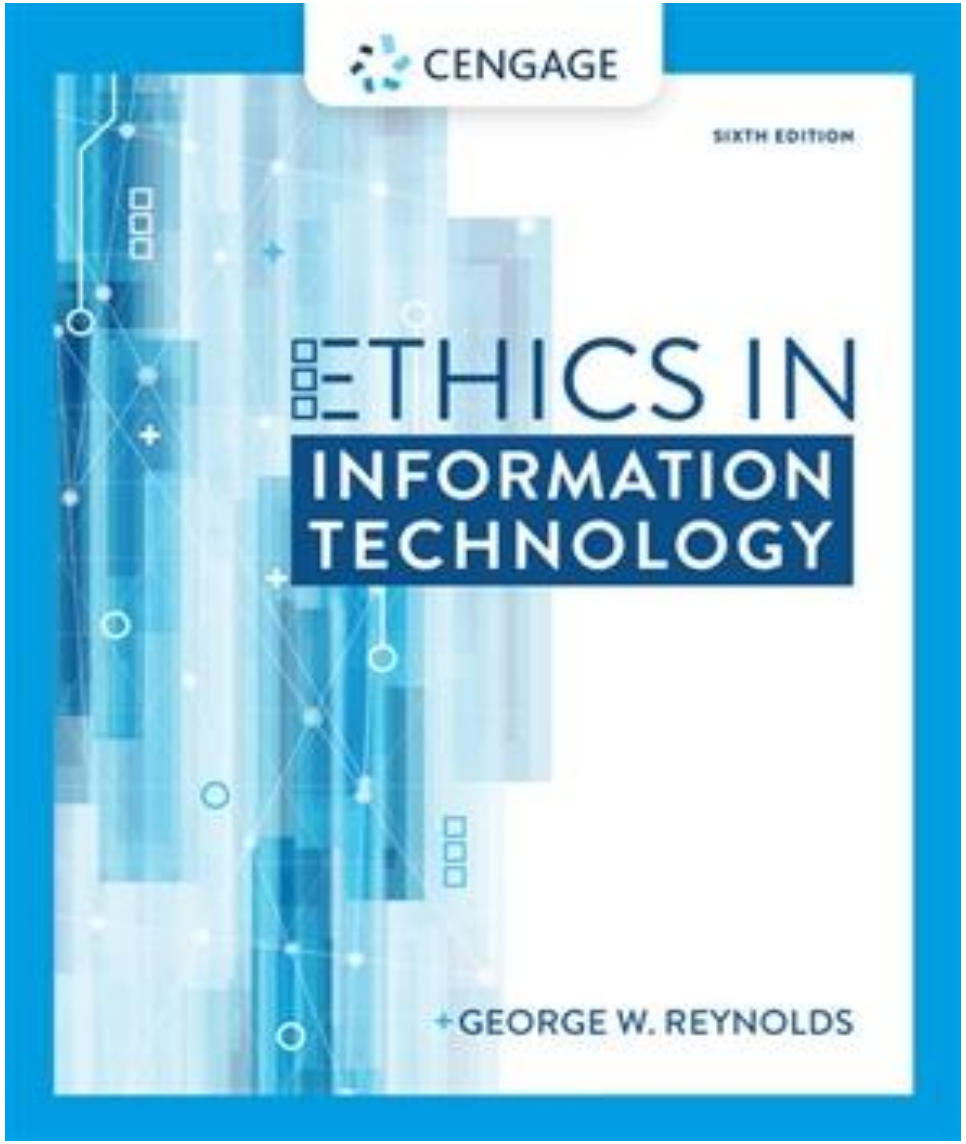
FROM POSSIBILITY TO ACTUALITY

ICT945 Professional Practice in Information Technology

Week 2

Prescribed Text

Reynolds, G. (2018), *Ethics in Information Technology*, 6th Edition, Cengage Learning, Boston, MA



Week 1: Overview of Ethics - Recap

- Ethics Vs Morals Vs Values
- Corporate Social Responsibility (CSR)
- Corporate Code of Ethics and Social Audit
- Ethical Decision-Making Process

Chapter 2

Ethics for IT Workers and IT Users

Learning Objectives

- What relationships must an IT worker manage, and what key ethical issues can arise in each?
- What can be done to encourage the professionalism of IT workers?
- What ethical issues do IT users face, and what can be done to encourage their ethical behavior?

