuable data during transmission, or alter messages without authorization. Radiation may disrupt a network at various points as well. Intruders can launch denial-of-service attacks or malicious software to disrupt the operation of Web sites. Those capable of penetrating corporate systems can steal, destroy, or alter corporate data stored in databases or files.

Internet Vulnerabilities

Large public networks, such as the Internet, are more vulnerable than internal networks because they are virtually open to anyone. The Internet is so huge that when abuses do occur, they can have an enormously widespread impact. When the Internet becomes part of the corporate network, the organization's information systems are even more vulnerable to actions from outsiders.

Vulnerability has also increased from widespread use of e-mail, instant messaging (IM), and peer-to-peer file-sharing programs. E-mail may contain attachments that serve as springboards for malicious software or unauthorized access to internal corporate systems. Employees may use e-mail messages to transmit valuable trade secrets, financial data, or confidential customer information to unauthorized recipients. Popular IM applications for consumers do not use a secure layer for text messages, so they can be intercepted and read by out-siders during transmission over the public Internet. Instant messaging activity over the Internet can in some cases be used as a back door to an otherwise secure network. Sharing files over peer-to-peer (P2P) networks, such as those for illegal music sharing, may also transmit malicious software or expose information on either individual or corporate computers to outsiders

Wireless Security Challenges

Both Bluetooth and Wi-Fi networks are susceptible to hacking by eavesdroppers. Although the range of Wi-Fi networks is only several hundred feet, it can be extended up to one-fourth of a mile using external antennae. Local area networks (LANs) using the 802.11 standard can be easily penetrated by outsiders armed with laptops, wireless cards, external antennae, and hacking software. Hackers use these tools to detect unprotected networks, monitor network traffic, and, in some cases, gain access to the Internet or to corporate networks.

A hacker can employ an 802.11 analysis tool to identify the SSID. An intruder that has associated with an access point by using the correct SSID is capable of accessing other resources on the network, using the Windows operating system to determine which other users are connected to the network, access their computer hard drives, and open or copy their files.

Intruders also use the information they have gleaned to set up rogue access points on a different radio channel in physical locations close to users to force a user's radio NIC to associate with the rogue access point. Once this association occurs, hackers using the rogue access point can capture the names and passwords of unsuspecting users.

Malicious Software: Viruses, Worms, Trojan Horses and Spyware

Malicious software programs are referred to as malware and include a variety of threats, such as computer viruses, worms, and Trojan horses.

Virus is a rogue software program that attaches itself to other software programs or data files in order to be executed, usually without user knowledge or permission.

Worms are independent computer programs that copy themselves from one computer to other computers over a network. (Unlike viruses, they can operate on their own without attaching to other computer program files and rely less on human behavior in order to spread from computer to computer. This explains why

computer worms spread much more rapidly than computer viruses.) Worms destroy data and programs as well as disrupt or even halt the operation of computer networks.

Trojan Horse is a software program that appears to be benign but then does something other than expected, such as the Zeus Trojan described in the chapter-opening case. The Trojan horse is not itself a virus because it does not replicate, but it is often a way for viruses or other malicious code to be introduced into a computer system.

SQL injection attacks are the largest malware threat. SQL injection attacks take advantage of vulnerabilities in poorly coded Web application software to introduce malicious program code into a company's systems and networks. These vulnerabilities occur when a Web application fails to properly validate or filter data entered by a user on a Web page, which might occur when ordering something online.

Some types of **spyware** also act as malicious software. These small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising. Thousands of forms of spyware have been documented. Many users find such spyware annoying and some critics worry about its infringement on computer users' privacy. Some forms of spyware are especially nefarious.

Keyloggers record every keystroke made on a computer to steal serial numbers for software, to launch Internet attacks, to gain access to e-mail accounts, to obtain passwords to protected computer systems, or to pick up personal information such as credit card numbers. Other spyware programs reset Web browser home pages, redirect search requests, or slow performance by taking up too much memory.

Hackers and Computer Crime
A hacker is an individual who intends to gain unauthorized access to a computer system.

Within the hacking community, the term cracker is typically used to denote a hacker with criminal intent, although in the public press, the terms hacker and cracker are used interchangeably. Hackers and crackers gain unauthorized access by finding weaknesses in the security protections employed by Web sites and computer systems, often taking advantage of various features of the Internet that make it an open system that is easy to use.

Spoofing and Sniffing
Hackers attempting to hide their true identities often spoof, or misrepresent, themselves by using fake e-mail addresses or masquerading as someone else.

Spoofing also may involve redirecting a Web link to an address different from the intended one, with the site masquerading as the intended destination. For example, if hackers redirect customers to a fake Web site that looks almost exactly like the true site, they can then collect and process orders, effectively stealing business as well as sensitive customer information from the true site.
A sniffer is a type of eavesdropping program that monitors information traveling over a network. Sniffers enable hackers to steal proprietary information from anywhere on a network, including e-mail messages, company files, and confidential reports.

Denial-of-Service Attacks
In a denial-of-service (DoS) attack, hackers flood a network server or Web server with many thousands of false communications or requests for services to crash the network. The network receives so many queries that it cannot keep up with them and is thus unavailable to service legitimate requests. A **Distributed Denial-Of-Service (DDoS)** attack uses numerous computers to inundate and overwhelm the network from numerous launch points.

Computer Crime
Most hacker activities are criminal offenses, and the vulnerabilities of systems we have just described make them targets for other types of computer crime as well.
Examples of computer crime

i. Breaching the confidentiality of protected computerized data
ii. Accessing a computer system without authority
iii. Knowingly accessing a protected computer to commit fraud
iv. Intentionally accessing a protected computer and causing damage, negligently or deliberately
v. Knowingly transmitting a program, program code, or command that intentionally causes damage to a protected computer

vi. Threatening to cause damage to a protected computer
vii. Theft of trade secrets
viii. Unauthorized copying of software or copyrighted intellectual property, such as articles, books, music, and video
ix. Schemes to defraud
x. Using e-mail for threats or harassment
xi. Intentionally attempting to intercept electronic communication
xii. Illegally accessing stored electronic communications, including e-mail and voice mail
xiii. Transmitting or possessing child pornography using a computer

Identity Theft
Identity theft is a crime in which an imposter obtains key pieces of personal information, such as social security identification numbers, driver's license numbers, or credit card numbers, to impersonate someone else. The information may be used to obtain credit, merchandise, or services in the name of the victim or to provide the thief with false credentials.

Click Fraud
Click fraud occurs when an individual or computer program fraudulently clicks on an online ad without any intention of learning more about the advertiser or making a purchase. Click fraud has become a serious problem at Google and other Web sites that feature pay-per-click online advertising.

Global Threats: Cyberterrorism and Cyberwarfare
The cybercriminal activities we have described—launching malware, denial-of service attacks, and phishing probes—are borderless. Concern is mounting that the vulnerabilities of the Internet or other networks make digital networks easy targets for digital attacks by terrorists, foreign intelligence services, or other groups seeking to create widespread disruption and harm. Such cyberattacks might target the software that runs electrical power grids, air traffic control systems, or networks of major banks and financial institutions. At least
20 countries, including China, are believed to be developing offensive and defensive cyberwarfare capabilities.

Internal Threats: Employees
Employees have access to privileged information, and in the presence of sloppy internal security procedures, they are often able to roam throughout an organization's systems without leaving a trace. Malicious intruders seeking system access sometimes trick employees into revealing their passwords by pretending to be legitimate members of the company in need of information. This practice is called social engineering.

Software Vulnerability
Software errors pose a constant threat to information systems, causing untold losses in productivity. Growing complexity and size of software programs, coupled with demands for timely delivery to markets, have contributed to an increase in software flaws or vulnerabilities. A major problem with software is the presence of hidden bugs or program code defects. The main source of bugs is the complexity of decision making code. A relatively small program of several hundred lines will contain tens of decisions leading to hundreds or even thousands of different paths. Important programs within most corporations are usually much larger, containing tens of thousands or even millions of lines of code, each with many times the choices and paths of the smaller programs.

B. Business Value of Security Control

Companies have very valuable information assets to protect. Systems often contain information on corporate operations, including trade secrets, new product development plans, and marketing strategies. These information assets have tremendous value, and the repercussions can be devastating if they are lost, destroyed, or placed in the wrong hands. Inadequate security and control may result in serious legal liability. Businesses must protect not only their own information assets but also those of customers, employees, and business partners. A sound security and control framework that protects business information assets can thus produce a high return on investment. Strong security and control also increase employee productivity and lower operational costs.

Legal and Regulatory Requirements for Electronic Records Management
Recent government regulations are forcing companies to take security and control more seriously by

mandating the protection of data from abuse, exposure, and unauthorized access. Firms face new legal obligations for the retention and storage of electronic records as well as for privacy protection.

For Example, if you work in a publicly traded company, your company will need to comply with the Public Company Accounting Reform and Investor Protection Act of 2002, better known as the Sarbanes-Oxley Act. This Act was designed to protect investors after the financial scandals at Enron, WorldCom, and other public companies. It imposes responsibility on companies and their management to safeguard the accuracy and integrity of financial information that is used internally and released externally. Sarbanes-Oxley is fundamentally about ensuring that internal controls are in place to govern the creation and documentation of information in financial statements. Because information systems are used to generate, store, and transport such data, the legislation requires firms to consider information systems security and other controls required to ensure the integrity, confidentiality, and accuracy of their data.

Electronic Evidence and Computer Forensics

Security, control, and electronic records management have become essential for responding to legal actions. Much of the evidence today for stock fraud, embezzlement, theft of company trade secrets, computer crime, and many civil cases is in digital form. Evidence can be represented as digital data stored on CDs, and computer hard disk drives, as well as in e-mail, instant messages, and e-commerce transactions over the Internet. E-mail is currently the most common type of electronic evidence.

An effective electronic document retention policy ensures that electronic documents, e-mail, and other records are well organized, accessible, and neither retained too long nor discarded too soon. It also reflects an awareness of how to preserve potential evidence for computer forensics.

Computer forensics is the scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media in such a way that the information can be used as evidence in a court of law. It deals with the following problems:

- Recovering data from computers while preserving evidential integrity
- Securely storing and handling recovered electronic data
- Finding significant information in a large volume of electronic data
- Presenting the information to a court of law

Data that a computer user may have deleted on computer storage media can be recovered through various techniques. Computer forensics experts try to recover such data for presentation as evidence. So, an awareness of computer forensics should be incorporated into a firm's contingency planning process.

C. Ethical Responsibilities of Business Professional

As a business professional, you have a responsibility to promote ethical uses of information technology in the workplace. Whether or not you have managerial responsibilities, you should accept the ethical responsibilities that come with your work activities. As a manager or business professional, it will be your responsibility to make decisions about business activities and the use of information technologies that may have an ethical dimension that must be considered.

Business ethics

Business ethics is concerned with the numerous ethical questions that managers must confront as part of their daily business decision making. The issues of intellectual property rights, customer and employee privacy, security of company records, and workplace safety are major areas of ethical controversy in information technology.

For example, in business ethics, the stockholder theory holds that managers are agents of the stockholders, and their only ethical responsibility is to increase the profits of the business without violating the law or engaging in fraudulent practices. However, the social contract theory states that companies have ethical responsibilities to all members of society, which allows corporations to exist according to a social contract. The first condition of the contract requires companies to enhance the economic satisfaction of consumers and employees. They must do that without polluting the environment or depleting natural resources, misusing political power, or subjecting their employees to dehumanizing working conditions. The second condition requires companies to avoid fraudulent practices, show respect for their employees as human beings, and avoid practices that systematically worsen the position of any group in society.

The stakeholder theory of business ethics maintains that managers have an ethical responsibility to manage

a firm for the benefit of all its stakeholders, that is, all individuals and groups that have a stake in, or claim on, a company.

Technology Ethics

Another important ethical dimension deals specifically with the ethics of the use of any form of technology. The principles of technology ethics can serve as basic ethical requirements that companies should meet to help ensure the ethical implementation of information technologies and information systems in business. Following figure outlines four principles of technology ethics.

Principles of Technology Ethics
• **Proportionality.** The good achieved by the technology must outweigh the harm or risk. Moreover, there must be no alternative that achieves the same or comparable benefits with less harm or risk.
• **Informed Consent.** Those affected by the technology should understand and accept the risks.
• **Justice.** The benefits and burdens of the technology should be distributed fairly. Those who benefit should bear their fair share of the risks, and those who do not benefit should not suffer a significant increase in risk.
• **Minimized Risk.** Even if judged acceptable by the other three guidelines, the technology must be implemented so as to avoid all unnecessary risk.

Many organizations display ethical behavior by scheduling work breaks and limiting the exposure of data entry workers to staring at a computer monitor to minimize their risk of developing a variety of work-related health disorders, such as hand or eye injuries.

Ethical Guidelines

The Association of Information Technology Professionals (AITP), an organization of professionals in the computing field, express the codes of professional conduct for IS professionals. Its code of conduct outlines the ethical considerations inherent in the major responsibilities of an IS professional. Following figure is a portion of the AITP code of conduct.

AITP Standards of Professional Conduct
In recognition of my obligation to my employer I shall:
• Avoid conflicts of interest and ensure that my employer is aware of any potential conflicts.
• Protect the privacy and confidentiality of all information entrusted to me.
• Not misrepresent or withhold information that is germane to the situation.
• Not attempt to use the resources of my employer for personal gain or for any purpose without proper approval.
• Not exploit the weakness of a computer system for personal gain or personal satisfaction.
In recognition of my obligation to society I shall:
• Use my skill and knowledge to inform the public in all areas of my expertise.
• To the best of my ability, ensure that the products of my work are used in a socially responsible way.
• Support, respect, and abide by the appropriate local, state, provincial, and federal laws.
• Never misrepresent or withhold information that is germane to a problem or a situation of public concern, nor will I allow any such known information to remain unchallenged.
• Not use knowledge of a confidential or personal nature in any unauthorized manner to achieve personal gain.

Source: 2007 PricewaterhouseCoopers Global Security Survey.

Business and IS professionals can live up to their ethical responsibilities by voluntarily following such guidelines. For example, you can be a responsible professional by (1) acting with integrity, (2) increasing your professional competence, (3) setting high standards of personal performance, (4) accepting responsibility for your work, and (5) advancing the health, privacy, and general welfare of the public. Then you would be demonstrating ethical conduct, avoiding computer crime, and increasing the security of any information system you develop or use.

D. Computer Crime

Computer crime is defined by the Association of Information Technology Professionals (AITP) as including (1) the unauthorized use, access, modification, and destruction of hardware, software, data, or network

resources; (2) the unauthorized release of information; (3) the unauthorized copying of software; (4) denying an end user access to his or her own hardware, software, data, or network resources; and (5) using or conspiring to use computer or network resources to obtain information or tangible property illegally. This definition was promoted by the AITP in a Model Computer Crime Act and is reflected in many computer crime laws.

Hacking and Cracking

Hacking, in computerese, is the obsessive use of computers or the unauthorized access and use of networked computer systems. Hackers can be outsiders or company employees who use the Internet and other networks to steal or damage data and programs. A hacker may also use remote services that allow one computer on a network to execute programs on another computer to gain privileged access within a network.

Common Hacking Tactics

Denial of Service. This is becoming a common networking prank. By hammering a Web site's equipment with too many requests for information, an attacker can effectively clog the system, slowing performance or even crashing the site. This method of overloading computers is sometimes used to cover up an attack.

Scans. Widespread probes of the Internet to determine types of computers, services, and connections. That way the bad guys can take advantage of weaknesses in a particular make of computer or software program.

Sniffer. Programs that covertly search individual packets of data as they pass through the Internet, capturing passwords or the entire contents.

Spoofing. Faking an e-mail address or Web page to trick users into passing along critical information like passwords or credit card numbers.

Trojan Horse. A program that, unknown to the user, contains instructions that exploit a known vulnerability in some software.

Back Doors. In case the original entry point has been detected, having a few hidden ways back makes reentry easy—and difficult to detect.

Malicious Applets. Tiny programs, sometimes written in the popular Java computer language, that misuse your computer's resources, modify files on the hard disk, send fake e-mail, or steal passwords.

War Dialing. Programs that automatically dial thousands of telephone numbers in search of a way in through a modem connection.

Logic Bombs. An instruction in a computer program that triggers a malicious act.

Buffer Overflow. A technique for crashing or gaining control of a computer by sending too much data to the buffer in a computer's memory.

Password Crackers. Software that can guess passwords.

Social Engineering. A tactic used to gain access to computer systems by talking unsuspecting company employees out of valuable information such as passwords.

Dumpster Diving. Sifting through a company's garbage to find information to help break into their computers. Sometimes the information is used to make a stab at social engineering more credible.

A cracker (also called a black hat or darkside hacker) is a malicious or criminal hacker. Usually a cracker is a person who maintains knowledge of the vulnerabilities he or she finds and exploits them for private advantage, not revealing them to either the general public or the manufacturer for correction. The general public uses the term hacker to refer to the same thing. In computer jargon, the meaning of hacker can be much more broad. The name comes from the opposite of white hat hackers.

Cyber-Theft

Cyber-theft refers to the act of using an internet to steal someone's property or to interfere with someone's use and enjoyment of property. In other words, cyber-theft is the stealing of financial and/or personal information through the use of computers for making its fraudulent or other illegal use

Cyberterrorism

Cyberterrorism is the leveraging of an organization's or government's computers and information, particularly via the Internet, to cause physical, real-world harm or severe disruption of infrastructure. The National Conference of State Legislatures (NCSL) puts a much finer point on the definition of the term: the use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically.

Unauthorized Use at Work

The unauthorized use of computer systems and networks can be called time and resource theft. A common example is unauthorized use of company-owned computer networks by employees. Network monitoring software, called sniffers, is frequently used to monitor network traffic to evaluate network capacity, as well as

to reveal evidence of improper use.

Software Piracy
Software piracy is defined as illegally copying software that does not belong to you in a manner that violates the copyright. A example of software piracy is when you download a copy of Microsoft Word from a file-sharing website without paying for it.

Theft of Intellectual Property
Intellectual property theft occurs in the form of infringements of copyrighted material, such as music, videos, images, articles, books, and other written works, which most courts have deemed illegal. The development of peer-to-peer (P2P) networking has made digital versions of copyrighted material even more vulnerable to unauthorized use.

Computer virus and Worms
Computer Virus is the more popular term, but technically, a virus is a program code that cannot work without being inserted into another program. A worm is a distinct program that can run unaided. In either case, these programs copy annoying or destructive routines into the networked computer systems of anyone who accesses computers infected with the virus or who uses copies of magnetic disks taken from infected computers. Thus, a computer virus or worm can spread destruction among many users.

Adware and Spyware
Two more recent entries into the computer vulnerabilities arena are adware and spyware. By definition, Adware is software that, while purporting to serve some useful function and often fulfilling that function, also allows Internet advertisers to display advertisements as banners and pop-up ads without the consent of the computer user. In the extreme, adware can also collect information about the user of its host computer and send it over the Internet to its owner. This special class of adware is called spyware and is defined as any software that employs users' Internet connection in the background without their knowledge or explicit permission.

Spyware programs collect specific information about you, ranging from general demographics like name, ad dress, and Internet surfing habits to credit card, Social Security number, user names, passwords, or other personal information. It is important to understand that not all adware programs are spyware.

Proper adware represents a viable, albeit sometimes irritating, revenue model for many software companies that allows you to get products for free and, when used correctly, does not pose any significant privacy threat. In contrast, spyware is and should be considered a clear threat to your privacy

E. Privacy Issues

Information technology makes it technically and economically feasible to collect, store, integrate, interchange, and retrieve data and information quickly and easily. This characteristic has an important beneficial effect on the efficiency and effectiveness of computer-based information systems. The power of information technology to store and retrieve information, however, can have a negative effect on the right to privacy of every individual. For example, confidential e-mail messages by employees are monitored by many companies. The unauthorized use of such information has badly damaged the privacy of individuals.

Governments around the world, but none more than in the United States, are debating privacy issues and considering various forms of legislation. With regard to the Inter net, opt- in versus opt-out is central to the debate over privacy legislation. Additional privacy issues under debate include:

- Accessing private e-mail conversations and computer records and collecting and sharing information about individuals gained from their visits to Internet Web sites and newsgroups (violation of privacy).
- Always knowing where a person is, especially as mobile and paging services become more closely associated with people rather than places (computer monitoring).
- Using customer information gained from many sources to market additional business services (computer matching).
- Collecting telephone numbers, e-mail addresses, credit card numbers, and other personal information to build individual customer profiles (unauthorized personal files).

Privacy on the Internet
The Internet is notorious for giving its users a feeling of anonymity when in reality they are highly visible and open to violations of their privacy. Most of the Internet and its World Wide Web, e-mail, chat, and newsgroups are still a wide open, unsecured electronic frontier, with no tough rules on what information is personal and

private. Information about Internet users is captured legitimately and automatically each time you visit a Web site or newsgroup and is recorded as a “cookie file” on your hard disk. One can protect his/her privacy in several ways. For example, sensitive e-mail can be protected by encryption, if both e-mail parties use compatible encryption software built into their e-mail programs.

Computer Matching
Computer profiling and mistakes in the computer matching of personal data are other controversial threats to privacy. Individuals have been mistakenly arrested and jailed and people have been denied credit because their physical profiles or personal data have been used by profiling software to match them incorrectly or improperly with the wrong individuals. Another threat is the unauthorized matching of computerized information about you extracted from the databases of sales transaction processing systems and sold to information brokers or other companies.

Computer Libel and Censorship
The opposite side of the privacy debate is the right of people to know about matters others may want to keep private (freedom of information), the right of people to express their opinions about such matters (freedom of speech), and the right of people to publish those opinions (freedom of the press). Some of the biggest battle grounds in the debate are the bulletin boards, e-mail boxes, and online files of the Internet and public information networks such as the Microsoft Network. The weapons being used in this battle include spamming, flame mail, libel laws, and censorship.

Spamming is the indiscriminate sending of unsolicited e-mail messages (spam) to many Internet users. Spamming is the favorite tactic of mass mailers of unsolicited advertisements, or junk e-mail. Spamming has also been used by cyber-criminals to spread computer viruses or infiltrate many computer systems.

Flaming is the practice of sending extremely critical, derogatory, and often vulgar e-mail messages (flame mail) or newsgroup postings to other users on the Internet or online services. Flaming is especially prevalent on some of the Internet’s special-interest newsgroups.

There have been many incidents of racist or defamatory messages on the Web that have led to calls for censorship and lawsuits for libel.

Privacy Laws
Many countries strictly regulate the collection and use of personal data by business corporations and government agencies. Many government privacy laws attempt to enforce the privacy of computer-based files and communications.

For example, in the United States, the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act prohibit intercepting data communications messages, stealing or destroying data, or trespassing in federal-related computer systems. Because the Internet includes federal-related computer systems, privacy attorneys argue that the laws also require notifying employees if a company intends to monitor Internet usage. Another example is the U.S. Computer Matching and Privacy Act, which regulates the matching of data held in federal agency files to verify eligibility for federal programs.

F. Current State of Cyber Law

Cyber law is the term used to describe laws intended to regulate activities over the Internet or via the use of electronic data communications. Cyber law encompasses a wide variety of legal and political issues related to the Internet and other communications technologies, including intellectual property, privacy, freedom of expression, and jurisdiction.

The intersection of technology and the law is often controversial. Some feel that the Internet should not (or possibly cannot) be regulated in any form. Furthermore, the development of sophisticated technologies, such as encryption and cryptography, make traditional forms of regulation extremely difficult. Finally, the fundamental end to-end nature of the Internet means that if one mode of communication is regulated or shut down, another method will be devised and spring up in its place. In the words of John Gilmore, founder of the Electronic Frontier Foundation, “the Internet treats Censorship as damage and simply routes around it.”

One example of advancements in cyber law is found in the Federal Trade Commission’s (FTC) Consumer Sentinel Project. Consumer Sentinel is a unique investigative cyber-tool that provides members of the Consumer Sentinel Network with access to data from millions of consumer complaints. Consumer Sentinel

includes complaints about identity theft, do-not- call registry violations, computers, the Internet, and online auctions, telemarketing scams, advance-fee loans, and credit scams, sweepstakes, lotteries, and prizes, business opportunities and work-at-home schemes, health and weight loss products, debt collection, credit reports, and other financial matters.

Consumer Sentinel is based on the premise that sharing information can make law enforcement even more effective. To that end, the Consumer Sentinel Network provides law- enforcement members with access to complaints provided directly to the Federal Trade Commission by consumers, as well as providing members with access to complaints shared by data contributors.

According to the FTC Sentinel Report for 2007, more than 800,000 complaints were processed through Sentinel with Internet-related offenses representing 11 percent of the total complaints, and computer-related identity theft representing 23 percent. While many of these complaints are difficult, if not impossible to prosecute, we are beginning to see more resources being committed to addressing cyber-related crime.

Cyber law is a new phenomenon, having emerged after the onset of the Internet. As we know, the Internet grew in a relatively unplanned and unregulated manner.

G. Other Challenges

Let's now explore some other important challenges that arise from the use of information technologies in business, as illustrated in Following Figure. These challenges include the potential ethical and societal impact of business applications of IT in the areas of employment, individuality, working conditions, and health.

Employment Challenges

The impact of information technologies on employment is a major ethical concern that is directly related to the use of computers to achieve automation of work activities. There can be no doubt that the use of information technologies has created new jobs and increased productivity while also causing a significant reduction in some types of job opportunities. For example, when computers are used for accounting systems or the automated control of machine tools, they are accomplishing asks formerly performed by many clerks and machinists. Also, jobs created by information echnology may require different types of skills and education than do the jobs that are eliminated. Therefore, people may become unemployed unless they can be retrained for new positions or new responsibilities.

Computer Monitoring

One of the most explosive ethical issues concerning workplace privacy and the quality of working conditions in business is computer monitoring. That is, computers are being used to monitor the productivity and behavior of millions of employees while they work. Supposedly, computer monitoring occurs so employers can collect productivity data about their employees to increase the efficiency and quality of service. Political pressure is building to outlaw or regulate computer monitoring in the workplace. However, computer monitoring has been criticized as unethical because it monitors individuals, not just work, and is done continually, which violates workers' privacy and personal freedom.

For example, when you call to make a reservation, an airline reservation agent may be timed on the exact number of seconds he or she took per caller, the time between calls, and the number and length of breaks taken. In addition, your conversation may be monitored.

Finally, computer monitoring has been blamed for robbing workers of the dignity of their work. In its extremes, computer monitoring can create an "electronic sweatshop," in which workers are forced to work at a hectic pace under poor working conditions. So computer monitoring of workers is one ethical issue in business that won't go away.

Challenges in Working Conditions
Information technology has eliminated monotonous or obnoxious tasks in the office and the factory that formerly had to be performed by people. For example, word processing and desktop publishing make producing office documents a lot easier to do, and robots have taken over repetitive welding and spray painting jobs in the automotive industry. Thus, information technology can be said to upgrade the quality of work because it can upgrade the quality of working conditions and the content of work activities.

To the extent that computers are used in some types of automation, IT must take some responsibility for the criticism of assembly-line operations that require the continual repetition of elementary tasks, thus forcing a worker to work like a machine instead of like a skilled craftsperson. Many automated operations are also criticized for relegating people to a "do- nothing" standby role, where workers spend most of their time waiting for infrequent opportunities to push some buttons. Such effects do have a detrimental effect on the quality of work, but they must be compared against the less burdensome and more creative jobs created by information technology.

Challenges of Individuality

A frequent criticism of information systems centers on their negative effect on the individuality of people. Computer-based systems are criticized as impersonal systems that dehumanize and depersonalize activities that have been computerized because they eliminate the human relationships present in non-computer systems.

Another aspect of the loss of individuality is the regimentation that seems required by some computer-based systems. The negative impact of IT on individuality is reinforced by horror stories that describe how inflexible and uncaring some organizations with computer-based processes are when it comes to rectifying their own mistakes.

However, many business applications of IT are designed to minimize depersonalization and regimentation Thus, the widespread use of personal computers and the Internet has dramatically improved the development of people-oriented and personalized information systems

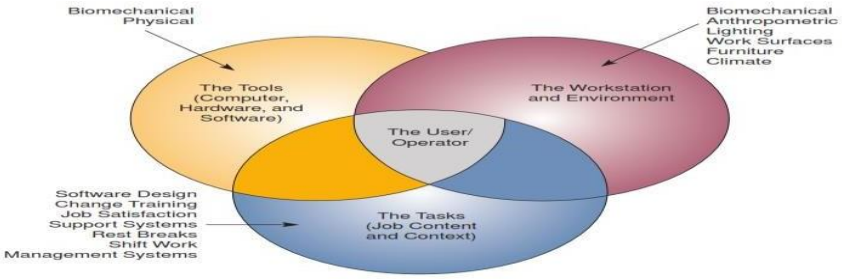
Health Issues
The use of information technology in the workplace raises a variety of health issues. Heavy use of computers is reportedly causing health problems like job stress, damaged arm and neck muscles, eyestrain, radiation exposure, and even death by computer caused accidents. For example, computer monitoring is blamed as a major cause of computer-related job stress. Workers, unions, and government officials criticize computer monitoring as putting so much stress on employees that it leads to health problems.

People who sit at PC workstations or visual display terminals (VDTs) in fast-paced, repetitive keystroke jobs can suffer a variety of health problems known collectively as Cumulative Trauma Disorders (CTDs). Their fingers, wrists, arms, necks, and backs may become so weak and painful that they cannot work.

Some pregnant workers have reported miscarriages and fetal deformities due to prolonged exposure to CRTs at work. Studies have failed to find conclusive evidence concerning this problem; still, several organizations recommend that female workers minimize their use of CRTs during pregnancy.

Ergonomics
Solutions to some of these health problems are based on the science of ergonomics, sometimes called human factors engineering. The goal of ergonomics is to design healthy work environments that are safe, comfortable, and pleasant for people to work in, thus increasing employee morale and productivity. Other health issues may require ergonomic solutions emphasizing job design rather than workplace design

For example, this approach may require policies providing for work breaks from heavy video monitor use every few hours, while limiting the CRT exposure of pregnant workers. Ergonomic job design can also provide more variety in job tasks for those workers who spend most of their workday at computer workstations.



Societal Solutions

We can use information technologies to solve human and social problems through societal solutions such as medical diagnosis, computer-assisted instruction, governmental program planning, environmental quality control, and law enforcement. For example, computers can help diagnose an illness, prescribe necessary treatment, and monitor the progress of hospital patients. Computer-Assisted-Instruction (CAI) and Computer- Based-Training (CBT) enable interactive instruction tailored to the needs of students. Distance learning is supported by tele communications networks, videoconferencing, e-mail, and other technologies.

Information technologies can be used for crime control through various law enforcement applications. For example, computerized alarm systems allow police to identify and respond quickly to evidence of criminal activity. Computers have been used to monitor the level of pollution in the air and in bodies of water, detect the Sources of pollution, and issue early warnings when dangerous levels are reached. Computers are being used in job placement systems to help match unemployed persons with available jobs. These and other applications illustrate that information technology can be used to help solve the problems of society.

If managers, business professionals, and IS specialists accept their ethical responsibilities, then information technology can help improve living and working conditions for all of society.

H. Establishing a Framework for Security and Control

Even with the best security tools, your information systems won't be reliable and secure unless you know how and where to deploy them. You'll need to know where your company is at risk and what controls you must have in place to protect your information systems. You'll also need to develop a security policy and plans for keeping your business running if your information systems aren't operational.

Information Systems Controls

Information systems controls are both manual and automated and consist of both general controls and application controls.

General controls govern the design, security, and use of computer programs and the security of data files in general throughout the organization's information technology infrastructure. On the whole, general controls apply to all computerized applications and consist of a combination of hardware, software, and manual procedures that create an overall control environment. **General controls includes:**

Software controls	Monitor the use of system software and prevent unauthorized access of software programs, system software, and computer programs.
Hardware controls	Ensure that computer hardware is physically secure, and check for equipment malfunction. Organizations that are critically dependent on their computers also must make provisions for backup or continued operation to maintain constant service.
Computer operations controls	Oversee the work of the computer department to ensure that programmed procedures are consistently and correctly applied to the storage and processing of data. They include controls over the setup of computer processing jobs and backup and recovery procedures for processing that ends abnormally.
Data security controls	Ensure that valuable business data files on either disk or tape are not subject to unauthorized access, change, or destruction while they are in use or in storage.
Implementation controls	Audit the systems development process at various points to ensure that the process is properly controlled and managed.
Administrative controls	Formalize standards, rules, procedures, and control disciplines to ensure that the organization's general and application controls are properly executed and enforced.

Application controls are specific controls unique to each computerized application, such as payroll or order processing. They include both automated and manual procedures that ensure that only authorized data are completely and accurately processed by that application.
Application controls can be classified as
i. Input Controls,
ii. Processing Controls, And
iii. Output Controls.

Input controls check data for accuracy and completeness when they enter the system. There are specific input controls for input authorization, data conversion, data editing, and error handling.

Processing controls establish that data are complete and accurate during updating.

Output controls ensure that the results of computer processing are accurate, complete, and properly distributed.

Risk Assessment
Before your company commits resources to security and information systems controls, it must know which assets require protection and the extent to which these assets are vulnerable. A risk assessment helps answer these questions and determine the most cost-effective set of controls for protecting assets.

A risk assessment determines the level of risk to the firm if a specific activity or process is not properly controlled. Not all risks can be anticipated and measured, but most businesses will be able to acquire some understanding of the risks they face. Business managers working with information systems specialists should try to determine the value of information assets, points of vulnerability, the likely frequency of a problem, and the potential for damage. **For example**, if an event is likely to occur no more than once a year, with a maximum of a $1,000 loss to the organization, it is not be wise to spend $20,000 on the design and maintenance of a control to protect against that event. However, if that same event could occur at least once a day, with a potential loss of more than $300,000 a year, $100,000 spent on a control might be entirely appropriate.

Security Policy
Once you've identified the main risks to your systems, your company will need to develop a security policy for protecting the company's assets. A **security policy** consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals.

The security policy drives policies determining acceptable use of the firm's information resources and which members of the company have access to its information assets. An **acceptable use policy (AUP)** defines acceptable uses of the firm's information resources and computing equipment, including desktop and laptop computers, wireless devices, telephones, and the Internet. The policy should clarify company policy regarding privacy, user responsibility, and personal use of company equipment and networks. A good AUP defines unacceptable and acceptable actions for every user and specifies consequences for noncompliance.

Security policy also includes provisions for identity management. **Identity management** consists of business processes and software tools for identifying the valid users of a system and controlling their access to system resources. It includes policies for identifying and authorizing different categories of system users, specifying what systems or portions of systems each user is allowed to access, and the processes and technologies for authenticating users and protecting their identities.

Disaster Recovery Planning and Business Continuity Planning
If you run a business, you need to plan for events, such as power outages, floods, earthquakes, or terrorist attacks that will prevent your information systems and your business from operating.

Disaster recovery planning devises plans for the restoration of computing and communications services after they have been disrupted. Disaster recovery plans focus primarily on the technical issues involved in keeping systems up and running, such as which files to back up and the maintenance of backup computer systems or disaster recovery services.

Business continuity planning focuses on how the company can restore business operations after a disaster strikes. The business continuity plan identifies critical business processes and determines action plans for

handling mission-critical functions if systems go down.

Business managers and information technology specialists need to work together on both types of plans to determine which systems and business processes are most critical to the company. They must conduct a business impact analysis to identify the firm's most critical systems and the impact a systems outage would have on the business. Management must determine the maximum amount of time the business can survive with its systems down and which parts of the business must be restored first.

The Role of Auditing

An MIS audit examines the firm's overall security environment as well as controls governing individual information systems. The auditor should trace the flow of sample transactions through the system and perform tests, using, if appropriate, automated audit software. The MIS audit may also examine data quality.

Security audits review technologies, procedures, documentation, training, and personnel. A thorough audit will even simulate an attack or disaster to test the response of the technology, information systems staff, and business employees.

The audit lists and ranks all control weaknesses and estimates the probability of their occurrence. It then assesses the financial and organizational impact of each threat.

I. Technologies and Tools for Security

Businesses have an array of technologies for protecting their information resources. They include tools for managing user identities, preventing unauthorized access to systems and data, ensuring system availability, and ensuring software quality.

Identity Management and Authentication

Identity management software automates the process of keeping track of all these users and their system privileges, assigning each user a unique digital identity for accessing each system. It also includes tools for authenticating users, protecting user identities, and controlling access to system resources. To gain access to a system, a user must be authorized and authenticated.

Authentication refers to the ability to know that a person is who he or she claims to be. Authentication is often established by using passwords known only to authorized users. An end user uses a password to log on to a computer system and may also use passwords for accessing specific systems and files. Passwords can also be "sniffed" if transmitted over a network or stolen through social engineering.

New authentication technologies, such as tokens, smart cards, and biometric authentication, overcome some of these problems. A token is a physical device, similar to an identification card that is designed to prove the identity of a single user. A smart card is a device about the size of a credit card that contains a chip formatted with access permission and other data. Biometric authentication uses systems that read and interpret individual human traits, such as fingerprints, irises, and voices, in order to grant or deny access. It compares a person's unique characteristics, such as the fingerprints, face, or retinal image, against a stored profile of these characteristics to determine whether there are any differences between these characteristics and the stored profile. If the two profiles match, access is granted.

Firewalls, Intrusion Detection Systems, and Antivirus Software

Firewalls prevent unauthorized users from accessing private networks. A firewall is a combination of hardware and software that controls the flow of incoming and outgoing network traffic. It is generally placed between the organization's private internal networks and distrusted external networks, such as the Internet, although firewalls can also be used to protect one part of a company's network from the rest of the network.

The firewall acts like a gatekeeper who examines each user's credentials before access is granted to a network. The firewall identifies names, IP addresses, applications, and other characteristics of incoming traffic. It checks this information against the access rules that have been programmed into the system by the network administrator. The firewall prevents unauthorized communication into and out of the network.

Intrusion detection systems feature full-time monitoring tools placed at the most vulnerable points or "hot spots" of corporate networks to detect and deter intruders continually. The system generates an alarm if it

finds a suspicious or anomalous event. Scanning software looks for patterns indicative of known methods of computer attacks, such as bad passwords, checks to see if important files have been removed or modified, and sends warnings of vandalism or system administration errors. The intrusion detection tool can also be customized to shut down a particularly sensitive part of a network if it receives unauthorized traffic.

Antivirus software prevents, detects, and removes malware, including computer viruses, computer worms, Trojan horses, spyware, and adware. However, most antivirus software is effective only against malware already known when the software was written. To remain effective, the antivirus software must be continually updated, and even then it is not always effective. According to a report by Solutionary Security Engineering Research Team (SERT), 54 percent of malware evades anti-virus detection. Organizations need to use additional malware detection tools for better protection (Solutionary, 2013).

Unified Threat Management Systems

To help businesses reduce costs and improve manageability, security vendors have combined into a single appliance various security tools, including firewalls, virtual private networks, intrusion detection systems, and Web content filtering and antispam software. These comprehensive security management products are called **unified threat management (UTM)** systems. Although initially aimed at small and medium-sized businesses, UTM products are available for all sizes of networks. Leading UTM vendors include Blue Coat, Fortinent, and Check Point, and networking vendors such as Cisco Systems and Juniper Networks provide some UTM capabilities in their products.

Securing Wireless Networks

The initial security standard developed for Wi-Fi called Wired Equivalent Privacy (WEP) is not very effective because its encryption keys are relatively easy to crack. Despite its flaws, WEP provides some margin of security if Wi-Fi users remember to activate it. A simple first step to thwart hackers is to assign a unique name to your network's SSID and instruct your router not to broadcast it. Corporations can further improve Wi-Fi security by using it in conjunction with virtual private network (VPN) technology when accessing internal corporate data. Corporations can further improve Wi-Fi security by using it in conjunction with virtual private network (VPN) technology when accessing internal corporate data.

Encryption and Public Key Infrastructure

Encryption is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the intended receiver. Data are encrypted by using a secret numerical code, called an encryption key that transforms plain data into cipher text. The message must be decrypted by the receiver.

Two methods for encrypting network traffic on the Web are SSL and S-HTTP. Secure Sockets Layer (SSL**)** and its successor Transport Layer Security (TLS) enable client and server computers to manage encryption and decryption activities as they communicate with each other during a secure Web session. Secure Hypertext Transfer Protocol (S-HTTP) is another protocol used for encrypting data flowing over the Internet, but it is limited to individual messages, whereas SSL and TLS are designed to establish a secure connection between two computers.

There are two alternative methods of encryption: symmetric key encryption and public key encryption. In symmetric key encryption, the sender and receiver establish a secure Internet session by creating a single encryption key and sending it to the receiver so both the sender and receiver share the same key. The strength of the encryption key is measured by its bit length.

The problem with all symmetric encryption schemes is that the key itself must be shared somehow among the senders and receivers, which exposes the key to outsiders who might just be able to intercept and decrypt the key. A more secure form of encryption called public key encryption uses two keys: one shared (or public) and one totally private as shown in Figure. The keys are mathematically related so that data encrypted with one key can be decrypted using only the other key. To send and receive messages, communicators first create separate pairs of private and public keys. The public key is kept in a directory and the private key must be kept secret. The sender encrypts a message with the recipient's public key. On receiving the message, the recipient uses his or her private key to decrypt it.

Digital certificates are data files used to establish the identity of users and electronic assets for protection of online transactions. A digital certificate system uses a trusted third party, known as a certificate authority (CA, or certification authority), to validate a user's identity. Public key infrastructure (PKI), the use of public key cryptography working with a CA, is now widely used in e-commerce.

Ensuring System Availability

As companies increasingly rely on digital networks for revenue and operations, they need to take additional steps to ensure that their systems and applications are always available. Firms such as those in the airline and financial services industries with critical applications requiring online transaction processing have traditionally used fault-tolerant computer systems for many years to ensure 100-percent availability. In online transaction processing, transactions entered online are immediately processed by the computer. Multitudinous changes to databases, reporting, and requests for information occur each instant.

Fault-tolerant computer systems contain redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service. Fault-tolerant computers use special software routines or self-checking logic built into their circuitry to detect hardware failures and automatically switch to a backup device. Parts from these computers can be removed and repaired without disruption to the computer system.

Fault tolerance should be distinguished from high-availability computing. Both fault tolerance and high-availability computing try to minimize downtime. Downtime refers to periods of time in which a system is not operational. However, high-availability computing helps firms recover quickly from a system crash, whereas fault tolerance promises continuous availability and the elimination of recovery time altogether.

Controlling Network Traffic: Deep Packet Inspection

Bandwidth-consuming applications such as file-sharing programs, Internet phone service, and online video are able to clog and slow down corporate networks, degrading performance. A technology called Deep Packet Inspection (DPI) helps solve this problem. DPI examines data files and sorts out low-priority online material while assigning higher priority to business- critical files. Based on the priorities established by a network's operators, it decides whether a specific data packet can continue to its destination or should be blocked or delayed while more important traffic proceeds.

Security Outsourcing

Many companies, especially small businesses, lack the resources or expertise to provide a secure high-availability computing environment on their own. They can outsource many security functions to Managed Security Service Providers (MSSPS) that monitor network activity and perform vulnerability testing and intrusion detection. Secure Works, BT managed Security Solutions Group, and Symantec are leading providers of MSSP services.

SECURITY ISSUES FOR CLOUD COMPUTING AND THE MOBILE DIGITAL PLATFORM

Although cloud computing and the emerging mobile digital platform have the potential to deliver powerful benefits, they pose new challenges to system security and reliability. We now describe some of these challenges and how they should be addressed.

Security in the Cloud

When processing takes place in the cloud, accountability and responsibility for protection of sensitive data still reside with the company owning that data. Understanding how the cloud computing provider organizes its services and manages the data is critical.

Cloud computing is highly distributed. Cloud applications reside in large remote data centers and server farms that supply business services and data management for multiple corporate clients. To save money and keep costs low, cloud computing providers often distribute work to data centers around the globe where work can be accomplished most efficiently. When you use the cloud, you may not know precisely where your data are being hosted. The dispersed nature of cloud computing makes it difficult to track unauthorized activity. Virtually all cloud providers use encryption, such as Secure Sockets Layer, to secure the data they handle while the data are being transmitted. But if the data are stored on devices that also store other companies' data, it's important to ensure these stored data are encrypted as well. Companies expect their systems to be running 24/7, but cloud providers haven't always been able to provide this level of service. On several occasions over the past few years, the cloud services of Amazon.com and Salesforce. com experienced outages that disrupted business operations for millions of users.

Securing Mobile Platforms

If mobile devices are performing many of the functions of computers, they need to be secured like desktops and laptops against malware, theft, accidental loss, unauthorized access, and hacking attempts. Mobile devices accessing corporate systems and data require special protection. Companies should make sure that their corporate security policy includes mobile devices, with additional details on how mobile devices should be supported, protected, and used. They will need mobile device management tools to authorize all devices in use; to maintain accurate inventory records on all mobile devices, users, and applications; to control updates to applications; and to lock down or erase lost or stolen devices so they can't be compromised. Data loss prevention technology can identify where critical data are saved, who is accessing the data, how data are leaving the company, and where the data are going. Firms should develop guidelines stipulating approved mobile platforms and software applications as well as the required software and procedures for remote access of corporate systems. The organization's mobile security policy should forbid employees from using unsecure, consumer-based applications for transferring and storing corporate documents and files, or sending such documents and files to oneself via e-mail without encryption.

ENSURING SOFTWARE QUALITY

In addition to implementing effective security and controls, organizations can improve system quality and reliability by employing software metrics and rigorous software testing. Software metrics are objective assessments of the system in the form of quantified measurements. Ongoing use of metrics allows the information systems department and end users to jointly measure the performance of the system and identify problems as they occur. Examples of software metrics include the number of transactions that can be processed in a specified unit of time, online response time, the number of payroll checks printed per hour, and the number of known bugs per hundred lines of program code. For metrics to be successful, they must be carefully designed, formal, objective, and used consistently.

J. Information Security Management

5.2 INFORMATION SECURITY MANAGEMENT

Security objectives to meet organization's business requirements include the following:

- Ensure the continued availability of their information systems.
- Ensure the integrity of the information stored on their computer systems and while in transit.
- Preserve the confidentiality of sensitive data while stored and in transit.
- Ensure conformity to applicable laws, regulations and standards.
- Ensure adherence to trust and obligation requirements in relation to any information relating to an identified or identifiable individual (i.e., data subject) in accordance with its privacy policy or applicable privacy laws and regulations.

COBIT 5 separates information goals into three sub-dimensions of quality:

- **Intrinsic quality-** The extent to which data values are in conformance with the actual or true values. it includes:
  - **Accuracy-** The extent to which information is correct and reliable
  - **Objectivity-** The extent to which information is unbiased, unprejudiced and impartial
  - **Believability-** The extent to which information is regarded as true and credible
  - **Reputation-** The extent to which information is highly regarded in terms of its source or content.

- **Contextual and representational quality-** The extent to which information is applicable to the task of the information user and is presented in a intelligible and clear manner, recognizing that information quality depends on the context of use. It includes:
  - **Relevancy-** The extent to which information is applicable and helpful for the task at hand
  - **Completeness-** The extent to which information is not missing and is of sufficient depth and breadth for the task at hand
  - **Currency-** The extent to which information is sufficiently up to date for the task at hand
  - **Appropriate amount of information-** The extent to which the volume of information is appropriate for the task at hand
  - **Concise representation-** The extent to which information is compactly represented
  - **Consistent representation-** The extent to which information is presented i the same formal

- **Security/accessibility quality-** The extent to which information is available or obtainable. It includes:
    - **Availability/timeliness-** The extent to which information is available when required or is easily and quickly retrievable
    - **Restricted access-** The extent to which access to information is restricted appropriately to authorized parties.

5.2.1 KEY ELEMENTS OF INFORMATION SECURITY MANAGEMENT

An information security management system (ISMS) is a framework of policies, procedures, guidelines and associated resources to establish, implement, operate, monitor, review, maintain and improved information security for all types of organizations.

Exhibit 5.2—Key Elements of Information Security Management

Senior management commitment and support	Commitment and support from senior management are important for successful establishment and continuance of an information security management program.
Policies and procedures	The policy framework should be established with a concise top management declaration of direction, addressing the value of information assets, the need for security, and the importance of defining a hierarchy of classes of sensitive and critical assets. After approval by the governing body of the organization and by related roles and responsibilities, the information security program will be substantiated with the following: • Standards to develop minimum security baselines • Measurement criteria and methods • Specific guidelines, practices and procedures The policy should ensure resource conformity with laws and regulations. Security policies and procedures must be up to date and reflect business objectives, as well as generally accepted security standards and practices.
Organization	Responsibilities for the protection of individual assets should be clearly defined. The information security policy should provide general guidance on the allocation of security roles and responsibilities in the organization and, where necessary, detailed guidance for specific sites, assets, services and related security processes, such as IT recovery and business continuity planning.
Security awareness and education	All employees of an organization and, where relevant, third-party users should receive appropriate training and regular updates to foster security awareness and compliance with written security policies and procedures. For new employees, this training should occur before access to information or service is granted. A number of different mechanisms available for raising security awareness include: • Regular updates to written security policies and procedures • Formal information security training • Internal certification program for relevant personnel • Statements signed by employees and contractors agreeing to follow the written security policy and procedures, including nondisclosure obligations • Use of appropriate publication media for distribution of security-related material (e.g., company newsletter, web page, videos, etc.) • Visible enforcement of security rules and periodic audits • Security drills and simulated security incidents
Monitoring and compliance	IS auditors are usually charged to assess, on a regular basis, the effectiveness of an organization's security program(s). To fulfill this task, they must have an understanding of the protection schemes, the security framework and the related issues, including compliance with applicable laws and regulations. As an example, these issues may relate to organizational due diligence for security and privacy of sensitive information, particularly as it relates to specific industries (e.g., banking and financial institutions, health care).
Incident handling and response	A computer security incident is an event adversely affecting the processing of computer usage. This includes loss of confidentiality of information, compromise of integrity of information, denial of service, unauthorized access to systems, misuse of systems or information, theft and damage to systems. Other incidents include virus attacks and intrusion by humans within or outside the organization.