IT Worker Relationships That Must be Managed

- Employers
- Clients
- Suppliers
- Other professionals
- IT users
- Society at large

Relationships Between IT Workers and Employers

Setting and enforcing policies regarding the ethical use of IT

- Employers need to establish clear guidelines on how IT resources should be used ethically.
- This includes policies on internet usage, data privacy, and cybersecurity.

The safeguarding of trade secrets

- IT workers often have access to confidential company data.
- Employers must implement security measures to protect trade secrets and prevent data leaks.

The potential for whistle-blowing

- Employees may witness unethical or illegal practices in their organization.
- Companies should have policies to handle whistle-blowing responsibly, ensuring protection for those who report misconduct.

Ethical Use of IT

- IT staff may actively engage in software piracy or allow it to happen—often to reduce IT-related spending. Example, use cracked version of software.
- Trade groups representing the world's largest IT companies are focused on stopping software piracy:
  - **Software & Information Industry Association (SIIA)**
  - The **Software & Information Industry Association (SIIA)** is a trade association that represents companies involved in software, digital content, and information services.
  - **BSA | The Software Alliance (BSA)**
  - **BSA | The Software Alliance (BSA)** is a global trade group that represents major software companies. It focuses on policy advocacy, intellectual property protection, cybersecurity, and digital trade.

Trade Secrets & Whistle-Blowing

- **Trade secret**: Information that a company has taken strong measures to keep confidential
  - Companies may require employees to sign confidentiality agreements promising not to reveal trade secrets.
- **Whistle-blowing** is the act of reporting unethical, illegal, or improper activities within an organization.
- A **whistleblower** is someone—often an employee, contractor, or insider—who exposes misconduct that could harm the public, customers, employees, or shareholders.

Relationships Between IT Workers and Clients

- Key issues:
  - **Conflict of interest:** A conflict between the IT worker's (or the IT firm's) self-interest and the client's interests
  - **Fraud:** The crime of obtaining goods, services, or property through deception or trickery
  - **Misrepresentation:** The misstatement or incomplete statement of a material fact
  - **Breach of contract:** Occurs when one party fails to meet the terms of a contract
  - **Material breach of contract:** Occurs when a party fails to perform certain obligations, thus, impairing or destroying the essence of the contract