5.2.2 INFORMATION SECURITY MANAGEMENT ROLES AND RESPONSIBILITIES

All defined and documented responsibilities and accountabilities must be established and communicated to all relevant personnel and management. Exhibit 5.3 presents roles and responsibilities of groups who interact with information security management.

IS security steering committee: Security policies, guidelines and procedures affect the entire organization and, as such, should have the support and suggestions of end users, executive management, auditors, security administration, IS personnel and legal counsel. Therefore, individuals representing various

management levels should meet as a committee to discuss these issues, and establish and approve security practices. The committee should be formally established with appropriate terms of reference.

Executive management	Responsible for the overall protection of information assets, and for issuing and maintaining the policy framework.
Security advisory group	Responsible for the review of the security plans of the organization. This group should include people involved in the business. The group should provide comments on security issues to the chief security officer and communicate to the business whether the security programs meet the business objectives.
Chief privacy officer (CPO)	A senior level corporate official responsible for articulating and enforcing the policies that companies use to protect their customers' and employees' privacy rights.
Chief information security officer (CISO)	A senior level corporate official responsible for articulating and enforcing the policies that companies use to protect their information assets. This is a much broader roll than a chief security officer (CSO), who is normally only responsible for physical security within the organization.

Process owners	Ensure appropriate security measures are consistent with organizational policy and are maintained.
Information assets owners and data owners	Ownership entails responsibility for the owned asset.
Users	Follow procedures set out in the organization's security policy and adhere to privacy and security regulations, which are often specific to sensitive application fields (e.g., health, finance, legal, etc.).
External parties	Include third-party providers and trading partners that deal with the organization's information assets or have access to company premises.
Security administrator	Staff level position responsible for providing adequate physical and logical security for IS programs, data and equipment. Normally, the information security policies will provide the basic guidelines under which the security administrator will operate.
Security specialists/ advisors	Assist with the design, implementation, management and review of the organization's security policy, standards and procedures.
IT developers	Implement information security within their applications.
IS auditors	Provide independent assurance to management on the appropriateness and effectiveness of information security objectives and the controls related to these objectives.

5.2.3 CLASSIFICATION OF INFORMATION ASSETS

Effective control requires a detailed inventory of information assets. Such a list is the first step in classifying the assets and determining the level of protection to be provided to each asset.

Information assets have varying degrees of sensitivity and criticality in meeting business objectives. By assigning classes or levels of sensitivity and criticality to information resources and establishing specific security rules for each class, it is possible to define the level of access controls that should be applied to each information asset. Classification of information assets reduces the risk and cost of over- or under-protecting information resources in linking security to business objectives since it helps to build and maintain a consistent perspective of the security requirements for information assets throughout the organization.

Data classification is a major part of managing data as an asset. Data classifications as a control measure should define:

- The importance of the information asset
- The information asset owner
- The process for granting access
- The person responsible for approving the access rights and access levels
- The extent and depth of security controls

Classification of information:

Public Information	Company brochures
Private Information	Internal policies, procedures, normal business e-mail messages, newsletter, etc.
Sensitive Information	Unpublished financials, company secrets, etc.

For rest of the topics: Page 338-352 of CISA Manual

K. Auditing Information Security Management Framework

5.5 AUDITING INFORMATION SECURITY MANAGEMENT FRAMEWORK

Auditing the information security framework of an organization involves the audit of logical access, the use of techniques for testing security and the use of investigation techniques.

5.5.1 AUDITING INFORMATION SECURITY MANAGEMENT FRAMEWORK

The information security management framework should be reviewed per the basic elements in an information security framework.

Reviewing Written Policies, Procedures and Standards

Policies and procedures provide the framework and guidelines for maintaining proper operation and control. The IS auditor should review the policies and procedures to determine if they set the tone for proper security and provide a means for assigning responsibility for maintaining a secure computer processing environment.

Logical Access Security Policies

These policies should encourage limiting logical access on a need-to-know basis. They should reasonably assess the exposure to the identified concerns.

Formal Security Awareness and Training

Effective security will always be dependent on people. As a result, security can only be effective if employees know what is expected of them and what their responsibilities are. They should know why various security measures, such as locked doors and use of logon IDs, are in place and the repercussions of violating security.

Data Ownership

Data ownership refers to the classification of data elements and the allocation of responsibility for ensuring that they are kept confidential, complete and accurate. A key point of ownership is that, by assigning responsibility for protecting computer data to particular employees, accountability is established.

Data Owners

These people are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rules for the data for which they are responsible.

Data Custodians

These people are responsible for storing and safeguarding the data, and include IS personnel such as systems analysts and computer operators.

Security Administrator

Security administrators are responsible for providing adequate physical and logical security for IS programs, data and equipment. (The physical security may be handled by someone else, not always by the security administrator.) Normally, the information security policy will provide the basic guidelines under which the security administrator will operate.

New IT Users

New IT users (employees or third parties) and, in general, all new users assigned PCs or other IT resources should sign a document containing the main IT security obligations that they are thereby engaged to know and observe. These are:

- Reading and agreeing to follow security policies
- Keeping logon IDs and passwords secret
- Creating quality passwords according to policy
- Locking their terminal screens when not in use
- Reporting suspected violations of security
- Maintaining good physical security by keeping doors locked,
- safeguarding access keys, not disclosing access door lock
- combinations and questioning unfamiliar people
- Conforming to applicable laws and regulations

- Use of IT resources only for authorized business purposes

Data Users
Data users, including the internal and the external user community, are the actual users of the computerized data. Their levels of access into the computer should be authorized by the data owners, and restricted and monitored by the security administrator. Their responsibilities regarding security are to be vigilant regarding the monitoring of unauthorized people in the work areas and comply with general security guidelines and policies.

Documented Authorizations
Data access should be identified and authorized in writing. The IS auditor can review a sample of these authorizations to determine if the proper level of written authority was provided. If the facility practices data ownership, only the data owners provide written authority.

Terminated Employee Access
Termination of employment can occur in the following circumstances:
- On the request of the employee (voluntary resignation from service)
- Scheduled (on retirement or completion of contract)
- Involuntary (forced by management in special circumstances)

Security Baselines
A baseline security plan is meant to be used as a first step to IT security. The baseline plan should be followed with a full security evaluation and plan.

Access Standards
Access standards should be reviewed by the IS auditor to ensure they meet organizational objectives for separating duties, prevent fraud or error, and meet policy requirements for minimizing the risk of unauthorized access.
Standards for security may be defined:
- At a generic level (e.g., all passwords must be at least five characters long)
- For specific machines (e.g., all UNIX machines can be configured to enforce password changes)
- For specific application systems (e.g., sales ledger clerks can access menus that allow entry of sales invoices, but may not access menus that allow check authorization)

5.5.2 AUDITING LOGICAL ACCESS
When evaluating logical access controls the IS auditor should:
- Obtain a general understanding of the security risks facing information processing, through a review of relevant documentation, inquiry, observation, risk assessment and evaluation techniques
- Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness by reviewing appropriate hardware and software security features and identifying any deficiencies or redundancies
- Test controls over access paths to determine whether they are functioning and effective by applying appropriate audit techniques
- Evaluate the access control environment to determine if the control objectives are achieved by analyzing test results and other audit evidence
- Evaluate the security environment to assess its adequacy by reviewing written policies, observing practices and procedures, and comparing them with appropriate security standards or practices and procedures used by other organizations

Familiarization with the IT Environment
This is the first step of the audit and involves obtaining a clear understanding of the technical, managerial and security environment of the IS processing facility. This typically includes interviews, physical walk - through, review of documents and risk assessments.

Assessing and Documenting the Access Paths
The access path is the logical route an end user takes to access computerized information. This starts with a terminal/workstation and typically ends with the data being accessed. Along the way, numerous hardware and software components are encountered. The IS auditor should evaluate each component for proper implementation and physical and logical access security.

Special consideration should be given to the:

- Origination and authorization of the data
- Validity and correctness of the input data
- Maintenance of the affected operating systems (patching, hardening and closing the unnecessarily open ports)

Interviewing Systems Personnel

To control and maintain the various components of the access path, as well as the operating system and computer mainframe, technical experts often are required. These people can be a valuable source of information to the IS auditor when gaining an understanding of security. To determine who these people are, the IS auditor should meet with the IS manager and review organizational charts and job descriptions. Key people include the security administrator, network control manager and systems software manager.

Reviewing Reports from Access Control Software

The reporting features of access control software provide the security administrator with the opportunity to monitor adherence to security policies. By reviewing a sample of security reports, the IS auditor can determine if enough information is provided to support an investigation and if the security administrator is performing an effective review of the report.

Reviewing Application Systems Operations Manual

An application systems manual should contain documentation on the programs that generally are used throughout a data processing installation to support the development, implementation, operations and use of application systems. This manual should include information about the platform the application can run on, DBMSs, compilers, interpreters, telecommunication monitors and other applications that can run with the application.

5.5.3 TECHNIQUES FOR TESTING SECURITY

Auditors can use different techniques for testing security. Some methods are described in the following subsections.

Terminal Cards and Keys

The IS auditor can take a sample of these cards or keys and attempt to gain access beyond that which is authorized. Also, the IS auditor will want to know if the security administrator followed up on any unsuccessful attempted violations.

Terminal Identification

The IS auditor can work with the network manager to get a listing of terminal addresses and locations. This list can then be used to inventory the terminals, looking for incorrectly logged, missing or additional terminals. The IS auditor should also select a sample of terminals to ensure that they are identified in the network diagram.

Logon IDs and Passwords

To test confidentiality, the IS auditor could attempt to guess the password of a sample of employees' logon IDs (though this is not necessarily a test). This should be done discreetly to avoid upsetting employees. The IS auditor should tour end-user and programmer work areas looking for passwords taped to the side of terminals, the inside of desk drawers or located in card files.

To test encryption, the IS auditor should work with the security administrator to attempt to view the internal password table. If viewing is possible, the contents should be unreadable. Being able to view encrypted passwords can still be dangerous.

To test access authorization, the IS auditor should review a sample of access authorization documents to determine if proper authority has been provided and if the authorization was granted on a need-to-know basis.

Account settings for minimizing authorized access should be available from most access control software or from the operating system. To verify that these settings actually are working, the IS auditor can perform the following manual tests:

- To test periodic change requirements, the IS auditor can draw on his/her experiences using the system and interview a sample of users to determine if they are forced to change their password after the prescribed time interval.

- To test for disabling or deleting of inactive logon IDs and passwords, the IS auditor should obtain a computer-generated list of active logon IDs. On a sample basis, the IS auditor should match this list to current employees, looking for logon IDs assigned to employees or consultants who are no longer with the company.
- To test for password syntax, the IS auditor should attempt to create passwords in a format that is invalid, such as too short, too long, repeated from the previous password, incorrect mix of alpha or numeric characters, or the use of inappropriate characters.
- To test for automatic logoff of unattended terminals, the IS auditor should log on to a number of terminals. The IS auditor then simply waits for the terminals to disconnect after the established time interval. Before beginning this test, the IS auditor should verify with the security administrator that this automatic logoff feature applies to all terminals.
- To test for automatic deactivation of terminals after unsuccessful access attempts, the IS auditor should attempt to log on, purposefully entering the wrong password a number of times. The logon ID should deactivate after the established number of invalid passwords has been entered. The IS auditor will be interested in how the security administrator reactivates the logon ID. If a simple telephone call to the security administrator with no verification of identification results in reactivation, then this function is not controlled properly.
- To test for masking of passwords on terminals, the IS auditor should log on to a terminal and observe if the password is displayed when entered.

Controls over Production Resources
The IS auditor should work with the system software analyst and operations manager to determine if access is on a need-to-know basis for all sensitive production resources. Working with the security administrator, the IS auditor should determine who can access these resources and what can be done with this access.

Logging and Reporting of Computer Access Violations
To test the reporting of access violations, the IS auditor should attempt to access computer transactions or data for which access is not authorized. The attempts should be unsuccessful and identified on security reports. This test should be coordinated with the data owner and security administrator to avoid violation of security regulations.

Follow-up Access Violations
To test the effectiveness and timeliness of the security administrator and data owner's responses to reported violation attempts, the IS auditor should select a sample of security reports and look for evidence of follow-up and investigation of access violations. If such evidence cannot be found, the IS auditor should conduct further interviews to determine why this situation exists.

Bypassing Security and Compensating Controls
This is a technical area of review. As a result, the IS auditor should work with the system software analyst, network manager, operations manager and security administrator to determine ways to bypass security.

Review Access Controls and Password Administration
Access controls and password administration are reviewed to determine that:
• Procedures exist for adding individuals to the list of those authorized to have access to computer resources, changing their access capabilities and deleting them from the list
• Procedures exist to ensure that individual passwords are not inadveliently disclosed
• Passwords issued are of an adequate length, cannot be easily guessed and do not contain repeating characters
• Passwords are periodically changed
• User organizations periodically validate the access capabilities currently provided to individuals in their department
• Procedures provide for the suspension of user identification codes (logon IDs or accounts) or the disabling of terminal, microcomputer or data entry device activity-after a particular number of security procedure violations

5.5.4 INVESTIGATION TECHNIQUES
Investigation of Computer Crime
Computer crimes are not reported in most cases simply because they are not detected. In many cases where computer crimes are detected, companies hesitate to report them since they generate a large amount of negative publicity that can affect their business. In such cases, the management of the affected company seeks to simply plug the loopholes used for the crime and move on.

In the aftermath of a computer crime, it is very important that proper procedures are used to collect evidence from the crime scene. If data and evidence is not collected in the proper manner, it could be damaged and, even if the perpetrator is eventually identified, prosecution will not be successful in the absence of undamaged evidence. Therefore, after a computer crime, the environment and evidence must be left unaltered and specialist law enforcement officials must be called in. If the incident is to be handled in-house, the company must have a suitably qualified and experienced incident response team.

Computer Forensics
Computer forensics is defined as the "process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings. An IS auditor may be required or asked to be involved in a forensic analysis in progress to provide expert opinion or to ensure the correct interpretation of information gathered.

Computer forensics includes activities that involve the exploration and application of methods to gather, process, interpret and use digital evidence that help to substantiate whether an incident happened such as:

- Providing validation that an attack actually occurred
- Gathering digital evidence that can later be used in judicial proceedings.

For evidence to be admissible in a court of law, the chain of custody needs to be maintained professionally. The chain of evidence essentially contains information regarding:

- Who had access to the evidence
- The procedures followed in working with the evidence e.g. disk duplication, virtual memory dump
- Proving that the analysis is based on copies that are identical to the original evidence e.g. documentation, checksums or timestamps.

There are four major considerations in the chain of events in regards to evidence in computer forensics:

- **Identify-** Refers to the identification of information that is available and might form the evidence of an incident.
- **Preserve-** Refers to the practice of retrieving identified information and preserving it as evidence.
- **Analyze-** Involves extracting, processing and interpreting the evidence.
- **Present-** Involves a presentation to the various audiences such as management, attorneys, court, etc.

The IS auditor should give consideration to key elements of computer forensics during audit planning. The key elements are described in the following subsection:

- Data protection
- Data acquisition
- Imaging
- Extraction
- Interrogation
- Ingestion/normalization
- Reporting
- Protection of evidence and chain of custody.

L. Cybersecurity

The Rise of the Cyber Threat
Cyber criminals are working on new techniques for getting through the security of established organizations, accessing everything from IP to individual customer information — they are doing this so that they can cause damage, disrupt sensitive data and steal intellectual property.
Every day, their attacks become more sophisticated and harder to defeat. Because of this ongoing development, we cannot tell exactly what kind of threats will emerge next year, in five years' time, or in 10 years' time; we can only say that these threats will be even more dangerous than those of today. We can also be certain that as old sources of this threat fade, new sources will emerge to take their place. Despite this uncertainty we need to be clear about the type of security controls needed.

Cyber-attacks have transformed the risk landscape
It's important to remember that cybersecurity is a business-wide issue and not just a technology risk. Since many opportunities for Internet of Things (IoT) will arise through technological integration and collaboration, which will continue to increase in complexity — this complexity breeds risk.

Traditional proven risk management models have their origins and wisdom still focused in a world where the organization owns and possesses most, if not all, of the data assets flowing through the systems. The increasing use of the internet and mobile working means that the boundary of the enterprise is disappearing: and as a result, the risk landscape also becomes unbounded.
A cybersecurity system should also include the organization's broader network, including clients, customers, suppliers/vendors, collaborators, business partners and even their alumni
— together called the "business ecosystem."

An extended ecosystem is governed and managed by various actors with individual policies and assurance requirements; and these actors sometimes have very different interests and business objectives within the collaboration. It is therefore necessary to adjust the organization's normal risk focus to take this into consideration.

An extended ecosystem is governed and managed by various actors with individual policies and assurance requirements; and these actors sometimes have very different interests and business objectives within the collaboration. It is therefore necessary to adjust the organization's normal risk focus to take this into consideration.

The Multiplying Effect Of Today's Cybersecurity Challenges

The overall risk "landscape" of the organization is only a part of a potentially contradictory and opaque universe of actual and potential threats that all too often come from completely unexpected and unforeseen threat actors, which can have an escalating effect.

The Speed of Change
In this post-economic-crisis world, businesses move fast. New product launches, mergers, acquisitions, market expansion, and introductions of new technology are all on the rise: these changes invariably have a complicating impact on the strength and breadth of an organization's cybersecurity, and its ability to keep pace.

A Network of Networks
The use of the internet via smartphones and tablets has made an organization's data accessible everywhere and at any time. Inevitably, one vulnerable device can lead to other vulnerable devices, and it is almost impossible to patch all the vulnerabilities for all the devices. For the cyber criminals, it won't be hard to find a target for their attack. With even more devices connected, it will be even easier for a cyber-criminal to get into your attack vector.

Infrastructure
Traditionally closed operating technology systems have increasingly been given IP addresses that can be accessed externally, so that cyber threats are making their way out of the back office systems and into critical infrastructures, such as power generation and transportation systems and other automation systems.

Cloud Computing

Cloud computing has been a prerequisite for IoT from the very early days of its evolution. The cloud provides a platform for IoT to flourish, however, there are still many challenges which we face today when it comes to cloud security or data security in the cloud. With our data stored on such cloud services, there is also a risk of increase in spam as the cloud servers are virtually moved from one geographic location to another in a matter of minutes, depending upon the requirement.

Application Risk
This presents mainly two security risks:

- Malicious apps (malware): the increase in the number of apps on the device increases the likelihood that some may contain malicious code or security holes
- App vulnerabilities: apps developed or deployed by the organization to enable access to corporate data may contain security weaknesses

Growing Use of Mobile Devices
Smart phones have already become an integral part of our lives; we rely on them to hold significant information, such as our home address, credit card details, personal photos/videos, e-mail accounts, official documents, contact numbers and messages. The information stored on our devices will include the places that we visit frequently and a "pattern" that uniquely identifies us, so anyone who can hack into any of these devices can get into our lives very easily.

The "Bring Your Own Device" employer
BYOD significantly impacts the traditional security model of protecting the perimeter of the IT organization by blurring the definition of that perimeter, both in terms of physical location and in asset ownership. A holistic and methodical approach should be used to define this risk and help to ensure that controls exist to maintain both the security and usability of the devices in the enterprise.

Bandwidth Consumption
The bandwidth consumption from billions of devices will put a strain on the spectrum of other wireless communications, which also operate on the megahertz frequencies like radio, television, emergency services, etc. However, companies have started taking this seriously; as a result, Qualcomm has launched its low power Wi-Fi connectivity platform for IoT.

Governance and Compliance Issues.
Increasing privacy legislation is a trend that likely will continue in the near future. A well- formed IoT policy should include defined, clear expectations on privacy-impacting procedures, bearing in mind that legislation may differ in certain geographical regions.

Privacy and Data Protection
All IoT devices gather accurate data from the real world, which is excellent from an analytics prospective, but a user might not be comfortable with sharing that data with a third party — even if not all the data is confidential or sensitive. Some of the top privacy risks also contain web application vulnerabilities, operator-side data leakage, insufficient data breach response, data sharing with third parties, and insecure data transfer.

If the organization is collecting personal data, the purpose, expiration, security, etc., of the data collected must be clearly stated in the information security policy. If data is processed by a third party (i.e., if the organization utilizes a cloud email provider), it is important that the data be protected by a data processing agreement with the third party.

Breach Investigation and Notification
Following the impact of highly publicized cyber-attacks, new and future legislation is proposed on cybersecurity, with fines being levied on companies who do not protect consumer data, and mandatory actions are being introduced around data breach notification. Organizations should prepare for this legislation by keeping an active inventory of devices, the data on them and the security controls in place to protect that data.

So How Can Organizations Get Ahead Of Cybercrime?

No organization or government can ever predict or prevent all (or even most) attacks; but they can reduce their attractiveness as a target, increase their resilience and limit damage from any given attack.
A state of readiness includes:

- Designing and implementing a cyber threat intelligence strategy to support strategic business decisions and leverage the value of security
- Defining and encompassing the organizations extended cybersecurity ecosystem, including partners, suppliers, services and business networks
- Taking a cyber economic approach — understanding your vital assets and their value, and investing specifically in their protection
- Using forensic data analytics and cyber threat intelligence to analyze and anticipate where the likely threats are coming from and when, increasing your readiness
- Ensuring that everyone in the organization understands the need for strong governance, user controls and accountability

Organizations may not be able to control when information security incidents occur, but they can control how they respond to them — expanding detection capabilities is a good place to start. A well-functioning security operations center (SOC) can form the heart of effective detection.

Follow leading cybersecurity practices

By leveraging-industry leading practices and adopting strategies that are flexible and scalable, organizations will be better equipped to deal with incoming (sometimes unforeseen) challenges to their security infrastructure.

Know your environment, inside and out

Comprehensive, yet targeted, situational awareness is critical to understanding the wider threat landscape and how it relates to the organization. Cyber threat intelligence can bring this knowledge — it incorporates both external and internal sources of risk, and covers both the present and future, while learning from the past.

Continually learn and evolve

Nothing is static — not the criminals, not the organization or any part of its operating environment — therefore the cycle of continual improvement remains. Become a learning organization: study data (including forensics), maintain and explore new collaborative relationships, refresh the strategy regularly and evolve cybersecurity capabilities.

Be confident in your incident response and crisis response mechanisms

Organizations that are in a state of anticipation regularly rehearse their incident response capabilities. This includes war gaming and table top exercises, through to enacting complex incident scenarios that really test the organization's capabilities.

Align cybersecurity to business objectives

The organization's leadership should understand and discuss how cybersecurity enables the business to innovate, open new channels to market and manage risk. To be successful, the information security function needs leadership support in providing the appropriate revenue to support and grow better security protection, to promote cybersecurity awareness within the workforce, and to sponsor cooperation with business peers.

CHAPTER # 05: DEVELOPING BUSINESS/ IT SOLUTIONS

A. Developing Business Systems

The Systems Approach

The systems approach to problem solving uses a systems orientation to define problems and opportunities and then develop appropriate, feasible solutions in response.

Analyzing a problem and formulating a solution involve the following interrelated activities:

1. Recognize and define a problem or opportunity using systems thinking.
2. Develop and evaluate alternative system solutions.
3. Select the system solution that best meets your requirements.
4. Design the selected system solution.
5. Implement and evaluate the success of the designed system.

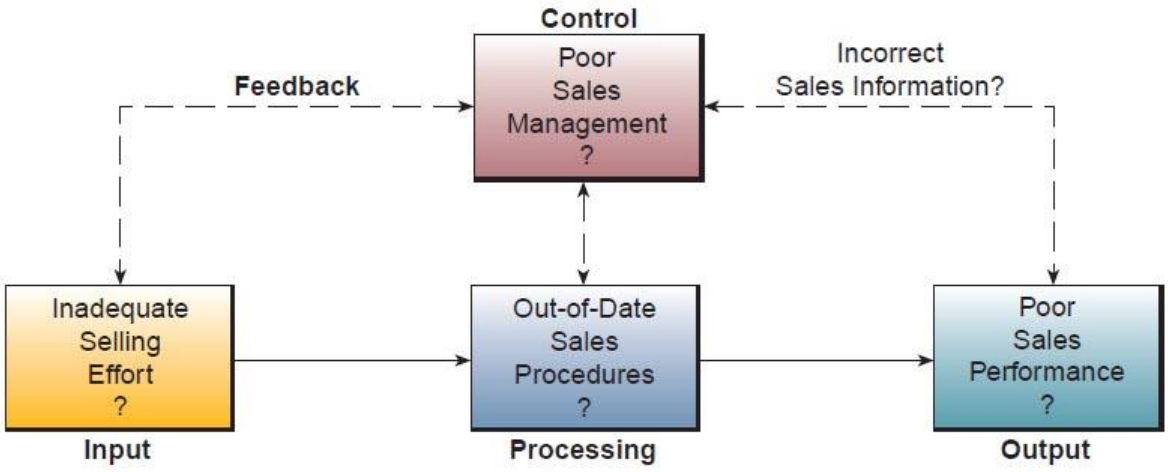
When the systems approach to problem solving is applied to the development of information systems solutions to business problems, it is called information systems development or application development.

Systems Thinking

Using systems thinking to understand a problem or opportunity is one of the most important aspects of the systems approach. Peter Senge argues that mastering systems thinking is vital to personal fulfillment and business success in a world of constant change. One way of practicing systems thinking is to try to find systems, subsystems, and components of systems in any situation you are studying. This is also known as using a systems context, or having a systemic view of a situation. For example, the business organization or business process in which a problem or opportunity arises could be viewed as a system of input, processing, output, feedback, and control components. Then to understand a problem and solve it, you would determine whether these basic systems functions are being properly performed.

Example. The sales process of a business can be viewed as a system. You could then ask: Is poor sales performance (output) caused by inadequate selling effort (input), out-of-date sales procedures (processing), incorrect sales information (feedback), or inadequate sales management (control)?

FIGURE 12.2
An example of systems thinking



Systems Analysis and Design

The overall process by which information systems are designed and implemented within organizations is referred to as systems analysis and design (SA&D). Within this process are contained activities that include the identification of business problems; the proposed solution, in the form of an information system (IS), to one or more of the problems identified; and the design and implementation of that proposed solution to achieve the desired and stated goals of the organization.

There have two most common approaches to SA & D are **object-oriented analysis and design** and the **life cycle approach.**

The Systems Development Life Cycle

One method of using the systems approach to develop information system solutions, and the most prevalent one in organization systems analysis and design, can be viewed as a multistep, iterative process called the systems development life cycle (SDLC). These are the stage of this process: (1) investigation, (2) analysis, (3) design, (4) implementation, and (5) maintenance.

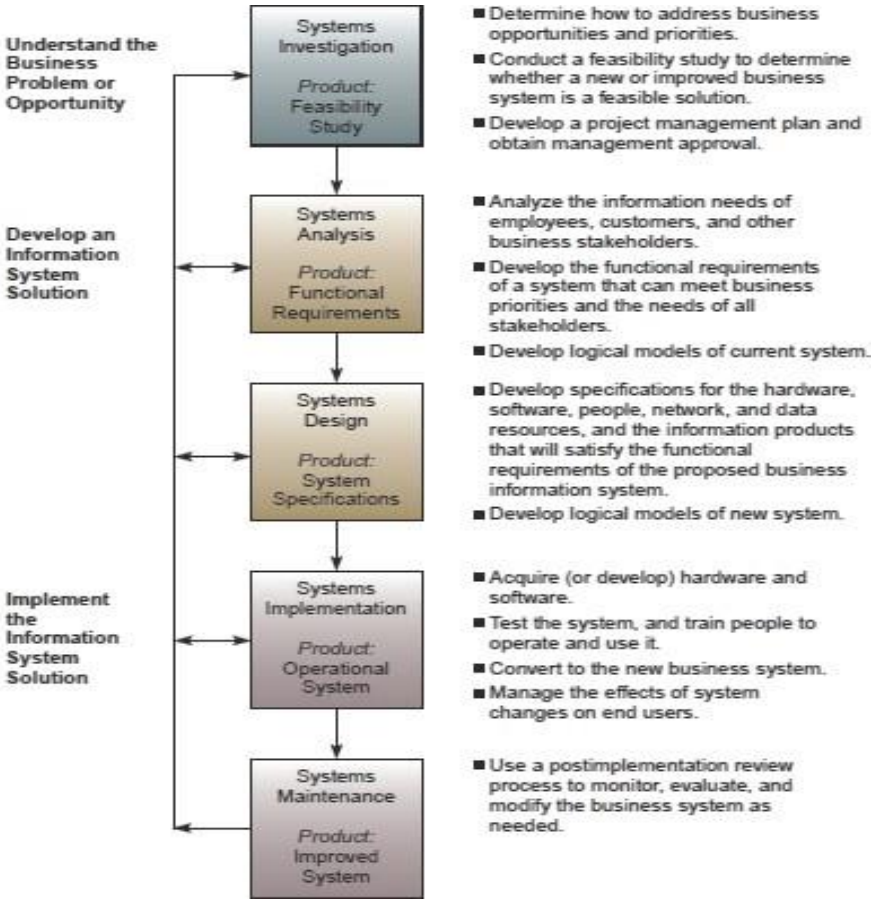


FIGURE 12.3
The traditional information systems development life cycle. Note how the five steps of the cycle are based on the stages of the systems approach. Also note the products that result from each step in the cycle, and that you can recycle back to any previous step if more work is needed.

Starting the Systems Development Process

The investigation stage includes the preliminary feasibility study of proposed information system solutions to meet a company's business priorities and opportunities as identified in a planning process.

Feasibility Studies

As the process of development can be costly, the systems investigation stage typically requires the development of a feasibility study. At this stage, this is a preliminary study where the information needs of prospective users and the resource requirements, costs, benefits, and feasibility of a proposed project are determined. A team of business professionals and IS specialists might then formalize the findings of this study in a written report that includes preliminary specifications and a developmental plan for a proposed business application. If the management of the company approves the recommendations of the feasibility study, the development process can continue.

The goal of the preliminary feasibility study is to evaluate alternative system solutions and to propose the most feasible and desirable business application for development. The feasibility of a proposed business system can be evaluated in terms of five major categories:

Operational Feasibility

The operational feasibility assessment focuses on the degree to which the proposed development project fits in with the existing business environment and objectives with regard to development schedule, delivery date, corporate culture, and existing business processes.

This assessment also determines the degree to which the project meets the specific business objectives set forth during the proposal phase.

Economic Feasibility

The purpose of the economic feasibility assessment is to determine the extent to which the proposed system will provide positive economic benefits to the organization. This determination involves the identification, and quantification, of all benefits expected from the system, as well as the explicit identification of all expected costs of the project. In the early stages of the project, defining and assessing all of the benefits and costs associated with the new system is impossible. Thus, the economic feasibility assessment is an ongoing process in which the definable short-term costs are constantly being weighed against the definable long- term benefits. The assessment of economic feasibility typically involves the preparation of a cost/ benefit analysis. If costs and benefits can be quantified with a high degree of certainty, they are referred to as tangible; if not, they are called intangible.

FIGURE 12.4
Operational, economic, technical, human, and legal/ political factors. Note that there is more to feasibility than cost savings or the availability of hardware and software.

Operational Feasibility	Economic Feasibility
• How well the proposed system supports the business priorities of the organization. • How well the proposed system will solve the identified problem. • How well the proposed system will fit with the existing organizational structure.	• Cost savings. • Increased revenue. • Decreased investment requirements. • Increased profits. • Cost/benefit analysis.
Technical Feasibility	**Human Factors Feasibility**
• Hardware, software, and network capability, reliability, and availability.	• Employee, customer, supplier acceptance. • Management support. • Determining the right people for the various new or revised roles.
Legal/Political Feasibility	
• Patent, copyright, and licensing. • Governmental restrictions. • Affected stakeholders and reporting authority.	

Technical Feasibility

The assessment of technical feasibility is focused on gaining an understanding of the present technical resources of the organization and their applicability to the expected needs of the proposed system.

FIGURE 12.5
Possible benefits of new information systems, with examples. Note that an opposite result for each of these benefits would be a cost or disadvantage of new systems.

Tangible Benefits	Example
• Increase in sales or profits.	• Development of IT-based products.
• Decrease in information processing costs.	• Elimination of unnecessary documents.
• Decrease in operating costs.	• Reduction in inventory carrying costs.
• Decrease in required investment.	• Decrease in inventory investment required.
• Increased operational efficiency.	• Less spoilage, waste, and idle time.
Intangible Benefits	**Example**
• Improved information availability.	• More timely and accurate information.
• Improved abilities in analysis.	• OLAP and data mining.
• Improved customer service.	• More timely service response.
• Improved employee morale.	• Elimination of burdensome job tasks.
• Improved management decision making.	• Better information and decision analysis.
• Improved competitive position.	• Systems that lock in customers.
• Improved business image.	• Progressive image as perceived by customers, suppliers, and investors.

The analyst must assess the degree to which the current technical resources, including hardware, software, and operating environments, can be upgraded or added to such that the needs of the proposed system can be met. If the current technology is deemed sufficient, then the technical feasibility of the project is clear. If this is not the case, however, the analyst must determine whether the technology necessary to meet the stated specifications exists.

Human Factors Feasibility

The human factors feasibility assessment focuses on the most important components of a successful system implementation: the managers and end users. No matter how elegant the technology, the system will not work if the end users and managers do not perceive it to be relevant and, therefore, do not support it.

Legal/Political Feasibility

The legal and political feasibility of a proposed project includes a thorough analysis of any potential legal ramifications resulting from the construction and implementation of the new system. Such legal issues include copyright or patent infringements.
The political side of the assessment focuses on understanding who the key stakeholders within the organization are and the degree to which the proposed system may positively or negatively affect the distribution of power. Such distribution can have major political repercussions and may cause disruption or failure of an otherwise relevant development effort.

FIGURE 12.6
Examples of how a feasibility study might measure the feasibility of a proposed e-commerce system for a business.

Operational Feasibility	Economic Feasibility
• How well a proposed e-commerce system fits the company's plans for developing Web-based sales, marketing, and financial systems.	• Savings in labor costs. • Increased sales revenue. • Decreased investment in inventory. • Increased profits. • Acceptable return on investment.
Technical Feasibility	**Human Factors Feasibility**
• Capability, reliability, and availability of Web store hardware, software, and management services.	• Acceptance of employees. • Management support. • Customer and supplier acceptance. • Staff developers have necessary skills.
Legal/Political Feasibility	
• No patent or copyright violations. • Software licensing for developer side only. • No governmental restrictions. • No changes to existing reporting authority.	

Systems Analysis

Systems analysis is not a preliminary study; however, it is an in depth study of end-user information needs that produces functional requirements that are used as the basis for the design of a new information system. Systems analysis traditionally involves a detailed study of:

- The information needs of a company and end users like yourself.
- The activities, resources, and products of one or more of the present information systems being used.
- The information system capabilities required to meet your information needs, and those of other business stakeholders that may use the system.

These are the steps of System analysis:

Organizational Analysis

An organizational analysis is an important first step in systems analysis. How can people improve an information system if they know very little about the organizational environment in which that system is located? They can't. That's why the members of a development team have to know something about the organization, its management structure, its people, its business activities, the environmental systems it must deal with, and its current information systems.

Analysis of the Present System

Before you design a new system, it is important to study the system that will be improved or replaced (assuming there is one). You need to analyze how this system uses hardware, software, network, and people resources to convert data resources, such as transactions data, into information products, such as reports and displays. Then you should document how the information system activities of input, processing, output, storage, and control are accomplished.

Logical Analysis

One of the primary activities that occur during the analysis phase is the construction of a logical model of the current system. The logical model can be thought of as a blueprint of the current system that displays only what the current system does without regard for how it does it. By constructing and analyzing a logical model of the current system, a systems analyst can more easily understand the various processes, functions, and

data associated with the system without getting bogged down with all the issues surrounding the hardware or the software.

Functional Requirements Analysis and Determination

Most difficult stage where teams work is necessary with IS analysts and other end users to determine specific business information needs. For example, first you need to determine what type of information each business activity requires; what its format, volume, and frequency should be; and what response times are necessary. Second, you must try to determine the information processing capabilities required for each system activity (input, processing, output, and storage, control) to meet these information needs.

When this step of the life cycle is complete, a set of functional requirements for the proposed new system will exist. Functional requirements are end-user information requirements that are not tied to the hardware, software, network, data, and people resources that end users presently use or might use in the new system.

FIGURE 12.7
Examples of functional requirements for a proposed e-commerce system for a business.

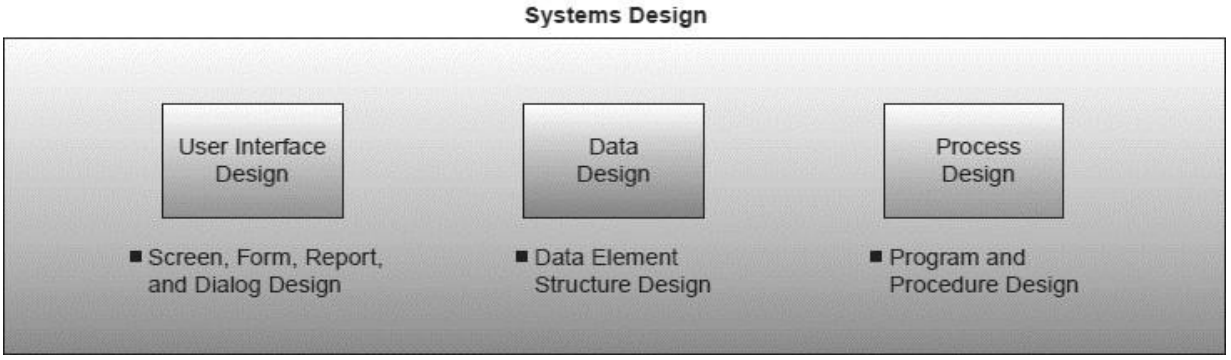
Examples of Functional Requirements
• **User Interface Requirements** Automatic entry of product data and easy-to-use data entry screens for Web customers.
• **Processing Requirements** Fast, automatic calculation of sales totals and shipping costs.
• **Storage Requirements** Fast retrieval and update of data from product, pricing, and customer databases.
• **Control Requirements** Signals for data entry errors and quick e-mail confirmation for customers.

Systems Design

Once the analysis portion of the life cycle is complete, the process of **systems design** can begin. Here is where the logical model of the current system is modified until it represents the blueprint for the new system. This version of the logical model represents what the new system will do. During the **physical** design portion of this step, users and analysts will focus on determining how the system will accomplish its objectives. This is where issues related to hardware, software, networking, data storage, security, and many others will be discussed and determined. Systems design consists of design activities that ultimately produce physical system specifications satisfying the functional requirements that were developed in the systems analysis process.

Systems design consists of three activities: user interface, data, and process design. This results in specifications for user interface methods and products, database structures, and processing and control procedures.

FIGURE 12.8 Systems design can be viewed as the design of user interfaces, data, and processes.



Prototyping

Prototyping is the rapid development and testing of working models, or **prototypes,** of new applications in an interactive, iterative process that can be used by both IS specialists and business professionals. Prototyping, as a development tool, makes the development process faster and easier, especially for projects where end-user requirements are hard to define.

The Prototyping Process

Prototyping can be used for both large and small applications. Typically, large business systems still require

using a traditional systems development approach, but parts of such systems can frequently be prototyped. A prototype of a business application needed by an end user is developed quickly using a variety of application development software tools.

FIGURE 12.9
Application development using prototyping. Note how prototyping combines the steps of the systems development life cycle and changes the traditional roles of IS specialists and end users.

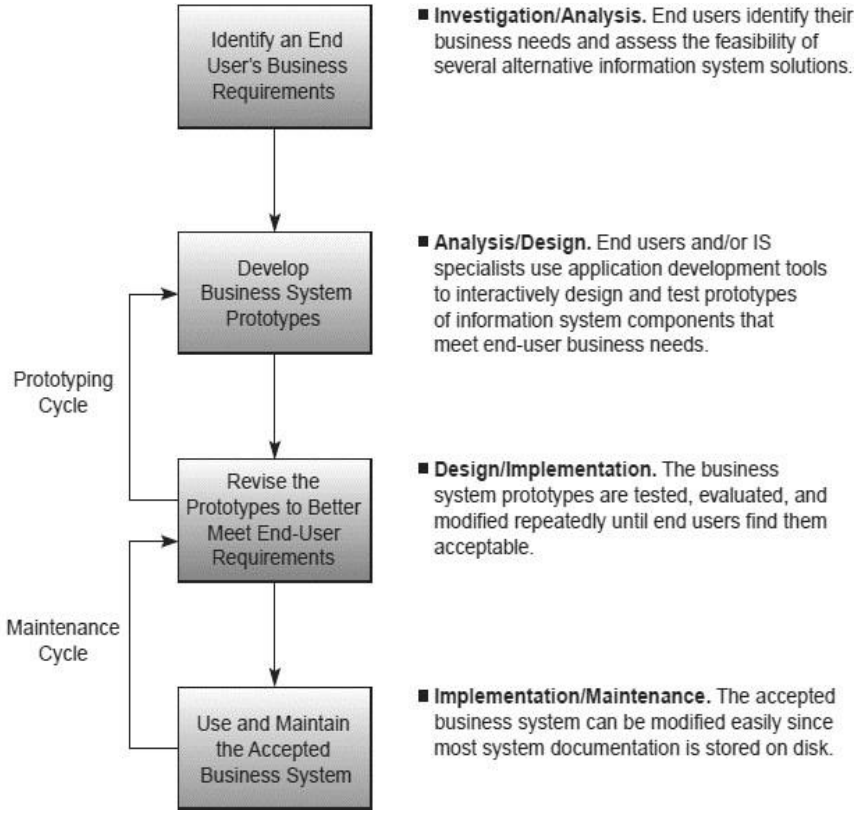


FIGURE 12.10
An example of a typical application of prototyping during a software development project.

Example of Prototyping Development
• **Team.** A few end users and IS developers form a team to develop a business application.
• **Schematic.** The initial prototype schematic design is developed.
• **Prototype.** The schematic is converted into a simple point-and-click prototype using prototyping tools.
• **Presentation.** A few screens and routine linkages are presented to users.
• **Feedback.** After the team gets feedback from users, the prototype is reiterated.
• **Reiteration.** Further presentations and reiterations are made.
• **Consultation.** Consultations are held with IT consultants to identify potential improvements and conformance to existing standards.
• **Completion.** The prototype is used as a model to create a finished application.
• **Acceptance.** Users review and sign off on their acceptance of the new business system.
• **Installation.** The new business software is installed on network servers.

User Interface Design

The user interface design activity focuses on supporting the interactions between end users and their computer-based applications. Designers concentrate on the design of attractive and efficient forms of user input and output, such as easy-to-use Internet or intranet Web pages.

User interface design is frequently a prototyping process, where working models or prototypes of user interface methods are designed and modified several times with feedback from end users. The user

interface design process produces detailed design specifications for information products such as display screens, interactive user/computer dialogues, audio responses, forms, documents, and reports.

System Specifications

System specifications formalize the design of an application's user interface methods and products, database structures, and processing and control procedures. Therefore, systems designers will frequently develop hardware, software, network, data, and personnel specifications for a proposed system

FIGURE 12.13
Examples of system specifications for a new e-commerce system for a business.

Examples of System Specifications
• **User Interface Specifications** Use personalized screens that welcome repeat Web customers and that make product recommendations.
• **Database Specifications** Develop databases that use object/relational database management software to organize access to all customer and inventory data and to multimedia product information.
• **Software Specifications** Acquire an e-commerce software engine to process all e-commerce transactions with fast responses, i.e., retrieve necessary product data and compute all sales amounts in less than one second.
• **Hardware and Network Specifications** Install redundant networked Web servers and sufficient high-bandwidth telecommunications lines to host the company e-commerce Web site.
• **Personnel Specifications** Hire an e-commerce manager and specialists and a Webmaster and Web designer to plan, develop, and manage e-commerce operations.

End-User Development

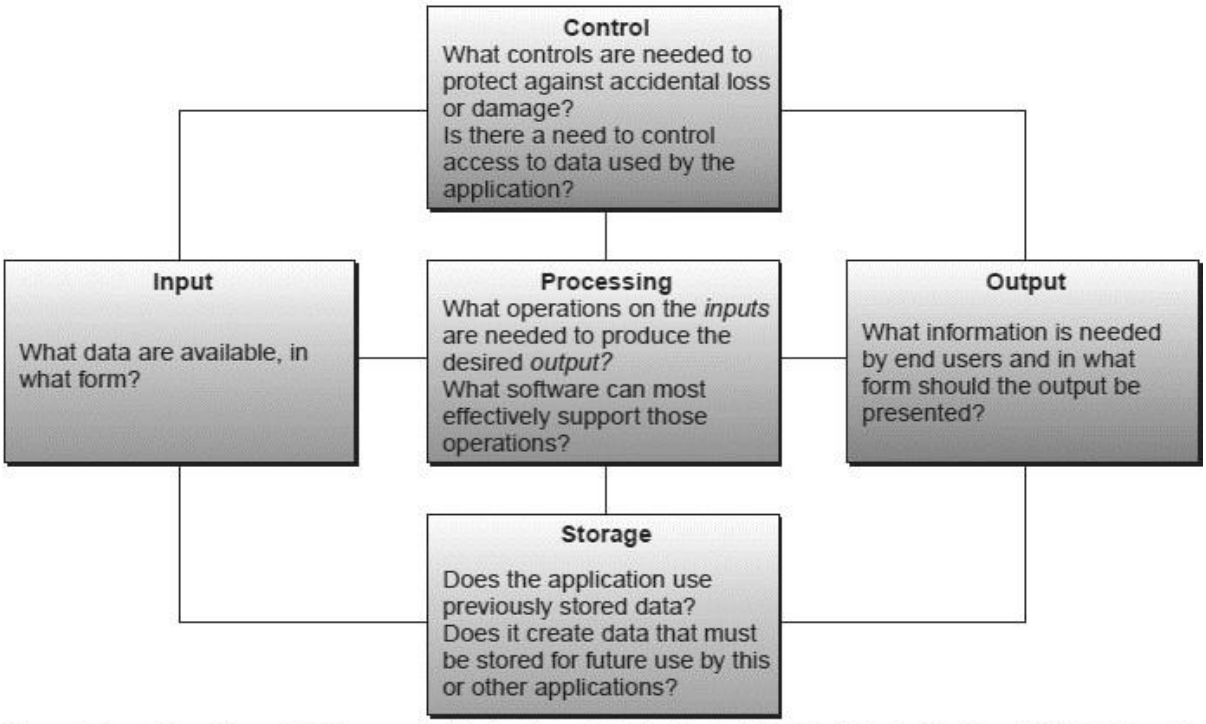
In a traditional systems development cycle, your role as a business end user is similar to that of a customer or a client. Typically, you make a request for a new or improved system, answer questions about your specific information needs and information processing problems, and provide background information on your existing business systems. IS professionals work with you to analyze your problem and suggest alternative solutions. When you approve the best alternative, it is designed and implemented. In end-user development, however, IS professionals play a consulting role while you do your own application development.

Focus on IS Activities

It is important to remember that end-user development should focus on the fundamental activities of any information system: input, processing, output, storage, and control.

When analyzing a potential application, you should first focus on the output to be produced by the application. What information is needed and in what form should it be presented? Next, look at the input data to be supplied to the application. What data are available? From what sources? In what form? Then you should examine the processing requirements. What operations or transformation processes will be required to convert the available inputs into the desired output? Among software packages the developer is able to use, which package can best perform the operations required?

FIGURE 12.14 End-user development should focus on the basic information processing activity components of an information system.



Source: Adapted from James N. Morgan, *Application Cases in MIS*, 4th ed. (New York: Irwin/McGraw-Hill, 2002), p. 31.

Doing End-User Development

In end-user development, you and other business professionals can develop new or improved ways to perform your jobs without the direct involvement of IS specialists. The application development capabilities built into a variety of end-user software packages have made it easier for many users to develop their own computer-based solutions.

Technical Note: Overview of Object-Oriented Analysis and Design

As stated at the beginning of the chapter, there are two common approaches to analysis and design: SDLC and object-oriented. Whereas the SDLC remains the predominant approach to software development, the object-oriented approach is gaining favor, particularly among programmers focusing on complex systems that require handling a wide variety of complex data structures, such as audio, video, images, documents, Web pages, and other types of data. An **object-oriented system** is composed of objects. An object can be anything a programmer wants to manage or manipulate—cars, people, animals, savings accounts, food products, business units, organizations, customers—literally anything. Once an object is defined by a programmer, its characteristics can be used to allow one object to interact with another object or pass information to another object. The behavior of an object-oriented system entails collaboration between these objects, and the state of the system is the combined state of all the object in it. Collaboration between objects requires them to send messages or information to one another.

The three areas of interest to us in an object-oriented system are object-oriented programming, object-oriented analysis and object-oriented design.

Object-oriented programming (OOP) is the programming paradigm that uses “objects” to design applications and computer programs. It employs several techniques from previously established paradigms, including: **Inheritance, Modularity, Polymorphism & Encapsulation.**

Object-oriented analysis (OOA) aims to model the problem domain, that is, the problem we want to solve, by developing an object oriented (OO) system.

Object-oriented design (OOD) describes the activity when designers look for logical solutions to solve a problem using objects. Object-oriented design takes the conceptual model that results from the object-oriented analysis and adds implementation constraints imposed by the environment, the programming

language, and the chosen tools, as well as architectural assumptions chosen as the basis of the design.

B. Implementing Business Systems

Implementing Business Systems

The systems implementation stage involves hardware and software acquisition, software development, testing of programs and procedures, conversion of data resources, and a variety of conversion alternatives. It also involves the education and training of end users and specialists who will operate a new system. Implementation can be a difficult and time- consuming process; however, it is vital in ensuring the success of any newly developed system. Even a well-designed system will fail if it is not properly implemented, which is why the implementation process typically requires a **project management** effort on the part of IT and business unit managers. They must enforce a project plan, which includes job responsibilities, timetables for major stages of development, and financial budgets. This is necessary if a project is to be completed on time and within its established budget, while still meeting its design objectives.