Frequent Causes of Problems in IT Projects

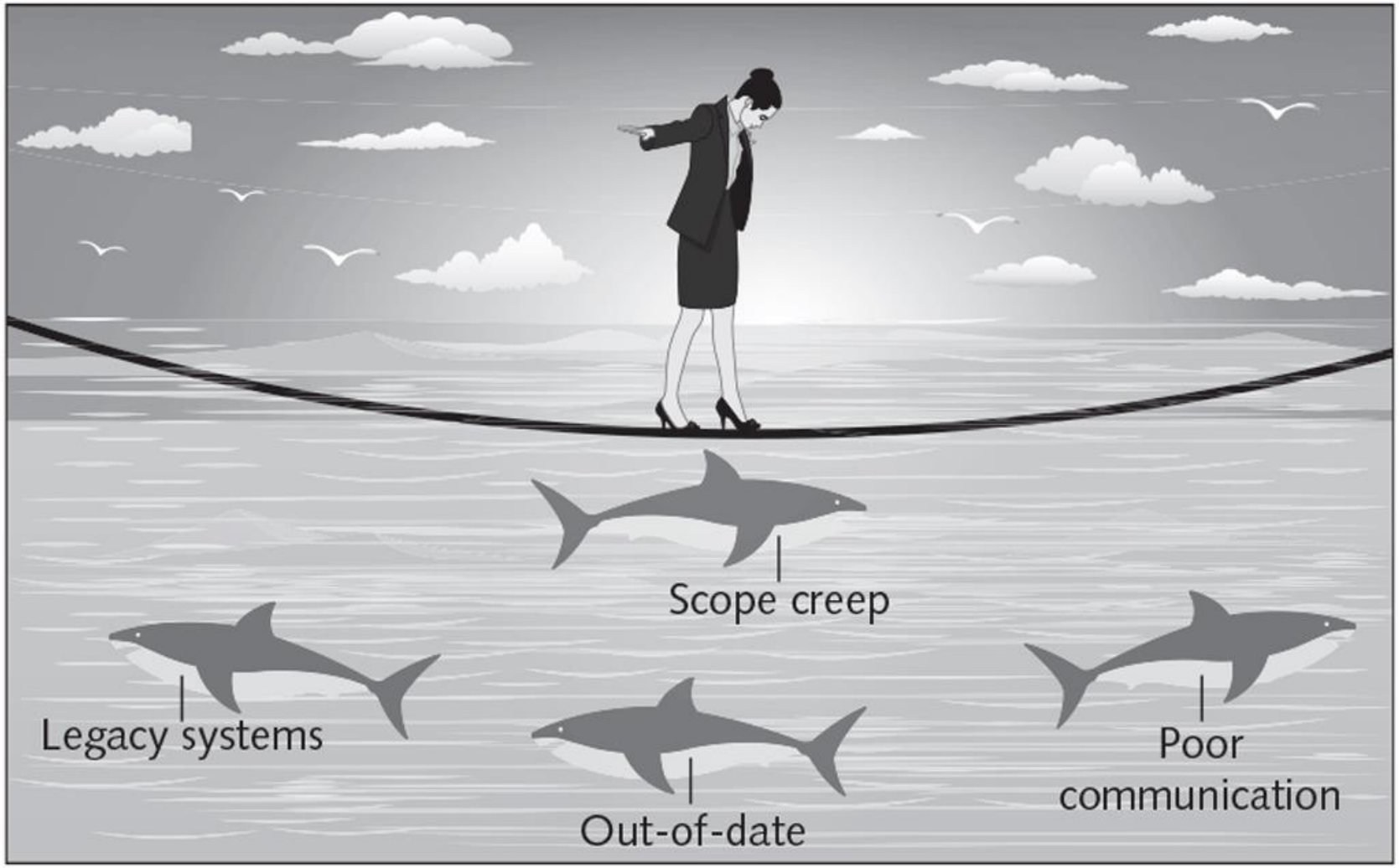


Fig: Frequent causes of problems in IT Projects

Frequent Causes of Problems in IT Projects

- Scope Creep:
  - Changes to the scope of the project or System requirements.
  - Results in cost overruns, missed deadlines and project that fails to meet user expectations
- Poor Communication:
  - Miscommunication or lack of communication between customer and vendor(seller service , or product) can lead to a system performance that does not meet user expectations.
- Delivery of Obsolete solution:
  - Vendor delivers a system that meets expectation, but competitor comes out with a system that is more advanced and useful features.
- Legacy Systems
  - If customer fails to reveal information on legacy systems or databases, implementation can become very difficult

Relationships Between IT Workers and Suppliers

- Key issue:
  - **Bribery**: The act of providing money, property, or favors to obtain a business advantage
    - **Internal control:** The process established to provide reasonable assurance for the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations
      - **Separation of duties:** The act of ensuring that different aspects of processes involving financial transactions are handled by different people