FIGURE 12.18 An overview of the implementation process. Implementation activities are needed to transform a newly developed information system into an operational system for end users.

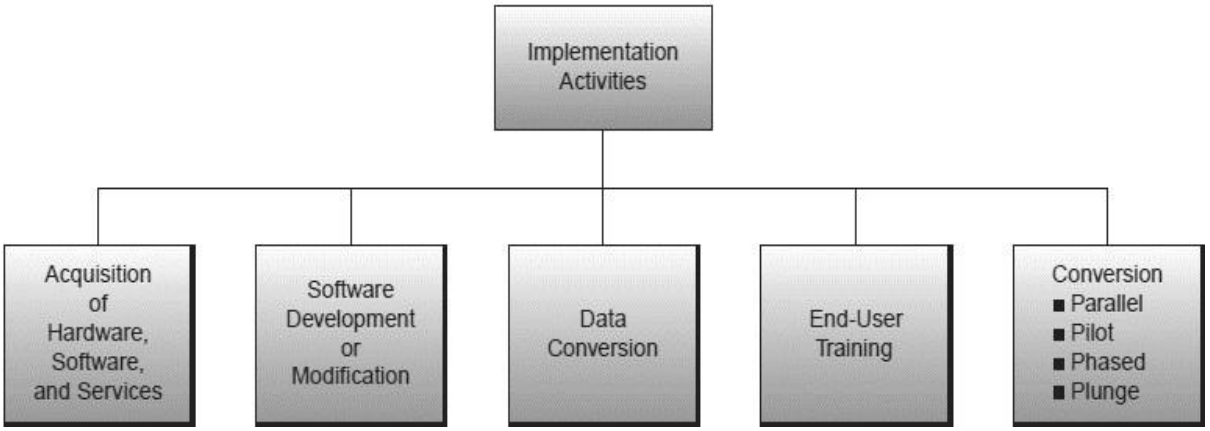
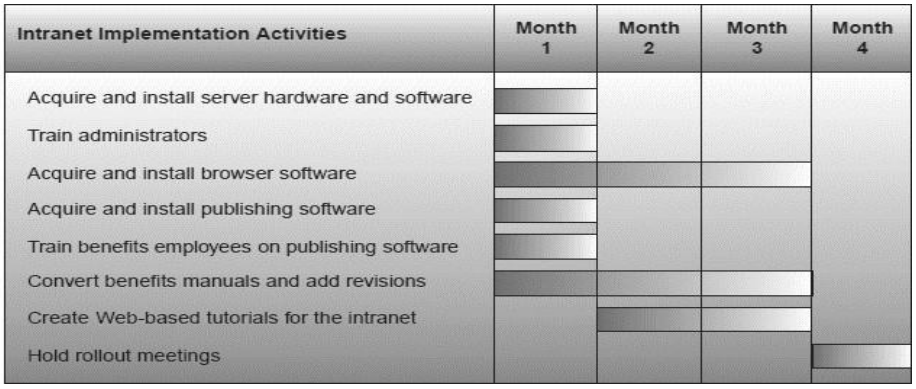


FIGURE 12.19 An example of the implementation process activities and timetables for a company installing an intranet-based employee benefits system in its human resource management department.



Project Management

Any discussion of information systems design and development would be incomplete without including a discussion of basic project management concepts, techniques, and tools. Before we progress any further in our discussion of implementation, we need to understand how our project, which we hope is on time and within budget, got to this point.

What Is a Project?

A **project** is a special set of activities with a clear beginning and end. Every project has a set of goals, objectives and tasks. Every project must also deal with a set of limitations or constraints. No matter what the project, three elements will be necessary to manage it effectively and efficiently: process, tools, and techniques.

The Process of Project Management

Initiating and Defining

The first phase of the project management process serves as a foundation for all that follows. The most important objective to achieve during this phase is the clear and succinct statement of the problem that the project is to solve or the goals that the project is to achieve. Also during this phase, it is necessary to identify and secure the resources necessary to execute the project, explore the costs and benefits, and identify any risks.

Planning

The next phase in the project management process involves planning the project. Here every project objective and every activity associated with that objective must be identified and sequenced. Several tools have been created to assist in the sequencing of these activities including simple dependence diagrams, program evaluation and review (PERT), critical path method (CPM), and a commonly used timeline diagram known as a Gantt chart. These same tools also help the project manager determine how long each activity will take and, thus, how long the project will take. Later in the project process, the tools will help determine whether the project is on schedule and, if not, where the delays occurred and what can be done to remedy the delay.

FIGURE 12.20
The five phases of project management.

Project Management Phase	Example Activities
Initiating/Defining	• State the problem(s)/goal(s). • Identify the objectives. • Secure resources. • Explore costs/benefits in feasibility study.
Planning	• Identify and sequence activities. • Identify the "critical path." • Estimate time and resources needed for completion. • Write a detailed project plan.
Executing	• Commit resources to specific tasks. • Add additional resources/personnel if necessary. • Initiate project work.
Controlling	• Establish reporting obligations. • Create reporting tools. • Compare actual progress with baseline. • Initiate control interventions if necessary.
Closing	• Install all deliverables. • Finalize all obligations/commitments. • Meet with stakeholders. • Release project resources. • Document the project. • Issue final report.

Executing

Once all of the activities in the planning phase are complete and all detailed plans have been created and approved, the execution phase of the project can begin. It is here that all of the plans are put into motion. Resources, tasks, and schedules are brought together, and the necessary work teams are created and set forth on their assigned paths.

Controlling

Some project management experts suggest that controlling is just an integral part of the execution phase of project management; others suggest it must be viewed as a separate set of activities that, admittedly, occur simultaneous to the execution phase. In either case, it is important to give sufficient attention to the controlling activities to ensure that the project objectives and deadlines are met.
Probably the single most important tool for project control is the report. Three common types of reports are generated to assist with project control. Variance report, status report & resource allocation report.

Closing

This last phase of the project management process focuses on bringing a project to a successful end. The beginning of the end of a project is the implementation and installation of all of the project deliverables. The next step is the formal release of the project resources so they can be redeployed into other projects or job roles. The final step in this phase is to review the final documentation and publish the final project report. This is where the good and bad news concerning the project are documented, and the elements necessary for a post project review are identified.

Evaluating Hardware, Software, and Services

Large companies may require suppliers to present bids and proposals based on system specifications developed during the design stage of systems development. Minimum acceptable physical and performance characteristics for all hardware and software requirements are established. Most large business firms and all government agencies formalize these requirements by listing them in a document called an RFP (request for proposal) or RFQ (request for quotation). Then they send the RFP or RFQ to appropriate vendors, who use it as the basis for preparing a proposed purchase agreement. Companies may use a scoring system of evaluation when there are several competing proposals for a hardware or software acquisition. They give each **evaluation factor** a certain number of maximum possible points. Then they assign each competing proposal points for each factor, depending on how well it meets the user's specifications. Scoring evaluation factors for several proposals helps organize and document the evaluation process. It also spotlights the strengths and weaknesses of each proposal.

Hardware Evaluation Factors

When you evaluate the hardware needed by a new business application, you should investigate specific physical and performance characteristics for each computer system or peripheral component to be acquired. Specific questions must be answered concerning many important factors.

FIGURE 12.22
A summary of 10 major hardware evaluation factors. Notice how you can use this to evaluate a computer system or a peripheral device.

Hardware Evaluation Factors	Rating
Performance What is its speed, capacity, and throughput?	
Cost What is its lease or purchase price? What will be its cost of operation and maintenance?	
Reliability What are the risk of malfunction and its maintenance requirements? What are its error control and diagnostic features?	
Compatibility Is it compatible with existing hardware and software? Is it compatible with hardware and software provided by competing suppliers?	
Technology In what year of its product life cycle is it? Does it use a new untested technology, or does it run the risk of obsolescence?	
Ergonomics Has it been "human factors engineered" with the user in mind? Is it user-friendly, designed to be safe, comfortable, and easy to use?	
Connectivity Can it be easily connected to wide area and local area networks that use different types of network technologies and bandwidth alternatives?	
Scalability Can it handle the processing demands of a wide range of end users, transactions, queries, and other information processing requirements?	
Software Are system and application software available that can best use this hardware?	
Support Are the services required to support and maintain it available?	
Overall Rating	

Software Evaluation Factors

You should evaluate software according to many factors that are similar to those used for hardware evaluation. Thus, the factors of performance, cost, reliability, availability, compatibility, modularity, technology, ergonomics, and support should be used to evaluate proposed software acquisitions.

FIGURE 12.23
A summary of selected software evaluation factors. Note that most of the hardware evaluation factors in Figure 12.22 can also be used to evaluate software packages.

Software Evaluation Factors	Rating
Quality Is it bug-free, or does it have many errors in its program code?	
Efficiency Is the software a well-developed system of program code that does not use much CPU time, memory capacity, or disk space?	
Flexibility Can it handle our business processes easily, without major modification?	
Security Does it provide control procedures for errors, malfunctions, and improper use?	
Connectivity Is it *Web-enabled* so it can easily access the Internet, intranets, and extranets, on its own, or by working with Web browsers or other network software?	
Maintenance Will new features and bug fixes be easily implemented by our own software developers?	
Documentation Is the software well documented? Does it include help screens and helpful software agents?	
Hardware Does existing hardware have the features required to best use this software?	
Other Factors What are its performance, cost, reliability, availability, compatibility, modularity, technology, ergonomics, scalability, and support characteristics? (Use the hardware evaluation factor questions in Figure 12.22.)	
Overall Rating	

Evaluating IS Services

Most suppliers of hardware and software products and many other firms offer a variety of **IS services** to end users and organizations. Examples include assistance in developing a company Web site; installation or conversion of new hardware and software; employee training; and hardware maintenance. Some of these services are provided without cost by hardware manufacturers and software suppliers.

FIGURE 12.24
Evaluation factors for IS services. These factors focus on the quality of support services business users may need.

Evaluation Factors for IS Services	Rating
Performance What has been their past performance in view of their past promises?	
Systems Development Are Web site and other e-business developers available? What are their quality and cost?	
Maintenance Is equipment maintenance provided? What are its quality and cost?	
Conversion What systems development and installation services will they provide during the conversion period?	
Training Is the necessary training of personnel provided? What are its quality and cost?	
Backup Are similar computer facilities available nearby for emergency backup purposes?	
Accessibility Does the vendor provide local or regional sites that offer sales, systems development, and hardware maintenance services? Is a customer support center at the vendor's Web site available? Is a customer hotline provided?	
Business Position Is the vendor financially strong, with good industry market prospects?	
Hardware Do they provide a wide selection of compatible hardware devices and accessories?	
Software Do they offer a variety of useful e-business software and application packages?	
Overall Rating	

FIGURE 12.21
Examples from the IBM Corporation of the kinds of hardware, software, and IS services that many companies are evaluating and acquiring to support their e-commerce initiatives.

Hardware
Full range of offerings, including xSeries servers, iSeries midrange servers for small and midsize businesses, RS/6000 servers for UNIX customers, and z900 mainframes for large enterprises. Also has full range of storage options.
Software
Web server: Lotus DominoGo Web server.
Storefront: WebSphere Commerce Suite (formerly known as Net.Commerce) for storefront and catalog creation, relationship marketing, and order management. Can add Commerce Integrator to integrate with back-end systems and Catalog Architect for content management.
Middleware/transaction services: WebSphere application server manages transactions. MQ Series queues messages and manages connections. CICS processes transactions.
Database: DB2 Universal Database.
Tools: WebSphere Studio includes set of predefined templates and common business logic.
Other applications include: IBM Payment Suite for handling credit cards and managing digital certificates.
Services
IBM Global Services, which includes groups organized by each major industry, including retail and financial. Can design, build, and host e-commerce applications.

Other Implementation Activities

Testing, data conversion, documentation, and training are keys to successful implementation of a new business system.

Testing

System testing may involve testing and debugging software, testing Web site performance, and testing new hardware. An important part of testing is the review of prototypes of displays, reports, and other output.

Data Conversion

Implementing new information systems for many organizations today frequently involves replacing a previous system and its software and databases. One of the most important implementation activities required when installing new software in such cases is called data conversion. For example, installing new software packages may require converting the data elements in databases that are affected by a new application into new data formats. Other data conversion activities that are typically required include correcting incorrect data, filtering out unwanted data, consolidating data from several databases, and organizing data into new data subsets, such as databases, data marts, and data warehouses. A good data conversion process is essential because improperly organized and formatted data are frequently reported to be one of the major causes of failures in implementing new systems. During the design phase, the analysts created a data dictionary that not only describes the various data elements contained in the new system but also specifies any necessary conversions from the old system. In some cases, only the name of the data element is changed, as in the old system field CUST_ID becoming CLIENT_ID in the new system.

Documentation

Developing good user documentation is an important part of the implementation process. Sample data entry display screens, forms, and reports are good examples of documentation. When computer-aided systems engineering methods are used, documentation can be created and changed easily because it is stored and accessible on disk in a system repository. Documentation serves as a method of communication among the people responsible for developing, implementing, and maintaining a computer-based system.

Training

Training is a vital implementation activity. IS personnel, such as user consultants, must be sure that end users are trained to operate a new business system or its implementation will fail. Training may involve only activities like data entry, or it may also involve all aspects of the proper use of a new system. In addition, managers and end users must be educated in how the new technology affects the company's business operations and management. This knowledge should be supplemented by training programs for any new hardware devices, software packages, and their use for specific work activities.

System Conversion Strategies

The initial operation of a new business system can be a difficult task. This typically requires a conversion process from the use of a present system to the operation of a new or improved application. Conversion methods can soften the impact of introducing new information technologies into an organization. Four major forms of system conversion are illustrated:

Direct Conversion

The simplest conversion strategy, and probably the most disruptive to the organization, is the **direct cutover** approach. This method, sometimes referred to as the **slam dunk** or **cold-turkey strategy,** is as abrupt as its name implies. Using this approach, the old system is just turned off, and the new system is turned on in its place. Although this method is the least expensive of all available strategies and may be the only viable solution in situations where activating the new system is an emergency or when the two systems cannot coexist under any conditions, it is also the one that poses the greatest risk of failure. Direct conversion should be considered only in extreme circumstances where no other conversion strategy is viable.

Parallel Conversion

At the opposite end of the risk spectrum is the **parallel conversion** strategy. Here, the old and new systems are run simultaneously until the end users and project coordinators are fully satisfied that the new system is functioning correctly and the old system is no longer necessary. Using this approach, a parallel conversion can be effected with either a **single cutover,** where a predetermined date for stopping the parallel operation is set, or a **phased cutover,** where some predetermined method of phasing in each piece of the new system and turning off a similar piece of the old system is employed.

Although clearly having the advantage of low risk, the parallel approach also brings with it the highest cost. To execute a parallel approach properly, the end users must literally perform all daily functions with both systems, thus creating a massive redundancy in activities and literally double the work.

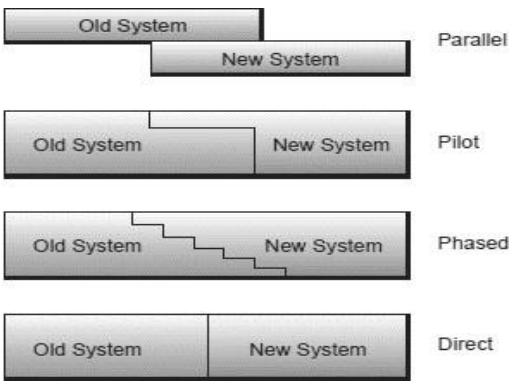
Pilot Conversion

In some situations, the new system may be installed in multiple locations, such as a series of bank branches or retail outlets. In other cases, the conversion may be able to be planned from a geographic perspective. When these types of scenarios exist, the possibility of using a **pilot conversion** strategy exists. This approach allows for the conversion to the new system, using either a direct or parallel method, at a single location. The advantage to this approach is that a location can be selected that best represents the conditions across the organization but also may be less risky in terms of any loss of time or delays in processing. Once the installation is complete at the pilot site, the process can be evaluated and any changes to the system made to prevent problems encountered at the pilot site from reoccurring at the remaining installations. This approach may also be required if the individual sites or locations have certain unique characteristics or idiosyncrasies making either a direct or parallel approach infeasible.

Phased Conversion

A **phased** or **gradual conversion** strategy attempts to take advantage of the best features of both the direct and parallel approaches, while minimizing the risks involved. This incremental approach to conversion allows for the new system to be brought online as a series of functional components that are logically ordered to minimize disruption to the end users and the flow of business. Phased conversion is analogous to the release of multiple versions of an application by a software developer. Each version of the software should correct any known bugs and should allow for 100 percent compatibility with data entered into or processed by the previous version. Although it has the advantage of lower risk, the phased approach takes the most time and, thus, creates the most disruption to the organization over time.

FIGURE 12.26
The four major forms of conversion to a new system.



Post-implementation Activities

When all is said and done, the single most costly activity occurs after the system implementation is complete: the **post-implementation maintenance phase.** The primary objectives associated with systems maintenance are to correct errors or faults in the system, provide changes to effect performance improvement, or adapt the system to changes in the operating or business environment. In a typical organization, more programmers and analysts are assigned to application maintenance activities than to application development. Further, although a new system can take several months or years to design and build and can cost hundreds of thousands or millions of dollars, the resulting system can operate around the clock and last for 5 to 10 years, or longer. One major activity in post-implementation involves making changes to the system after the users have finally had an opportunity to use it. These are called **change requests.** Such requests can range from fixing a software bug not found during testing to designing an enhancement to an existing process or function.

Systems Maintenance

Managing and implementing change requests is only one aspect of the systems maintenance phase activities. In some ways, once the maintenance phase begins, the life cycle starts over again. New requirements are articulated, analyzed, designed, checked for feasibility, tested, and implemented. Although the range and nature of specific maintenance requests vary from system to system, four basic categories of maintenance can be identified: (1) corrective, (2) adaptive, (3) perfective, and (4) preventive. The activities associated with **corrective maintenance** are focused on fixing bugs and logic errors not detected during the implementation testing period. **Adaptive maintenance** refers to those activities associated with modifying existing functions or adding new functionality to accommodate changes in the business or operating environments. **Perfective maintenance** activities involve changes made to an existing system that are intended to improve the performance of a function or interface. The final category of maintenance activities, **preventive maintenance,** involves those activities intended to reduce the chances of a system failure or extend the capacity of a current system's useful life. Although often the lowest-priority maintenance activity, preventive maintenance is, nonetheless, a high-value-adding function and is vital to an organization realizing the full value of its investment in the system.

Post-implementation Review

The maintenance activity also includes a post-implementation review process to ensure that newly implemented systems meet the business objectives established for them. Errors in the development or use of a system must be corrected by the maintenance process. This includes a periodic review or audit of a system to ensure that it is operating properly and meeting its objectives. This audit is in addition to continually monitoring a new system for potential problems or necessary changes.

FIGURE 12.27
An overview of the implementation process. Implementation activities are needed to transform a newly developed information system into an operational system for end users.

Implementing New Systems
• **Acquisition** Evaluate and acquire necessary hardware and software resources and information system services. Screen vendor proposals.
• **Software Development** Develop any software that will not be acquired externally as software packages. Make any necessary modifications to software packages that are acquired.
• **Data Conversion** Convert data in company databases to new data formats and subsets required by newly installed software.
• **Training** Educate and train management, end users, customers, and other business stakeholders. Use consultants or training programs to develop user competencies.
• **Testing** Test and make necessary corrections to the programs, procedures, and hardware used by a new system.
• **Documentation** Record and communicate detailed system specifications, including procedures for end users and IS personnel and examples of input screens and output displays and reports.
• **Conversion** Convert from the use of a present system to the operation of a new or improved system. This may involve operating both new and old systems in *parallel* for a trial period, operation of a *pilot* system on a trial basis at one location, *phasing* in the new system one location at a time, or a *direct cutover* to the new system.

CHAPTER # 06: INFORMATION SYSTEMS AUDITING

A. Management of the IS Audit Function

1.2.1 ORGANIZATION OF THE IS AUDIT FUNCTION

1.2.2 IS AUDIT RESOURCE MANAGEMENT

IS technology is constantly changing. Therefore, it is important that IS auditors maintain their competency through updates of existing skills and obtain training directed toward new audit techniques and technological areas. ISACA IS Auditing Standards require that the IS auditor be technically competent (S4 Professional Competence), having the skills and knowledge necessary to perform the auditor's work. Further, the IS auditor is to maintain technical competence through appropriate continuing professional education. Skills and knowledge should be taken into consideration when planning audits and assigning staff to specific audit assignments.

Preferably, a detailed staff training plan should be drawn for the year based on the organization's direction in terms of technology and related risk issues that need to be addressed. This should be reviewed periodically to ensure that the training needs are aligned to the direction that the audit organization is taking. Additionally, IS audit management should also provide the necessary IT resources to properly perform IS audits of a highly specialized nature (e.g., tools, methodology, work programs).

1.2.3 AUDIT PLANNING

Annual Planning

Audit planning consists of both short- and long-term planning. Short-term planning takes into account audit issues that will be covered during the year, whereas long-term planning relates to audit plans that will take into account risk-related issues regarding changes m the organization's IT strategic direction that will affect the organization's IT environment.

All of the relevant processes that represent the blueprint of the entity’s business should be included in the audit universe. The audit universe ideally lists all of the processes that may be considered for audit.

Evaluation of the risk factors should be based on objective criteria, although subjectivity cannot be completely avoided. For example, in respect to reputation factor, the criteria based on which inputs can be solicited from the business may be rated as:

- High- A process issue may result in damage to the reputation of the entity that will take more than six months to recover;
- Medium- A process issue may result in damage to the reputation of the entity that will take less than six months but more than three months to recover;
- Low- A process issue may result in damage to the reputation of the entity that will take less than three months to recover.

Analysis of short- and long-term issues should occur at least annually. This is necessary to take into account new control issues; changes in the risk environment, technologies and business processes; and enhanced evaluation techniques.

Individual Audit Assignments

In addition to overall annual planning, each individual audit assignment must be adequately planned. The IS auditor should understand that other considerations, such as the results of periodic risk assessments, changes in the application of technology, and evolving privacy issues and regulatory requirements, may impact the overall approach to the audit.

When planning an audit, the IS auditor must have an understanding of the overall environment under review. This should include a general understanding of the various business practices and functions relating to the audit subject, as well as the types of information systems and technology supporting the activity. For example, the IS auditor should be familiar with the regulatory environment in which the business operates.

To perform audit planning, the IS auditor should perform the steps indicated

Exhibit 1.2 –Steps to Perform Audit Planning

- Gain an understanding of the business's mission, objectives, purpose and processes, which include information and processing requirements such as availability, integrity, security and business technology, and information confidentiality.
- Identify stated contents such as policies, standards and required guidelines, procedures and organization structure.
- Perform a risk analysis to help in designing the audit plan.
- Set the audit scope and audit objectives.
- Develop the audit approach or audit strategy.
- Assign personnel resources to the audit.
- Address engagement logistics.

ISACA IS Auditing Standards require the IS auditor to plan the IS audit work to address the audit objectives and comply with applicable professional auditing standards (S5 Planning).

Steps an IS auditor could take to gain an understanding of the business include:

- Reading background material including industry publications, annual reports and independent financial analysis reports
- Reviewing prior audit reports or IT-related reports (from external or internal audits, or specific reviews such as regulatory reviews)
- Reviewing business and IT long-term strategic plans
- Interviewing key managers to understand business issues
- Identifying specific regulations applicable to IT
- Identifying IT functions or related activities that have been outsourced
- Touring key organization facilities

1.2.4 EFFECT OF LAWS AND REGULATIONS ON IS AUDIT PLANNING

Each organization, regardless of its size or the industry within which it operates, will need to comply with a number of governmental and external requirements related to computer system practices and controls and to the manner in which computers, programs and data are stored and used. Additionally, business regulations can impact the way data are processed transmitted and stored (stock exchange, central banks, etc.)

Special attention should be given to these issues in those industries that, historically, have been closely regulated.

The contents of these legal regulations regard:

- Establishment of the regulatory requirements
- Organization of the regulatory requirements
- Responsibilities assigned to the corresponding entities
- Correlation to financial, operational and IT audit functions

A similar example is the Basel II Accord which regulates the minimum amount of capital for financial organizations based on the level of risk faced by these organizations. The Basel II Committee on Banking Supervision recommends conditions that should be fulfilled, in addition to capital requirements, to manage risk exposures. These conditions will ideally result in an improvement of:

- Credit risk
- Operational risk

- Market risk

The following are steps an IS auditor would perform to determine an organization's level of compliance with external requirements:

- Identify those government or other relevant external requirements dealing with:
  - Electronic data, personal data, copyrights, e-commerce, e-signatures, etc.
  - Computer system practices and controls
  - The manner in which computers, programs and data are stored
  - The organization or the activities of information technology services
  - -IS audits
- Document applicable laws and regulations.
- Assess whether the management of the organization and the IS function have considered the relevant external requirements in making plans and in setting policies, standards and procedures, as well as business application features.
- Review internal IS department/function/activity documents that address adherence to laws applicable to the industry.
- Determine adherence to established procedures that address these requirements.
- Determine if there are procedures in place to ensure contracts or agreements with external IT services providers reflect any legal requirements related to responsibilities.