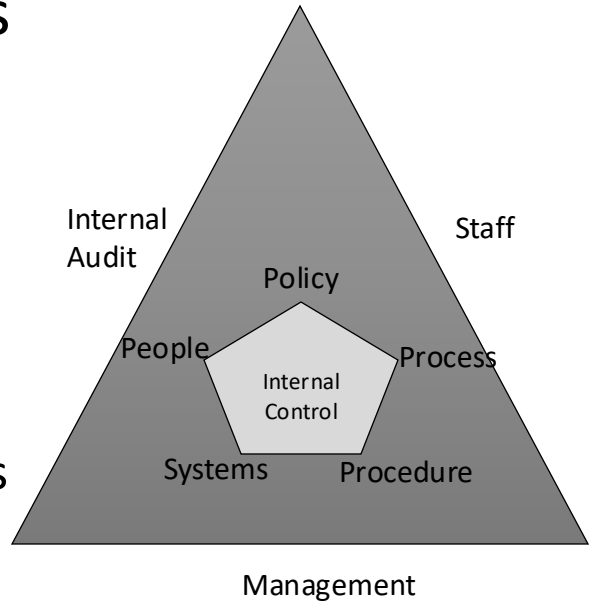


Fig: Internal Control

Relationships Between IT Workers and Suppliers: Internal Control

- **Policies:** Guidelines and standards by which the organization must abide.
  - Usually created as a response to a law
- **Processes:** Collection of tasks designed to accomplish a stated objective
- **Procedure:** Defines exact instructions for completing each task in a process.

- **Management** is responsible for ensuring adequate system of internal control is setup, documented with written procedures, and implemented.
- **Employees** are responsible for following the P&P's**(Policies & Procedures)** , also provide feedback in meetings for continuous improvement.
- **Internal Audit organization** is responsible for assessing whether internal controls have been implemented correctly and functioning as designed.

Fig: Internal Control

Foreign Corrupt Practices Act (FCPA)

- **Foreign Corrupt Practices Act (FCPA):** Makes it a crime to bribe a foreign official, a foreign political party official, or a candidate for foreign political office
  - Applies to any U.S. citizen or company and to any company with shares listed on any U.S. stock exchange
  - FCPA penalties:
    - Corporations: A fine of up to $2 million per violation
    - Individuals: A fine of up to $100,000 and a 5-year prison term

Anti-Bribery Laws in Australia*

- Bribery of foreign public officials
  - Section 70.2 of the Schedule to the Criminal Code.
  - Has the following elements
    - Provide/Offer A Benefit
    - Cause a benefit to be provided/offered
    - Benefit is not legitimately due
    - Intention of influencing a foreign public official to obtain/retain business or business advantage
- Domestic Bribery
- False accounting offences

**Reference: https://www.ashurst.com/en/news-and-insights/legal-updates/anti-bribery-laws-in-australia/*

Distinguishing Between Bribes and Gifts

Bribes	Gifts
Made in secret, as they are neither legally nor morally acceptable	Made openly and publicly, as a gesture of friendship or goodwill
Often made indirectly through a third party	Made directly from donor to recipient
Encourage an obligation for the recipient to act favorably toward the donor	Come with no expectation of a future favor for the donor

Relationships Between IT Workers and Other Professionals

- Professional loyalty
  - Quick to support each other obtain new jobs, but slow to criticize each other in public.
- Professionals owe each other an adherence(commitment) to their profession's code of conduct
  - Experienced professionals can serve as mentors to help develop new members of the profession.

- Key issues:
  - **Résumé inflation:** Lying on a résumé about one's qualifications
  - Inappropriate sharing of corporate information, which may be sold or shared informally with third parties

Relationships Between IT Workers and Society

- Regulatory laws establish safety standards for products and services to protect the public.
  - Laws are not perfect; cannot safeguard against all negative side effects of a product or process.
- Society expects members of a profession to:
  - Provide significant benefits
  - Not cause harm through their actions
- Professional organizations provide codes of ethics to guide IT workers' actions