B. ISACA IS Audit and Assurance Standards and Guidelines

1.3 ISACA AUDIT AND ASSURANCE STANDARDS AND GUIDELINES

1.3.1 ISACA CODE OF PROFESSIONAL ETHICS

Members and ISACA certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.
3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities that they can reasonably expect to complete with professional competence.
6. Inform appropriate parties of the results of work performed, revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding ofIS security and control.

1.3.2 ISACA IS AUDIT AND ASSURANCE STANDARDS

Standards contain statements of mandatory requirements for IS audit and assurance. The inform:

- IS audit and assurance professional of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
- Management and other interested parties of the profession’s expectations concerning the work of practitioners;
- Holders of the Certified Information Systems Auditor (CISA) designation of their requirements. Failure to comply with these standards may result in an investigation into the ISA holder’s conduct by the ISACA Board of Directors or appropriate ISACA group and ultimately in disciplinary action.

The framework for the ISACA IS Auditing Standards provides for multiple levels as follows:

- Standards define mandatory requirements for IS auditing and reporting.
- Guidelines provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the above standards, use professional judgment in their application and be prepared to justify any difference.
- Tools and techniques provide examples of processes an IS auditor might follow in an audit engagement. The tools and techniques documents provide information on how to meet the standards when completing IS auditing work, but do not set requirements.

There are three categories of standards and guidelines- general, performance and reporting.

- **General:** The guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments, and deal with the IS audit and assurance professional ethics, independence, objectivity and due care as well as knowledge, competency and skill.
- **Performance:** Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilization, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgment and due care.
- **Reporting:** Address the types of reports, means of communication and the information communicated.

1.3.3 ISACA IS AUDIT AND ASSURANCE GUIDELINES

The objective of the ISACA IS Auditing Guidelines is to provide further information on how to comply with the ISACA IS Auditing Standards. The IS auditor should:

- Consider them in determining how to implement the above standards.
- Use professional judgment in applying them.
- Be able to justify any difference.

1.3.4 ISACA IS AUDIT AND ASSURANCE TOOLS AND TECHNIQUES

Tools and techniques developed by ISACA provide examples of possible processes an IS auditor may follow in an audit engagement. In determining the appropriateness of any specific tool and technique, IS auditors should apply their own professional judgment to the specific circumstances. The tools and techniques documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements.

Tools and techniques are currently categorized into:

- White papers;
- Audit/Assurance programs;
- COBIT 5 family of products;
- Technical and Risk Management Reference series;
- ISACA Journal IT audit basics column.

1.3.5 RELATIONSHIP AMONG STANDARDS, GUIDELINES, AND TOOLS AND TECHNIQUES

Standards defined by ISACA are to be followed by the IS auditor Guidelines provide assistance on how the auditor can implement standards in various audit assignments. Tools and techniques are not intended to provide exhaustive guidance to the auditor when performing an audit. Tools and techniques provide examples of steps the auditor may follow in specific audit assignments to implement the standards; however, the IS auditor should use professional judgment when using guidelines and tools and techniques.

There may be situations in which the legal/regulatory requirements are more stringent than the requirements contained in ISACA IS Audit and Assurance Standards. In such cases, the IS auditor should ensure compliance with the more stringent legal/regulatory requirements.

1.3.6 INFORMATION TECHNOLOGY ASSURANCE FRAMEWORK (ITAFTM)

The Information Technology Assurance Framework (ITAF™) is a comprehensive and good-practice-setting model that:

- Establishes standards that address IT audit and assurance professional roles and responsibilities, knowledge and skills, and diligence, conduct and reporting requirements
- Defines terms and concepts specific to IT assurance
- Provides guidance on the design, conduct and reporting of IT audit and assurance assignments

ITAF is focused on ISACA material and provides a single source through which IS an audit and assurance professional can seek guidance, research policies and procedures, obtain audit and assurance programs, and develop effective reports.

C. IS Controls

1.4 IS CONTROLS

In order for information systems to fully realize the benefits and risk and resource optimization goals, risk that could prevent or inhibit obtaining these goals needs to be addressed. Organizations design, develop, implement and monitor information systems through policies, procedures, practices and organizational

structures to address these types of risk. The internal control life cycle is dynamic in nature and designed to provide reasonable assurance that business goals and objectives will be achieved and undesired events will be prevented or detected and corrected.

1.4.1 RISK ANALYSIS

Risk analysis is part of audit planning, and helps identify risks and vulnerabilities so the IS auditor can determine the controls needed to mitigate those risks.

In evaluating IT-related business processes applied by an organization, understanding the relationship between risk and control is important for IS audit and control professionals. IS auditors must be able to identify and differentiate risk types and the controls used to mitigate these risks. They must have knowledge of common business risks, related technology risks and relevant controls. They must also be able to evaluate the risk assessment and management techniques used by business managers, and to make assessments of risk to help focus and plan audit work. In addition to an understanding of business risk and control, IS auditors must understand that risk exists within the audit process.

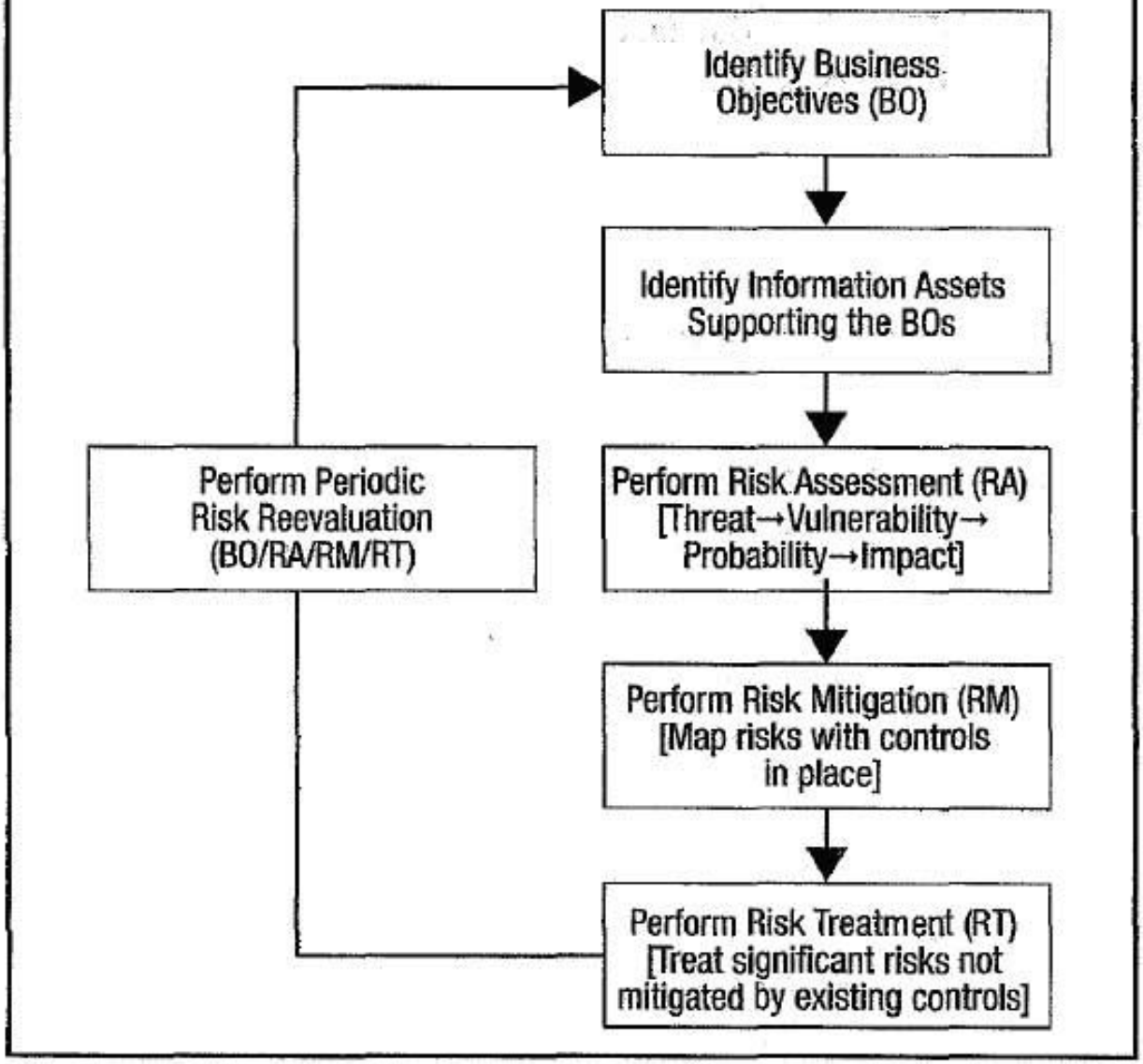
In analyzing the business risk arising from the use of IT, it is important for the IS auditor to have a clear understanding of:

- Industry and or internationally accepted risk management processes
- The purpose and nature of business, the environment in which the business operates and related business risk
- The dependence on technology to process and deliver business information
- The business risk of using IT and how it impacts the achievement of the business goals and objectives
- A good overview of the business processes and the impact of IT and related risk on the business process objectives.

The assessment of countermeasures should be performed through a cost-benefit analysis where controls to mitigate risks are selected to reduce risks to a level acceptable to management. This analysis process may be based on any ofthe following:

- The cost of the control compared to the benefit of minimizing the risk
- Management's appetite for risk (i.e., the level of residual risk that management is prepared to accept)
- Preferred risk-reduction methods (e.g., terminate the risk, minimize probability of occurrence, minimize impact, transfer the risk via insurance)

Exhibit 1.3 –Summary of Risk Assessment Process



From the IS auditor's perspective risk analysis serves more than one purpose:

- It assists the IS auditor in identifying risk and threats to an IT environment and IS system-risk and threats that would need to be addressed by management- and in identifying system-specific internal controls. Depending on the level of risk, this assists the IS auditor in selecting certain areas to examine;
- It helps the IS auditor in his/her evaluation of controls in audit planning;
- It assists the IS auditor in determining audit objectives;
- It supports risk-based audit decision making.

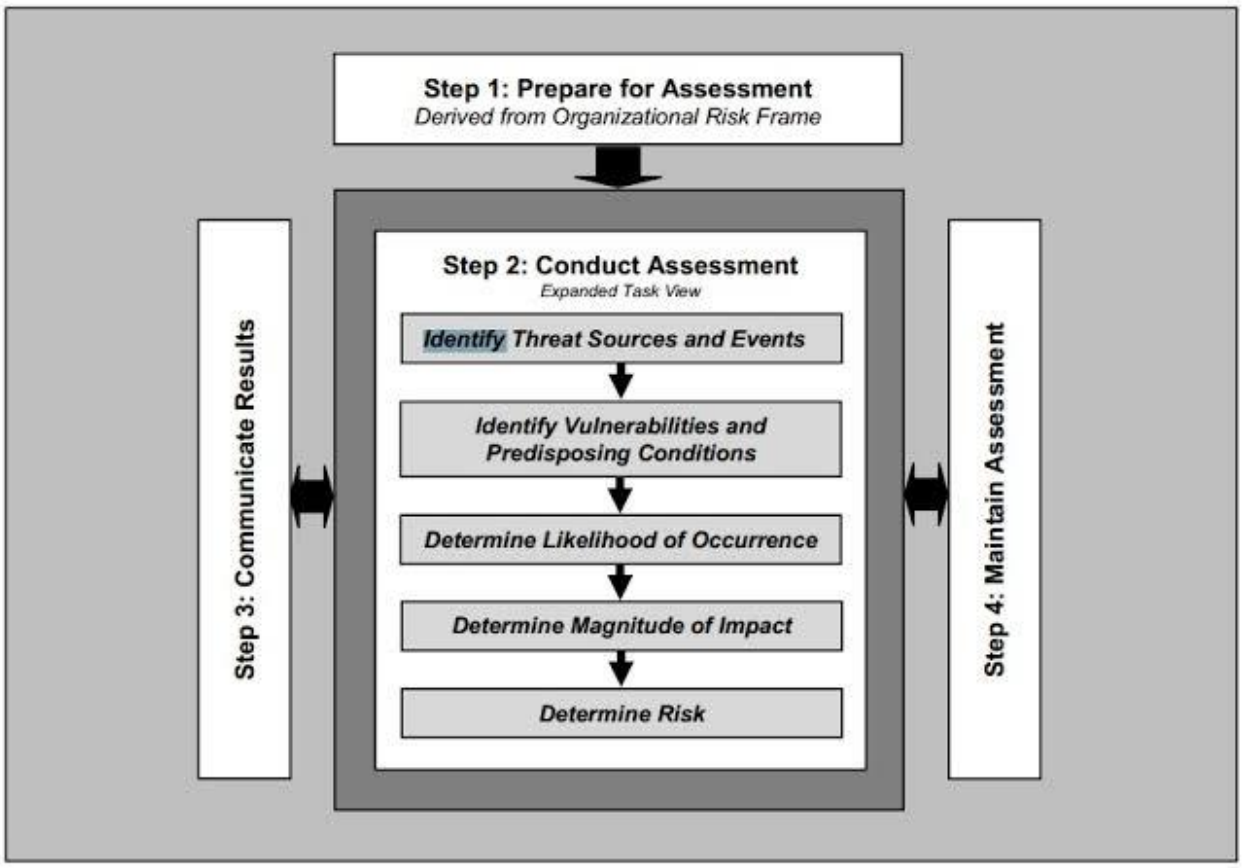


FIGURE 5: RISK ASSESSMENT PROCESS

1.4.2 INTERNAL CONTROLS

Internal controls are normally composed of policies, procedures, practices and organizational structures which are implemented to reduce risks to the organization.

Internal controls are developed to provide reasonable assurance to management that the organization's business objectives will be achieved and risk events will be prevented, or detected and corrected.

There are two key aspects that controls should address: what should be achieved, and what should be avoided. Not only do internal controls address business/operational objectives, but they should also address undesired events through prevention, detection and correction.

Elements of controls that should be considered when evaluating control strength are classified as preventive, detective or corrective in nature.

Control Classifications		
Class	**Function**	**Examples**
Preventive	• Detect problems before they arise. • Monitor both operation and inputs. • Attempt to predict potential problems before they occur and make adjustments. • Prevent an error, omission or malicious act from occurring.	• Employ only qualified personnel. • Segregate duties (deterrent factor). • Control access to physical facilities. • Use well-designed documents (prevent errors). • Establish suitable procedures for authorization of transactions. • Complete programmed edit checks. • Use access control software that allows only authorized personnel to access sensitive files. • Use encryption software to prevent unauthorized disclosure of data.
Detective	• Use controls that detect and report the occurrence of an error, omission or malicious act.	• Hash totals • Check points in production jobs • Echo controls in telecommunications • Error messages over tape labels • Duplicate checking of calculations • Periodic performance reporting with variances • Past-due account reports • Internal audit functions • Review of activity logs to detect unauthorized access attempts
Corrective	• Minimize the impact of a threat. • Remedy problems discovered by detective controls. • Identify the cause of a problem. • Correct errors arising from a problem. • Modify the processing system(s) to minimize future occurrences of the problem.	• Contingency planning • Backup procedures • Rerun procedures

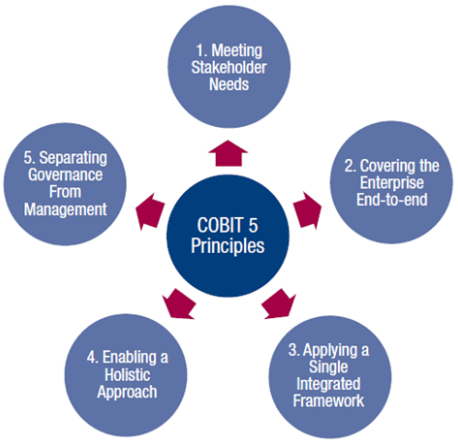
1.4.3 IS CONTROL OBJECTIVES

Specific IS control objectives may include:

- Safeguarding assets. Information on automated systems is secure from improper access and current.
- Ensuring integrity of general operating system (OS) environments, including network management and operations.
- Ensuring integrity of sensitive and critical application system environments, including accounting/financial and management
- information (information objectives) and customer data, through:
    - Authorization of the input. Each transaction is authorized and entered only once.
    - Validation of the input. Each input is validated and will not cause negative impact to the processing of transactions.
    - Accuracy and completeness of processing of transactions. All transactions are recorded and entered into the computer for the proper period.
    - Reliability of overall information processing activities
    - Accuracy, completeness and security of the output
    - Database integrity, availability and confidentiality
- Ensuring appropriate identification and authentication of users of IS resources (end users as well as infrastructure support).
- Ensuring the efficiency and effectiveness of operations (operational objectives).
- Complying with the users' requirements, organizational policies and procedures, and applicable laws and regulations (compliance objectives).
- Ensuring availability of IT services by developing efficient business continuity (BCP) and disaster recovery plans (DRP).
- Enhancing protection of data and systems by developing an incident response plan.
- Ensuring integrity and reliability of systems by implementing effective change management procedures.

1.4.4 COBIT 5

COBIT 5, developed by ISACA, provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT (GEIT). Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.



Principle 1: Meeting Stakeholder Needs: Enterprises exist to create value for their stakeholders, by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT.

Principle 2: Covering the Enterprise End-to-End: COBIT 5 integrates governance of enterprise IT into enterprise governance:

- It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the "IT function," but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.
- It considers all IT-related governance and management enablers to be enterprise-wide and end-to-end.

Principle 3: Applying a Single, Integrated Framework: There are many IT-related standards and good practices, each providing guidance on a subset of IT activities. COBIT 5 aligns with other relevant standards and frameworks at a high level, and thus can serve as the overarching framework for governance and management of enterprise IT. The COBIT 5 framework defines seven categories of enablers:

- Principles, Policies and Frameworks
- Processes
- Organizational Structures
- Culture, Ethics and Behavior
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

Principle 5: Separating Governance from Management: The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes. COBIT 5's view on this key distinction between governance and management is:

- **Governance:** Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.
- **Management:** Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

1.4.5 GENERAL CONTROLS

Controls include policies, procedures and practices (tasks and activities) established by management to provide reasonable assurance that specific objectives will be achieved. General controls apply to all areas of the organization including IT infrastructure and support services. General controls include:

- Internal accounting controls that are primarily directed at accounting operations-controls that concern the safeguarding of assets and reliability of financial records
- Operational controls that concern day-to-day operations, functions and activities, and ensure that the operation is meeting the business objectives

- Administrative controls that concern operational efficiency in a functional area and adherence to management policies (administrative controls support the operational controls specifically concerned with operating efficiency and adherence to organizational policies)
- Organizational security policies and procedures to ensure proper usage of information and technology assets
- Overall policies for the design and use of adequate documents and records (manual/automated) to help ensure proper recording of transactions-transactional audit trail
- Procedures and practices to ensure adequate safeguards over access to and use of assets and facilities
- Physical and logical security policies for all data centers and IT resources (e.g., servers and telecom infrastructure)

1.4.6 IS SPECIFIC CONTROLS

Each general control procedure can be translated into an IS-specific control procedure. A well-designed information system should have controls built in for all its sensitive or critical functions. For example, the general procedure to ensure that adequate safeguards over access to assets and facilities can be translated into an IS related set of control procedures, covering access safeguards over computer programs, data and computer equipment. The IS auditor should understand the basic control objectives that exist for all functions. IS control procedures include:

- Strategy and direction
- General organization and management
- Access to IT resources, including data and programs
- Systems development methodologies and change control
- Operations procedures
- Systems programming and technical support functions
- Quality assurance (QA) procedures
- Physical access controls
- Business continuity (BCP)/disaster recovery planning (DRP)
- Networks and communications
- Database administration
- Protection and detective mechanisms against internal and external attacks

D. Performing an IS Audit

1.5 PERFORMING AN IS AUDIT

Several steps are required. Adequate planning is a necessary first step in performing effective IS audits. To effectively use IS audit resources, audit organizations must assess the overall risks for the general and application areas and related services being audited, and then develop an audit program that consists of objectives and audit procedures to satisfy the audit objectives. The audit process requires the IS auditor to gather evidence, evaluate the strengths and weaknesses of controls based on the evidence gathered through audit tests, and prepare an audit report that presents those issues (areas of control weaknesses with recommendations for remediation) in an objective manner to management.

Audit management must ensure the availability of adequate audit resources and a schedule for performing the audits and, in the case of internal IS audit, for follow-up reviews on the status of corrective actions taken by management. The process of auditing includes defining the audit scope, formulating audit objectives, identifying audit criteria, performing audit procedures, reviewing and evaluating evidence, forming audit conclusions and opinions, and reporting to management after discussion with key process owners.

Project management techniques for managing and administering audit projects, whether automated or manual, include the following steps:

- **Plan the audit engagement-** Plan the audit considering project-specific risk.
- **Build the audit plan-** Chart out the necessary audit tasks across a time line, optimizing resource use. Make realistic estimates of the time requirements for each task with proper consideration given to the availability of the auditee.
- **Execute the plan-** Execute audit tasks against the plan.
- **Monitor project activity-** IS auditor's report their actual progress against planned audit steps to ensure challenges are managed proactively and the scope is completed within time and budget.

1.5.1 AUDIT OBJECTIVES

Audit objectives refer to the specific goals that must be accomplished by the audit. In contrast, a control objective refers to how an internal control should function. An audit generally incorporates several audit objectives.

Audit objectives often focus on substantiating that internal controls exist to minimize business risk and that they function as expected. These audit objectives include assuring compliance with legal and regulatory requirements as well as the confidentiality, integrity, reliability and availability of information and IT resources. Audit management may give the IS auditor a general control objective to review and evaluate when performing an audit.

A key element in planning an IS audit is to translate basic and wide-ranging audit objectives into specific IS audit objectives.

1.5.2 TYPES OF AUDITS

- **Compliance audits-** Compliance audits include specific tests of controls to demonstrate adherence to specific regulatory or industry standards.
- **Financial audits-**The purpose of a financial audit is to assess the correctness of an organization's financial statements. A financial audit will often involve detailed, substantive testing, although increasingly, auditors are placing more emphasis on a risk- and control-based audit approach. This kind of audit relates to financial information integrity and reliability.
- **Operational audits-** An operational audit is designed to evaluate the internal control structure in a given process or area. IS audits of application controls or logical security systems are some examples of operational audits.
- **Integrated audits-** An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess the overall objectives within an organization, related to financial information and assets' safeguarding, efficiency and compliance. An integrated audit can be performed by external or internal auditors and would include compliance tests of internal controls and substantive audit steps.
- **Administrative audits-**These are oriented to assess issues related to the efficiency of operational productivity within an organization.
- **IS audits-**This process collects and evaluates evidence to determine whether the information systems and related resources adequately safeguard assets, maintain data and system integrity and availability, provide relevant and reliable information, achieve organizational goals effectively, consume resources efficiently, and have, in effect, internal controls that provide reasonable assurance that business, operational and control objectives will be met and that undesired events will be prevented, or detected and corrected, in a timely manner.
- **Specialized audits-**Within the category of IS audits, there are a number of specialized reviews that examine areas such as services performed by third parties. Because businesses are becoming increasingly reliant on third-party service providers, it is important that internal controls be evaluated in these environments.
- **Forensic audits-**Forensic auditing has been defined as auditing specialized in discovering, disclosing and following up on frauds and crimes. The primary purpose of such a review is the development of evidence for review by law enforcement and judicial authorities. In recent years, the forensic professional has been called on to participate in investigations related to corporate fraud and cybercrime. In cases where computer resources may have been misused, further investigation is necessary to gather evidence for possible criminal activity that can then be reported to appropriate authorities. A computer forensic investigation includes the analysis of electronic devices such as computers, phones, personal digital assistants (PDAs), disks, switches, routers, hubs and other electronic equipment.

1.5.3 AUDIT METHODOLOGY

An audit methodology is a set of documented audit procedures designed to achieve planned audit objectives. Its components are a statement of scope, audit objectives and audit program.
The audit methodology should be set up and approved by audit management to achieve consistency in the audit approach. This methodology should be formalized and communicated to all audit staff.

Audit Phases	
Audit Phase	**Description**
Audit subject	• Identify the area to be audited.
Audit objective	• Identify the purpose of the audit. For example, an objective might be to determine whether program source code changes occur in a well-defined and controlled environment.
Audit scope	• Identify the specific systems, function or unit of the organization to be included in the review. For example, in the previous program changes example, the scope statement might limit the review to a single application system or to a limited period of time.
Preaudit planning	• Identify technical skills and resources needed. • Identify the sources of information for test or review such as functional flow charts, policies, standards, procedures and prior audit workpapers. • Identify locations or facilities to be audited.
Audit procedures and steps for data gathering	• Identify and select the audit approach to verify and test the controls. • Identify a list of individuals to interview. • Identify and obtain departmental policies, standards and guidelines for review. • Develop audit tools and methodology to test and verify control.
Procedures for evaluating the test or review results	Organization-specific
Procedures for communication with management	Organization-specific
Audit report preparation	• Identify follow-up review procedures. • Identify procedures to evaluate/test operational efficiency and effectiveness. • Identify procedures to test controls. • Review and evaluate the soundness of documents, policies and procedures.

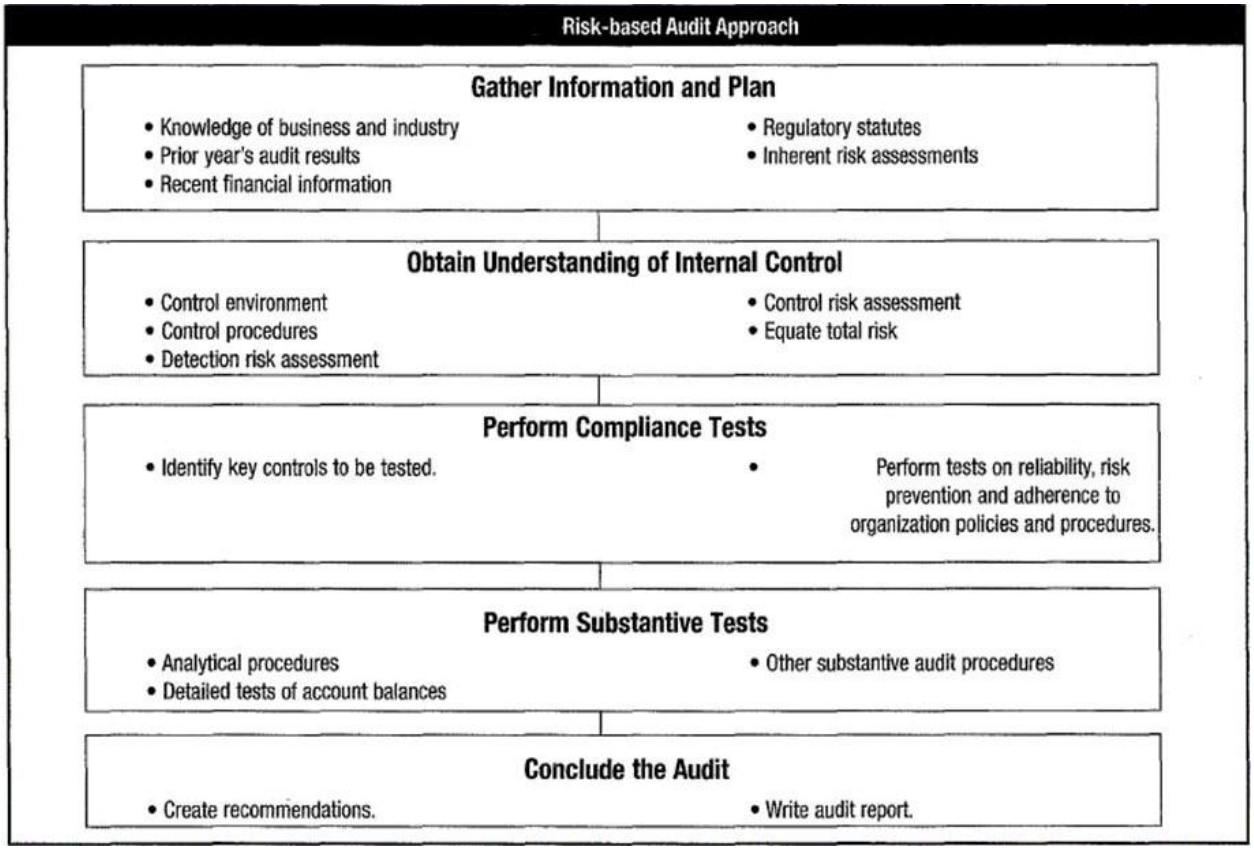
1.5.4 RISK-BASED AUDITING

Effective risk-based auditing is driven by two processes:

1. The risk assessment that drives the audit schedule
2. The risk assessment that minimizes the audit risk during the execution of an audit

A risk-based audit approach is usually adapted to develop and improve the continuous audit process. This approach is used to assess risk and to assist an IS auditor in making the decision to perform either compliance testing or substantive testing. It is important to stress that the risk-based audit approach efficiently assists the auditor in determining the nature and extent of testing.

Within this concept, inherent risk, control risk or detection risk should not be of major concern, despite some weaknesses. In a risk-based audit approach, IS auditors are not just relying on risk; they also are relying on internal and operational controls as well as knowledge of the company or the business. This type of risk assessment decision can help relate the cost-benefit analysis of the control to the known risk, allowing practical choices.



1.5.5 AUDIT RISK AND MATERIALITY

Audit risk can be defined as the risk that information may contain a material error that may go undetected during the course of the audit. The IS auditor should also take into account, if applicable, other factors relevant to the organization: customer data, privacy, availability of provided services as well as corporate and public image as in the case of public organizations or foundations.

Audit risk can be categorized as:

- **Inherent** risk-The risk that an error exists that could be material or significant when combined with other errors encountered during the audit, assuming that there are no related compensating controls. Inherent risk can also be categorized as the susceptibility to a material misstatement in the absence of related controls. For example, complex calculations are more likely to be misstated than simple ones and cash is more likely to be stolen than an inventory of coal. Inherent risks exist independent of an audit and can occur because of the nature of the business.
- **Control** risk-The risk that a material error exists that will not be prevented or detected in a timely manner by the internal controls system. For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often easily missed due to the volume of logged information. The control risk associated with computerized data validation procedures is ordinarily low if the processes are consistently applied.
- **Detection** risk-The risk that an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when, in fact, they do. Detection of an error would not be determined during the risk assessment phase of an audit. However, identifying detection risk would better evaluate and assess the auditor's ability to test, identity and recommend the correction of material errors as the result of a test.
- **Overall audit** risk-The combination of the individual categories of audit risks assessed for each specific control objective. An objective in formulating the audit approach is to limit the audit risk in the area under scrutiny so the overall audit risk is at a sufficiently low level at the completion of the examination. Another objective is to assess and control those risks to achieve the desired level of assurance as efficiently as possible.

1.5.6 RISK ASSESSMENT AND TREATMENT

Assessing Risks

To develop a more complete understanding of audit risk, the IS auditor should also understand how the organization being audited approaches risk assessment and treatment.

Risk assessments should identify, quantify and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action, priorities for managing information security risks, and priorities for implementing controls selected to protect against these risks.
Risk assessments should also be performed periodically to address changes in the environment, security requirements and in the risk situation (e.g., in the assets, threats, vulnerabilities, impacts), and when significant changes occur. These risk assessments should be undertaken in a methodical manner capable of producing comparable and reproducible results.

Treating Risks
Before considering the treatment of a risk, the organization should decide the criteria for determining whether risks can be accepted. Risks may be accepted if, for example, it is assessed that the risk is low or that the cost of treatment is not cost-effective for the organization. Such decisions should be recorded.
Each of the risks identified in the risk assessment needs to be treated. Possible options for risk **treatment include:**
- Applying appropriate controls to reduce the risks.
- Knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance.
- Avoiding risks by not allowing actions that would cause the risks to occur.
- Transferring the associated risks to other parties, e.g. insurers or suppliers.

For those risks where the risk treatment decision has been to apply appropriate controls, controls should be selected to ensure that risks are reduced to an acceptable level, taking into account:
- Requirements and constraints of national and international legislation and regulations
- Organizational objectives
- Operational requirements and constraints
- Cost effectiveness (the need to balance the investment in implementation and operation of controls against the harm likely to result from security failures)

1.5.7 IS AUDIT RISK ASSESSMENT TECHNIQUES
There are many risk assessment methodologies, computerized and non-computerized, from which the IS auditor may choose. These range from simple classifications of high, medium and low, based on the IS auditor's judgment, to complex scientific calculations that provide a numeric risk rating.

One such risk assessment approach is a scoring system that is useful in prioritizing audits based on an evaluation of risk factors. The system considers variables such as technical complexity, level of control procedures in place and level of financial loss. These variables mayor may not be weighted. The risk values are then compared to each other and audits are scheduled accordingly. Another form of risk assessment is judgmental, where an independent decision is made based on business knowledge, executive management directives, historical perspectives, business goals and environmental factors. A combination of techniques may be used as well. Risk assessment methods may change and develop over time to best serve the needs of the organization. The IS auditor should consider the level of complexity and detail appropriate for the organization being audited.
Using risk assessment to determine areas to be audited:
- Enables management to effectively allocate limited audit resources.
- Ensures that relevant information has been obtained from all levels of management, including boards of directors, IS auditors and functional area management. Generally, this information assists management in effectively discharging its responsibilities and ensures that the audit activities are directed to high-risk areas, which will add value for management.
- Establishes a basis for effectively managing the audit department.
- Provides a summary of how the individual audit subject is related to the overall organization as well as to the business plans.

1.5.8 AUDIT PROGRAMS
An audit program is a step-by-step set of audit procedures and instructions that should be performed to complete an audit. Audit programs for financial, operational, integrated, and administrative and IS audits are based on the scope and objective of the particular assignment.

General audit procedures are the basic steps in the performance of an audit and usually include:
- Obtaining and recording an understanding of the audit area/ subject
- A risk assessment and general audit plan and schedule

- Detailed audit planning
- Preliminary review of the audit area/subject
- Evaluating the audit area/Subject
- Verifying and evaluating the appropriateness of controls designed to meet control objectives
- Compliance testing (tests of the implementation of controls, and their consistent application)
- Substantive testing (confirming the accuracy of information)
- Reporting (communicating results)
- Follow-up in cases where there is an internal audit function

The IS auditor must understand the procedures for testing and evaluating IS controls. These procedures could include:

- The use of generalized audit software to survey the contents of data files (including system logs)
- The use of specialized software to assess the contents of operating system database and application parameter files (or detect deficiencies in system parameter settings)
- Flow-charting techniques for documenting automated applications and business processes
- The use of audit logs/reports available in operation/application systems
- Documentation review
- Inquiry and observation
- Walkthroughs
- Reperformance of controls

The IS auditor should have a sufficient understanding of these procedures to allow for the planning of appropriate audit tests.

1.5.9 FRAUD DETECTION

Management is primarily responsible for establishing, implementing and maintaining a framework and design of IT controls to meet the internal control objectives. A well-designed internal control system provides good opportunities for deterrence and/or timely detection of fraud. Internal controls may fail where such controls are circumvented by exploiting vulnerabilities or through management perpetrated weakness in controls or collusion among people.

Legislation and regulations relating to corporate governance cast significant responsibilities on management, auditors and the audit committee regarding detection and disclosure of any frauds, whether material or not.

The presence of internal controls does not altogether eliminate fraud. IS auditors should be aware of the possibility and means of perpetrating fraud, especially by exploiting the vulnerabilities and overriding controls in the IT-enabled environment. IS auditors should have knowledge of fraud and fraud indicators, and be alert to the possibility of fraud and errors while performing an audit.

1.5.10 COMPLIANCE VERSUS SUBSTANTIVE TESTING

Compliance testing is evidence gathering for the purpose of testing an organisation’s compliance with control procedures. This differs from substantive testing in which evidence is gathered to evaluate the integrity of individual transactions, data or other information.

A compliance test determines if controls are being applied in a manner that complies with management policies and procedures. For example, if the IS auditor is concerned about whether production program library controls are working properly, the IS auditor might select a sample of programs to determine if the source and object versions are the same. The broad objective of any compliance test is to provide IS auditors with reasonable assurance that the particular control on which the IS auditor plans to rely is operating as the IS auditor perceived in the preliminary evaluation.

It is important that the IS auditor understands the specific objective of a compliance test and of the control being tested. Compliance tests can be used to test the existence and effectiveness of a defined process, which may include a trail of documentary and/or automated evidence-for example, to provide assurance that only authorized modifications are made to production programs.

Examples of compliance testing of controls where sampling could be considered include user access rights, program change control procedures, documentation procedures, program documentation, follow-up of exceptions, review of logs, software license audits, etc.

A substantive test substantiates the integrity of actual processing. It provides evidence of the validity and integrity of the balances in the financial statements, and the transactions that support these balances. IS auditors could use substantive tests to test for monetary errors directly affecting financial statement balances, or other relevant data ofthe organization. Additionally, an IS auditor might develop a substantive

test to determine if the tape library inventory records are stated correctly. To perform this test, the IS auditor might take a thorough inventory or might use a statistical sample, which will allow the IS auditor to develop a conclusion regarding the accuracy of the entire inventory.

There is a direct correlation between the level of internal controls and the amount of substantive testing required. If the results of testing controls (compliance tests) reveal the presence of adequate internal controls, then the IS auditor is justified in minimizing the substantive procedures. Conversely, if the control testing reveals weaknesses in controls that may raise doubts about the completeness, accuracy or validity of the accounts, substantive testing can alleviate those doubts.
Examples of substantive tests where sampling could be considered include performance of a complex calculation (e.g., interest) on a sample of accounts or a sample of transactions to vouch for supporting documentation, etc.

1.5.11 EVIDENCE

Evidence is any information used by the IS auditor to determine whether the entity or data being audited follows the established criteria or objectives, and supports audit conclusions. It is a requirement that the auditor's conclusions be based on sufficient, relevant and competent evidence. When planning the IS audit, the IS auditor should take into account the type of audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability.

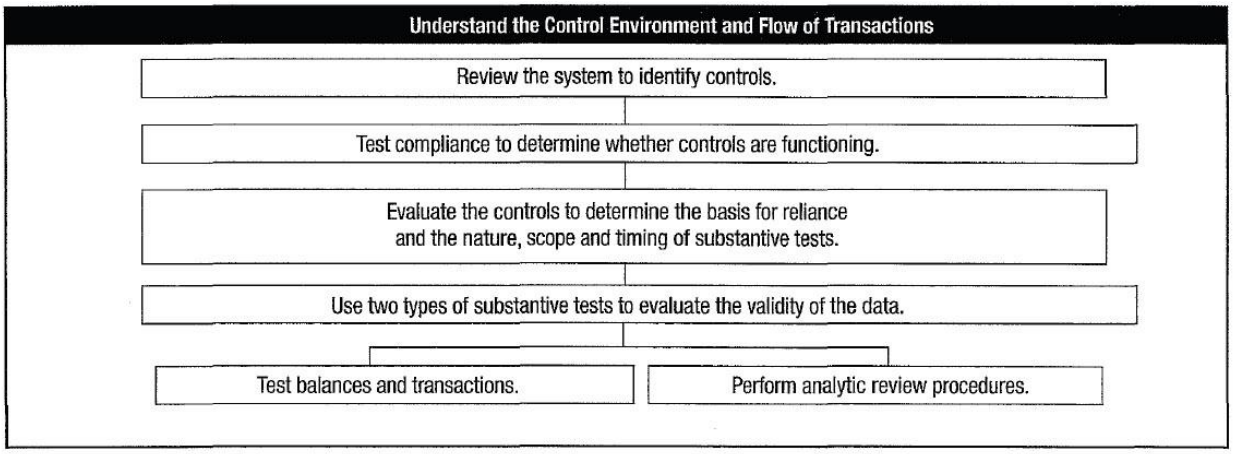
Audit evidence may include:

- The IS auditor's observations
- Notes taken from interviews
- Results of independent confirmations obtained by the IS auditor from different stakeholders
- Material extracted from correspondence and internal documentation or contracts with external partners
- The results of audit test procedures

While all evidence will assist the IS auditor in developing audit conclusions, some types of evidence are more reliable than others. The rules of evidence and sufficiency as well as the competency of evidence must be taken into account as required audit standards.

Determinants for evaluating the reliability of audit evidence include:

- **Independence of the provider of the evidence-** Evidence obtained from outside sources is more reliable than from within the organization. This is why confirmation letters are used for verification of accounts receivable balances. Additionally, signed contracts or agreements with external parties could be considered reliable if the original documents are made available for review.
- **Qualifications of the individual providing the information/evidence-**Whether the providers of the information/evidence are inside or outside of the organization, the IS auditor should always consider the qualifications and functional responsibilities of the persons providing the information. This can also be true of the IS auditor. If an IS auditor does not have a good understanding of the technical area under review, the information gathered from testing that area may not be reliable, especially if the IS auditor does not fully understand the test.
- **Objectivity of the evidence-**Objective evidence is more reliable than evidence that requires considerable judgment or interpretation. An IS auditor's review of media inventory is direct, objective evidence. An IS auditor's analysis of the efficiency of an application, based on discussions with certain personnel, may not be objective audit evidence.
- **Timing of the evidence-**The IS auditor should consider the time during which information exists or is available in determining the nature, timing and extent of compliance testing and, if applicable, substantive testing. For example, audit evidence processed by dynamic systems, such as spreadsheets, may not be retrievable after a specified period of time if changes to the files are not controlled or the files are not backed up.



The following are techniques for gathering evidence:

- **Reviewing IS organization structures-**An organizational structure that provides an adequate separation or segregation of duties is a key general control in an IS environment. The IS auditor should understand general organizational controls and be able to evaluate these controls in the organization under audit.
- **Reviewing IS policies and procedures-**An IS auditor should review whether appropriate policies and procedures are in place, determine whether personnel understand the implemented policies and procedures, and ensure that policies and procedures are being followed.
- **Reviewing IS standards-**The IS auditor should first understand the existing standards in place within the organization.
- **Reviewing IS documentation-**A first step in reviewing the documentation for an information system is to understand the existing documentation in place within the organization.
  Documentation may include:
  - Systems development initiating documents (e.g., feasibility study)
  - Documentation provided by external application suppliers
  - Service level agreements (SLAs) with external IT providers
  - Functional requirements and design specifications
  - Tests plans and reports
  - Program and operations documents
  - Program change logs and histories
  - User manuals
  - Operations manuals
  - Security-related documents (e.g., security plans, risk assessments)
  - -BCPs
  - -QA reports
  - Reports on security metrics

- **Interviewing appropriate personnel-**Interviewing techniques are an important skill for the IS auditor. Interviews should be organized in advance with objectives clearly communicated, follow a fixed outline and be documented by interview notes. An interview form or checklist prepared by an IS auditor is a good approach.
- **Observing processes and employee performance-**The observation of processes is a key audit technique for many types of review. The IS auditor should be unobtrusive while making observations and should document everything in sufficient detail to be able to present it, if required, as audit evidence at a later date.
- **Reperformance-**The reperformance process is a key audit technique that generally provides better evidence than the other techniques and is therefore used when a combination of inquiry, observation and examination of evidence does not provide sufficient assurance that a control is operating effectively.
- **Walkthroughs-**The walkthrough is an audit technique to confirm the understanding of controls.

1.5.12 INTERVIEWING AND OBSERVING PERSONNEL IN PERFORMANCE OF THEIR DUTIES

Observing personnel in the performance of their duties assists an IS auditor in identifying:

- **Actual functions--**Observation could be an adequate test to ensure that the individual who is assigned and authorized to perform a particular function is the person who is actually doing the job. It allows the

IS auditor an opportunity to witness how policies and procedures are understood and practiced. Depending on the specific situation, the results of this type of test should be compared with the respective logical access rights.

- **Actual processes/procedures-**Performing a walk-through of the process/procedure allows the IS auditor to gain evidence of compliance and observe deviations, if any. This type of observation could prove to be useful for physical controls.
- **Security awareness**-Security awareness should be observed to verify an individual's understanding and practice of good preventive and detective security measures to safeguard the company's assets and data. This type of information could be complemented with an examination of previous and planned security training.
- **Reporting relationships**-Reporting relationships should be observed to ensure that assigned responsibilities and adequate segregation of duties are being practiced. Often, the results of this type of test should be compared with the respective logical access rights.

1.5.13 SAMPLING

Sampling is used when time and cost considerations preclude a total verification of all transactions or events in a predefined population. The population consists of the entire group of items that need to be examined.

The two general approaches to audit sampling are statistical and non-statistical:
I. Statistical sampling-An objective method of determining the sample size and selection criteria. Statistical sampling uses the mathematical laws of probability to: a) calculate the sampling size, b) select the sample items, and c) evaluate the sample results and make the inference. With statistical sampling, the IS auditor quantitatively decides how closely the sample should represent the population (assessing sample precision) and the number of times in 100 that the sample should represent the population (the reliability or confidence level). This assessment will be represented as a percentage. The results of a valid statistical sample are mathematically quantifiable.
2. Non-statistical sampling (often referred to as judgmental sampling)-Uses auditor judgment to determine the method of sampling, the number of items that will be examined from a population (sample size) and which items to select (sample selection). These decisions are based on subjective judgment as to which items/transactions are the most material and most risky.

When using either statistical or non-statistical sampling methods, the IS auditor should design and select an audit sample, perform audit procedures, and evaluate sample results to obtain sufficient, reliable, relevant and useful audit evidence. These methods of sampling require the IS auditor to use judgment when defining the population characteristics, and, thus are subject to the risk that the IS auditor will draw the wrong conclusion from the sample (sampling risk).

When using either statistical or non-statistical sampling methods, the IS auditor should design and select an audit sample, perform audit procedures, and evaluate sample results to obtain sufficient, reliable, relevant and useful audit evidence. These methods of sampling require the IS auditor to use judgment when defining the population characteristics, and, thus are subject to the risk that the IS auditor will draw the wrong conclusion from the sample (sampling risk).

Within these two general approaches to audit sampling, there are two primary methods of sampling used by IS auditors-attribute sampling and variable sampling. Attribute sampling, generally applied in compliance testing situations, deals with the presence or absence of the attribute and provides conclusions that are expressed in rates of incidence. Variable sampling, generally applied in substantive testing situations, deals with population characteristics that vary, such as monetary values and weights (or any other measurement), and provides conclusions related to deviations from the norm.

Attribute sampling refers to three different but related types of proportional sampling:

1. Attribute sampling (also referred to as fixed sample-size attribute sampling or frequency-estimating sampling)-A sampling model that is used to estimate the rate (percent) of occurrence of a specific quality (attribute) in a population. Attribute sampling answers the question of "how many?" An example of an attribute that might be tested is approval signatures on computer access request forms.
2. Stop-or-go sampling-A sampling model that helps prevent excessive sampling of an attribute by allowing an audit test to be stopped at the earliest possible moment. Stop-or-go sampling is used when the IS auditor believes that relatively few errors will be found in a population.

3. Discovery sampling-A sampling model that can be used when the expected occurrence rate is extremely low. Discovery sampling is most often used when the objective of the audit is to seek out (discover) fraud, circumvention of regulations or other irregularities.

Variable sampling-also known as dollar estimation or mean estimation sampling-is a technique used to estimate the monetary value or some other unit of measure (such as weight) of a population from a sample portion. An example of variable sampling is a review of an organization's balance sheet for material transactions and an application review of the program that produced the balance sheet.

Variable sampling refers to a number of different types of quantitative sampling models:

1. **Stratified mean per unit-**A statistical model in which the population is divided into groups and samples are drawn from the various groups. Stratified mean sampling is used to produce a smaller overall sample size relative to unstratified mean per unit.
2. **Unstratified mean per unit-**A statistical model in which a sample mean is calculated and projected as an estimated total.
3. **Difference estimation-**A statistical model used to estimate the total difference between audited values and book (unaudited) values based on differences obtained from sample observations. To perform attribute or variable sampling, the following statistical sampling terms need to be understood:

- **Confidence coefficient (also referred to as confidence level or reliability factor)--**A percentage expression (90 percent, 95 percent, 99 percent, etc.) of the probability that the characteristics of the sample are a true representation of the population. Generally, a 95 percent confidence coefficient is, considered a high degree of comfort. If the IS auditor knows internal controls are strong, the confidence coefficient may be lowered. The greater the confidence coefficient, the larger the sample size.
- **Level of risk-**Equal to one minus the confidence coefficient. For example, if the confidence coefficient is 95 percent, the level of risk is five percent (100 percent minus 95 percent).
- **Precision-**Set by the IS auditor, it represents the acceptable range difference between the sample and the actual population. For attribute sampling, this figure is stated as a percentage. For variable sampling, this figure is stated as a monetary amount or a number. The higher the precision amount, the smaller the sample size and the greater the risk of fairly large total error amounts going undetected. The smaller the precision amount, the greater the sample size. A very low precision level may lead to an unnecessarily large sample size.
- **Expected error rate--**An estimate stated as a percent of the errors that may exist. The greater the expected error rate, the greater the sample size. This figure is applied to attribute sampling formulas but not to variable sampling formulas.
- **Sample mean-**The sum of all sample values, divided by the size of the sample. The sample mean measures the average value of the sample.
- **Sample standard deviation-**Computes the variance of the sample values from the mean of the sample. Sample standard deviation measures the spread or dispersion of the sample values.
- **Tolerable error rate--**Describes the maximum misstatement or number of errors that can exist without an account being materially misstated. Tolerable rate is used for the planned upper limit of the precision range for compliance testing. The term is expressed as a percentage. Precision range and precision have the same meaning when used in substantive testing.
- **Population standard deviation-**A mathematical concept that measures the relationship to the normal distribution. The greater the standard deviation, the larger the sample size. This figure is applied to variable sampling formulas but not to attribute sampling formulas.

Key steps in the construction and selection of a sample for an audit test include:

- Determining the objectives of the test
- Defining the population to be sampled
- Determining the sampling method, such as attribute vs. variable sampling
- Calculating the sample size
- Selecting the sample
- Evaluating the sample from an audit perspective

1.5.4 USING THE SERVICES OF OTHER AUDITORS AND EXPERTS

Due to the scarcity of IS auditors and the need for IT security specialists and other subject matter experts to conduct audits of highly specialized areas, the audit department or auditors entrusted with providing assurance may require the services of other auditors or experts. Outsourcing of IS assurance and security services is increasingly becoming a common practice. External experts could include experts in specific

technologies such as networking, automated teller machine (ATM), wireless, systems integration and digital forensics, or subject matter experts such as specialists in a particular industry or area of specialization such as banking, securities trading, insurance, legal experts, etc.
When a part or all of IS audit services are proposed to be outsourced to another audit or external service provider, the following should be considered with regard to using the services of other auditors and experts:

- Restrictions on outsourcing of audit/security services provided by laws and regulations
- Audit charter or contractual stipulations
- Impact on overall and specific IS audit objectives
- Impact on IS audit risk and professional liability
- Independence and objectivity of other auditors and experts
- Professional competence, qualifications and experience
- Scope of work proposed to be outsourced and approach
- Supervisory and audit management controls
- Method and modalities of communication of results of audit work
- Compliance with legal and regulatory stipulations
- Compliance with applicable professional standards

Based on the nature of assignment, the following may also require special consideration:
• Testimonials/references and background checks
• Access to systems, premises and records
• Confidentiality restrictions to protect customer-related information
• Use of computer-assisted audit techniques (CAATs) and other tools to be used by the external audit service provider
• Standards and methodologies for performance of work and documentation
• Nondisclosure agreements

The IS auditor or entity outsourcing the services should monitor the relationship to ensure the objectivity and independence throughout the duration of the arrangement.
It is important to understand that often, even though a part of or the whole of the audit work may be delegated to an external service provider, the related professional liability is not necessarily delegated. Therefore, it is the responsibility of the IS auditor or entity employing the services of external service providers to:
• Clearly communicate the audit objectives, scope and methodology through a formal engagement letter.
• Put in place a monitoring process for regular review of the work of the external service provider with regard to planning, supervision, review and documentation. For example, review of the work papers of other IS auditors or experts to confirm the work was appropriately planned, supervised, documented and reviewed, and to consider the appropriateness and sufficiency of the audit evidence provided; or review of the report of other IS auditors or experts to confirm the scope specified in the audit charter, terms of reference or letter of engagement has been met, that any significant assumptions used by other IS auditors or experts have been identified, and the findings and conclusions reported have been agreed on by management.
• Assess the usefulness and appropriateness of reports of such external providers, and assess the impact of significant findings on the overall audit objectives.

1.5.15 COMPUTER-ASSISTED AUDIT TECHNIQUES

CAATs are important tools for the IS auditor in gathering information from these environments. When systems have different hardware and software environments, data structure, record formats or processing functions, it is almost impossible for the auditors to collect evidence without a software tool to collect and analyze the records.

CAATs include many types of tools and techniques such as generalized audit software (GAS), utility software, debugging and scanning software, test data, application software tracing and mapping, and expert systems.

GAS refers to standard software that has the capability to directly read and access data from various database platforms, flat-file systems and ASCII formats. GAS provides IS auditors an independent means to gain access to data for analysis and the ability to use high-level, problem-solving software to invoke functions to be performed on data files. Features include mathematical computations, stratification, statistical analysis, sequence checking, duplicate checking and recomputations. The following functions are commonly supported by GAS:

- **File** access-Enables the reading of different record formats and file structures

- **File** reorganization-Enables indexing, sorting, merging and linking with another file
- **Data** selection-Enables global filtration conditions and selection criteria
- **Statistical** functions-Enables sampling, stratification and frequency analysis
- **Arithmetical** functions-Enables arithmetic operators and functions

Utility software is a subset of software-such as report generators of the database management system-that provides evidence to auditors about system control effectiveness. Test data involve the auditors using a sample set of data to assess whether logic errors exist in a program and whether the program meets its objectives. The review of an application system will provide information about internal controls built in the system. The audit-expert system will give direction and valuable information to all levels of auditors while carrying out the audit because the query-based system is built on the knowledge base of the senior auditors or managers.
These tools and techniques can be used in performing various audit procedures:
- Tests of the details of transactions and balances
- Analytical review procedures
- Compliance tests of IS general controls
- Compliance tests of IS application controls
- Network and operating system (OS) vulnerability assessments
- Penetration testing
- Application security testing and source code security scans

An IS auditor should weigh the costs and benefits of CAATs before going through the effort, time and expense of purchasing or developing them. Issues to consider include:
- Ease of use, both for existing and future audit staff
- Training requirements
- Complexity of coding and maintenance
- Flexibility of uses
- Installation requirements
- Processing efficiencies (especially with a PC CAAT)
- Effort required to bring the source data into the CAATs for analysis
- Ensuring the integrity of imported data by safeguarding its authenticity
- Recording the time stamp of data downloaded at critical processing points to sustain the credibility of the review
- Obtaining permission to install the software on the auditee servers
- Reliability of the software
- Confidentiality of the data being processed

When developing CAATs, the following are examples of documentation to be retained:
- Online reports detailing high-risk issues for review
- Commented program listings
- Flowcharts
- Sample reports
- Record and file layouts
- Field definitions
- Operating instructions
- Description of applicable source documents

CAATs documentation should be referenced to the audit program, and clearly identify the audit procedures and objectives being served. When requesting access to production data for use with CAATs, the IS auditor should request read-only access. Any data manipulation by the IS auditor should be done to copies of production files in a controlled environment to ensure that production data are not exposed to unauthorized updating. Most of the CAATs provide for downloading production data from production systems to a standalone platform and then conducting analysis from the standalone platform, thereby insulating the production systems from any adverse impact.

CAATs as a Continuous Online Audit Approach
An increasingly important advantage of CAATs is the ability to improve audit efficiency through continuous online auditing techniques. To this end, IS auditors must develop audit techniques that are appropriate for use with advanced computerized systems. In addition, they must be involved in the creation of advanced systems at the early stages of development and implementation, and must make greater use of automated tools that are suitable for their organization's automated environment. This takes the form of the continuous

audit approach. (For more detailed information on continuous online auditing, see chapter 3, Systems and Infrastructure Life Cycle Management.)

1.5.16 EVALUATION OF THE CONTROL ENVIRONMENT

The IS auditor will review evidence gathered during the audit to determine if the operations reviewed are well controlled and effective. This is also an area that requires the IS auditor's judgment and experience. The IS auditor should assess the strengths and weaknesses of the controls evaluated and then determine if they are effective in meeting the control objectives established as part of the audit planning process.
A control matrix is often utilized in assessing the proper level of controls. Known types of errors that can occur in the area under review are placed on the top axis and known controls to detect or correct errors are placed on the side axis. Then, using a ranking method, the matrix is filled with the appropriate measurements. When completed, the matrix will illustrate areas where controls are weak or lacking.
In some instances, one strong control may compensate for a weak control in another area. For example, if the IS auditor finds weaknesses in a system's transaction error report, the IS auditor may find that a detailed manual balancing process over all transactions compensates for the weaknesses in the error report.

Judging the Materiality of Findings
The concept of materiality is a key issue when deciding which findings to bring forward in an audit report. Key to determining the materiality of audit findings is the assessment of what would be significant to different levels of management. Assessment requires judging the potential effect of the finding if corrective action is not taken. A weakness in computer security physical access controls at a remote distributed computer site may be significant to management at the site, but will not necessarily be material to upper management at headquarters. However, there may be other matters at the remote site that would be material to upper management.

The IS auditor must use judgment when deciding which findings to present to various levels of management. For example, the IS auditor may find that the transmittal form for delivering tapes to the offsite storage location is not properly initialed or authorization evidenced by management as required by procedures. If the IS auditor finds that management otherwise pays attention to this process and that there have been no problems in this area, the IS auditor may decide that the failure to initial transmittal documents is not material enough to bring to the attention of upper management.

E. Communicating Audit Results

1.6 COMMUNICATING AUDIT RESULTS

The exit interview, conducted at the end of the audit, provides the IS auditor with the opportunity to discuss findings and recommendations with management. During the exit interview the IS auditor should:

- Ensure that the facts presented in the report are correct;
- Ensure that the recommendations are realistic and cost-effective and, if not, seek alternatives through negotiation with auditee management;
- Recommend implementation dates for agreed-on recommendations.

The IS auditor will frequently be asked to present the results of audit work to various levels of management. The IS auditor should have a thorough understanding of the presentation techniques necessary to communicate these results.

Presentation techniques could include the following:

- **Executive summary-** An easy-to-read, concise report that presents findings to management in an understandable manner. Findings and recommendations should be communicated from a business perspective. Detailed attachments can be more technical in nature because operations management will require the detail to correct the reported situations.
- **Visual presentation-** May include slides or computer graphics.

Before communicating the results of an audit to senior management, the IS auditor should discuss the findings with the management staff of the audited entity. The goal of such a discussion would be to gain agreement on the findings and develop a course of corrective action. In cases where there is disagreement, the IS auditor should elaborate on the significance of the findings, risk and effects of not correcting the control weakness.

1.6.1 AUDIT REPORT STRUCTURE AND CONTENTS

There is no specific format for an IS audit report; the organization's audit policies and procedures will dictate the general format. Audit reports will usually have the following structure and content.

- An introduction to the report including a statement of audit objectives, limitations to the audit and scope, the period of audit coverage, and a general statement on the nature and extent of audit procedures conducted and processes examined during the audit, followed by a statement on the IS audit methodology and guidelines.
- Audit findings included in separate sections and often grouped in sections by materially and/or intended recipient.
- The IS auditor's overall conclusion and opinion on the adequacy of controls and procedures examined during the audit, and the actual potential risk indentified as a consequence of detected deficiencies.
- The IS auditor's reservations or qualifications with respect to the audit:
    - This may state that the controls or procedures examined were found to be adequate or inadequate. The balance of the audit report should support that conclusion, and the overall evidence gathered during the audit should provide an even greater level of support for the audit conclusions.
- Detailed audit findings and recommendations
    - The IS auditor decides whether to include specific findings in an audit report. This should be based on the materiality of the findings and the intended recipient of the audit report. An audit report directed to the audit committee of the board of directors, for example, may not include findings that are important only to local management but have little control significance or the overall organization.
- A variety of findings, some of which may e quite material while others are minor in nature.
    - The auditor may choose to present minor findings to management in an alternate format such as by memorandum.

The IS auditor should be concerned with providing a balanced report, describing not only negative issues in terms of findings but positive constructive comments regarding improving processes and controls or effective controls already in place. Overall, the IS auditor should exercise independence in the reporting process.
Auditee management evaluates the findings, stating corrective actions to be taken and timing for implementing these anticipated corrective actions.

1.6.2 AUDIT DOCUMENTATION

Audit documentation should include, at a minimum, a record of the following:

- Planning and preparation of the audit scope and objectives
- Description and/or walk-throughs on the scoped audit area
- Audit program
- Audit steps performed and audit evidence gathered
- Use of services of other auditors and experts
- Audit findings, conclusions and recommendations
- Audit documentation relation with document identification and dates

It is also recommended that documentation include:

- A copy of the report issued as a result of the audit work
- Evidence of audit supervisory review

Documents should include audit information that is required by laws and regulations, contractual stipulations and professional standards.
The IS auditor/IS audit department should also develop policies regarding custody, retention requirements and release of audit documentation.
Audit documentation should support the findings and conclusions/ opinion. Time of evidence can be crucial to supporting audit findings and conclusions.

1.6.3 CLOSING FINDINGS

IS auditors should realize that auditing is an ongoing process. The IS auditor is not effective if audits are performed and reports issued but no follow-up is conducted to determine whether management has taken appropriate corrective actions. IS auditors should have a follow-up program to determine if agreed-on corrective actions have been implemented. Although IS auditors who work for external audit firms may not necessarily follow this process, they may achieve these tasks if agreed to by the audited entity.

The timing of the follow-up will depend on the criticality of the findings and would be subject to the IS auditor's judgment. The results of the follow-up should be communicated to appropriate levels of management.
The level of the IS auditor's follow-up review will depend on several factors. In some instances, the IS auditor may merely need to inquire as to the current status.

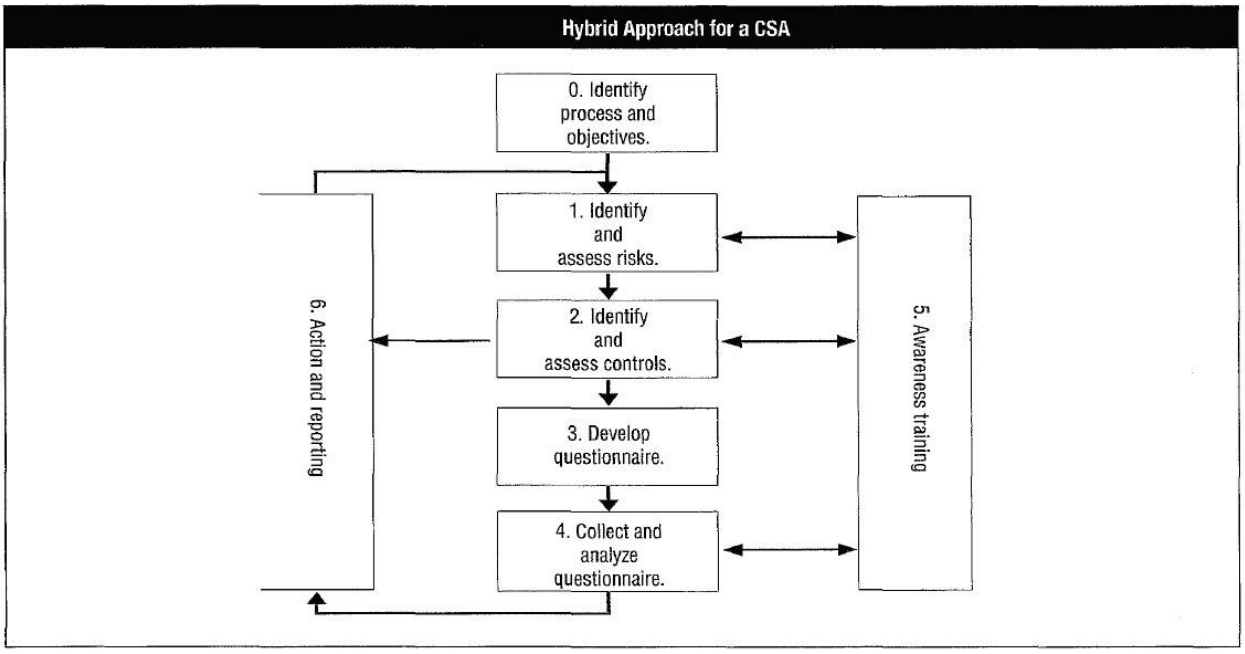
1.7 CONTROL SELF-ASSESSMENT

Control self-assessment (CSA) can be defined as a management technique that assures stakeholders, customers and other parties that the internal control system of the organization is reliable. It also ensures that employees are aware ofthe risks to the business and they conduct periodic, proactive reviews of controls. It is a methodology used to review key business objectives, risks involved in achieving the business objectives and internal controls designed to manage these business risks in a formal, documented collaborative process.

In practice, CSA is a series of tools on a continuum of sophistication ranging from simple questionnaires to facilitated workshops, designed to gather information about the organization by asking those with a day-to-day working knowledge of an area as well as their managers. The basic tools used during a CSA project are the same whether the project is technical, fmancial or operational. These tools include management meetings, client workshops, worksheets, rating sheets and the CSA project approach. Like the continuum of tools used to gather information, there are diverse approaches to the levels below management that are queried; some organizations even include outsiders (such as clients or trading partners) when making CSA assessments.

The CSA program can be implemented by various methods. For small business units within organizations, it can be implemented by facilitated workshops where functional management and control professionals such as auditors can come together and deliberate how best to evolve a control structure for the business unit.
In a workshop, the role of a facilitator is to support the decision making process. The facilitator creates a supportive environment to help participants explore their own experiences and those of others, identify control strengths and weaknesses, and share their knowledge, ideas and concerns. If appropriate, a facilitator may also offer his/her own expertise in addition to facilitating the exchange of ideas and experience. A facilitator does not have to be an expert in a certain process or subject matter; however, the facilitator should have basic skills such as:

- active listening skills and the ability to ask good questions, including questions that probe the topics and move the discussions forward.
- good verbal communication skills, including the ability to pose questions in a nonthreatening manner and the ability to summarize material.
- the ability to manage the dynamics of the group, including managing various personalities so that a few members do not
- dominate the discussions and managing processes so that goals are met.
- the ability to resolve conflicts.
- the ability to manage time and keep the proceedings on schedule.



1.7.1 OBJECTIVES OF CSA

There are several objectives associated with adopting a CSA program. The primary objective is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional areas. It is not intended to replace audit's responsibilities, but to enhance them. Auditees such as line managers are responsible for controls in their environment; the managers also should be responsible for monitoring the controls. CSA programs also must educate management about control design and monitoring, particularly concentration on areas of high risk.

When employing a CSA program, measures of success for each phase (planning, implementation and monitoring) should be developed to determine the value derived from CSA and its future use. One critical success factor (CSF) is to conduct a meeting with the business unit representatives (including appropriate and relevant staff and management) to identify the business unit's primary objective-to determine the reliability of the internal control system.

A generic set of goals and metrics for each process, which can be used in designing and monitoring the CSA program, has been provided in COBIT.

1.7.2 BENEFITS OF CSA

Some of the benefits of a CSA include the following:

- Early detection of risks
- More effective and improved internal controls
- Creation of cohesive teams through employee involvement
- Developing a sense of ownership of the controls in the employees and process owners, and reducing their resistance to control improvement initiatives
- Increased employee awareness of organizational objectives, and knowledge of risk and internal controls
- Increased communication between operational and top management
- Highly motivated employees
- Improved audit rating process
- Reduction in control cost
- Assurance provided to stakeholders and customers
- Necessary assurance given to top management about the adequacy of internal controls as required by the various regulatory agencies and laws such as the US Sarbanes-Oxley Act

1. 7.3 DISADVANTAGES OF CSA

CSA does potentially contain several disadvantages which include:

- It could be mistaken as an audit function replacement
- It may be regarded as an additional workload (e.g., one more report to be submitted to management)
- Failure to act on improvement suggestions could damage employee morale
- Lack of motivation may limit effectiveness in the detection of weak controls

1.7.4 AUDITOR ROLE IN CSA

The auditor's role in CSAs should be considered enhanced when audit departments establish a CSA program. When these programs are established, auditors become internal control professionals and assessment facilitators. Their value in this role is evident when management takes responsibility and ownership for internal control systems under their authority through process improvements in their control structures, including an active monitoring component. For an auditor to be effective in this facilitative and innovative role, the auditor must understand the business process being assessed. This can be attained via traditional audit tools such as a preliminary surveyor walk -through. Also, the auditors must remember that they are the facilitators and the management client is the participant in the CSA process. For example, during a CSA workshop, instead of the auditor performing detailed audit procedures, the auditor will lead and guide the auditees in assessing their environment by providing insight about the objectives of controls based on risk assessment. The managers, with a focus on improving the productivity of the process, might suggest replacement of preventive controls. In this case, the auditor is better positioned to explain the risks associated with such changes.

1. **7.5 TECHNOLOGY DRIVERS FOR CSA**

The development of techniques for empowerment, information gathering and decision making is a necessary part of a CSA program implementation. Some of the technology drivers include the combination of hardware and software to support CSA selection, and the use of an electronic meeting system and computer-supported decision aids to facilitate group decision making. Group decision making is an essential component of a workshop-based CSA where employee empowerment is a goal. In case of a questionnaire approach, the same principle applies for the analysis and readjustment of the questionnaire.

1. 7.6 TRADITIONAL VS. CSA APPROACH

The traditional approach can be summarized as any approach in which the primary responsibility for analyzing and reporting on internal control and risk is assigned to auditors, and to a lesser extent, controller departments and outside consultants. This approach has created and reinforced the notion that auditors and consultants, not management and work teams, are responsible for assessing and reporting on internal control. The CSA approach, on the other hand, emphasizes management and accountability over developing and monitoring internal controls of an organization's sensitive and critical business processes.

Traditional and CSA Attributes	
Traditional Historical	**CSA**
Assigns duties/supervises staff	Empowered/accountable employees
Policy/rule-driven	Continuous improvement/learning curve
Limited employee participation	Extensive employee participation and training
Narrow stakeholder focus	Broad stakeholder focus
Auditors and other specialists	Staff at all levels, in all functions, are the primary control analysts.
Reporters	Reporters

1.8 THE EVOLVING IS AUDIT PROCESS

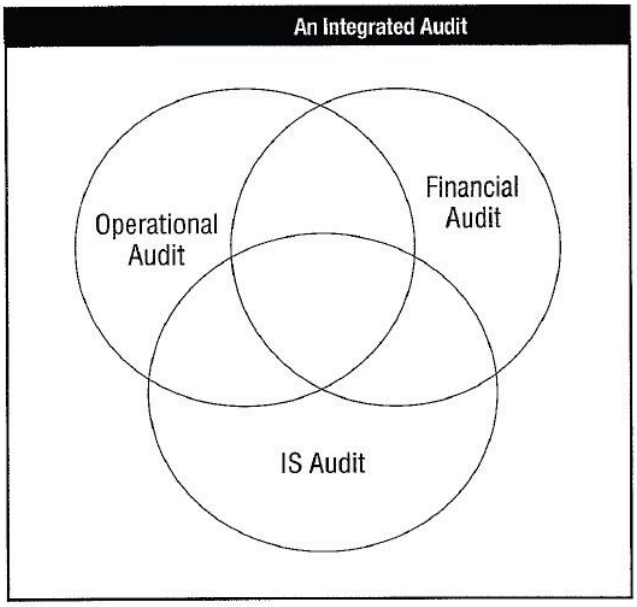
1.8.1 INTEGRATED AUDITING

Integrated auditing can be defined as the process whereby appropriate audit disciplines are combined to assess key internal controls over an operation, process or entity.

The integrated approach focuses on risk. A risk analysis assessment aims to understand and identify risks arising from the entity and its environment, including relevant internal controls. At this stage, the role of IT audit is typically to understand and identify risks under topical areas such as information management, IT infrastructure, IT governance and IT operations. Other audit specialists will seek to understand the organizational environment, business risks and business controls. A key element of the integrated approach is discussion of the risks arising among the whole audit team, with consideration of impact and likelihood.

The integrated audit process typically involves:

- Identification of risks faced by the organization for the area being audited
- Identification of relevant key controls
- Review and understanding of the design of key controls
- Testing that key controls are supported by the IT system
- Testing that management controls operate effectively
- A combined report or opinion on control risks, design and weaknesses



1.8.2 CONTINUOUS AUDITING

The focus on increased effectiveness and efficiency of assurance, internal auditing and control has spurred the development of new studies and examination of new ideas concerning continuous auditing as opposed to more traditional periodic auditing reviews. Several research studies and documents addressing the subject carry different definitions of continuous auditing. All studies, however, recognize that a distinctive character of continuous auditing is the short time lapse between the facts to be audited, the collection of evidence and audit reporting.

Some of the drivers of continuous auditing are a better monitoring of financial issues within a company, ensuring that real-time transactions also benefit from real-time monitoring, prevention of financial fraud and audit scandals such as Enron and WorldCom, and the use of software to determine that financial controls are proper. Continuous auditing involves a large amount of work because the company practicing continuous auditing will not provide one report at the end of a quarter, but will provide financial reports on a more frequent basis.

To properly understand the implications and requirements of continuous auditing, a clear distinction has to be made between continuous auditing and continuous monitoring:

- Continuous monitoring-Provided by IS management tools and typically based on automated procedures to meet fiduciary responsibilities. For instance, real-time antivirus or intrusion detection systems (IDSs) may operate in a continuous monitoring fashion.
- Continuous auditing-"A methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors' reports issued simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter".

Prerequisites/preconditions for continuous auditing to succeed include:

- A high degree of automation
- An automated and highly reliable process in producing information about subject matter soon after or during the occurrence of events underlying the subject matter
- Alarm triggers to report timely control failures
- Implementation of highly automated audit tools that require the IS auditor to be involved in setting up the parameters
- Quickly informing IS auditors of the results of automated procedures, particularly when the process has identified anomalies or errors
- The quick and timely issuance of automated audit reports
- Technically proficient IS auditors
- Availability of reliable sources of evidence
- Adherence to materiality guidelines
- A change of mindset required for IS auditors to embrace continuous reporting
- Evaluation of cost factors

IT techniques that are used to operate in a continuous auditing environment must work at all data levels-single input, transaction and databases-and include:

- Transaction logging
- Query tools
- Statistics and data analysis (CAAT)
- Database management system (DBMS)
- Data warehouses, data marts, data mining
- Intelligent agents
- Embedded audit modules (EAM)
- Neural network technology
- Standards such as Extensible Business Reporting Language (XBRL)