Summary, Part 1

- **What relationships must an IT worker manage, and what key ethical issues can arise in each?**
  - IT workers and employers:
    - Setting policies regarding the ethical use of IT, safeguarding trade secrets, and whistle-blowing
  - IT workers and clients:
    - Defining and fulfilling each party's responsibilities for successfully completing an IT project
  - IT workers and suppliers:
    - Developing working relationships in which no action can be perceived as unethical
    - Internal control: Assures effectiveness of operations, reliability of financial reporting and compliance; separation of duties

Summary, Part 2

- **What relationships must an IT worker manage, and what key ethical issues can arise in each?**
  - IT workers and other professionals:
  - Mentoring inexperienced colleagues, demonstrating professional loyalty, avoiding résumé inflation, and preventing inappropriate sharing of information
  - IT workers and IT users:
    - Software piracy, inappropriate use of IT resources, and inappropriate sharing of information
  - IT workers and society at large:
    - Practicing the profession in ways that cause no harm and provide benefits to society

Week 3

- Encouraging Professionalism of IT Workers
  - Professional Code of Ethics
  - Professional Organizations
  - Certification
  - Licensing
- Common Ethical Issues for IT Users
- Supporting Ethical Practices of IT Users
  - Acceptable Use Policy (AUP)
  - Compliance

Encouraging the Professionalism of IT Workers

- Characteristics of professionals:
  - Have expertise in the tools and skills needed to do their job
  - Adhere to high ethical and moral standards
  - Produce high-quality results
  - Meet their commitments
  - Communicate effectively
  - Train and develop others with less experience

Improving IT Workers' Reputation for Professionalism

- IT can workers can improve their profession's reputation for professionalism by:
  - Subscribing to a professional code of ethics
  - Joining and participating in professional organizations
  - Obtaining appropriate certifications
  - Supporting government licensing where available

Professional Code of Ethics

- **Professional code of ethics:** A statement of the principles and core values that are essential to the work of a particular occupational group
- A professional code of ethics produces benefits for the individual, the profession, and society as a whole:
  - Ethical decision making
  - High standards of practice and ethical behavior
  - Trust and respect from the general public
  - Evaluation benchmarks

Professional Organizations

- Help IT workers network with others, seek out new ideas, and build on their personal skills and expertise
- Prominent IT-related organizations:
  - Association for Computing Machinery (ACM)
  - Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS)
  - Association of Information Technology Professionals (AITP)
  - SysAdmin, Audit, Network, Security (SANS) Institute

Certification

- **Certification**: A recognition that a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization
  - Obliges an individual to have the prerequisite education and experience, and to pass an exam
  - Certifications from industry associations require a higher level of experience and a broader perspective than vendor certifications
- IT-related certifications may or may not include a requirement to adhere to a code of ethics

Licensing of IT Professionals

- **Government license:** Permission to engage in an activity or to operate a business
- The case for licensing IT workers:
  - Improve information systems
  - Encourage IT workers to follow the highest standards of the profession and practice a code of ethics
  - Without licensing: No well-defined requirements for heightened care and no concept of professional malpractice
- State licensing boards have authority over the specific requirements for licensing in their jurisdiction

Joint Steering Committee for the Establishment of Software Engineering as a Profession

- Joint committee of the ACM and IEEE-CS
- Initial recommendations:
  - Define ethical standards
  - Define the required body of knowledge and recommended practices in software engineering
    - **Body of knowledge:** For a given profession—outlines an agreed-upon set of skills and abilities that all licensed professionals must possess
  - Define appropriate curricula to acquire knowledge

Potential Legal Issues Related to Licensing IT Workers

- **Negligence:** Not doing something that a reasonable person would do or doing something that a reasonable person would not do
- **Duty of care:** The obligation to protect people against unreasonable harm or risk
- **Reasonable person standard:** A standard used by courts to evaluate how an objective, careful, and conscientious person would have acted in the same circumstances
- **Reasonable professional standard:** Used to measure the actions of professionals who have particular expertise or competence

IT Professional Malpractice

- **Breach of the duty of care**: The failure to act as a reasonable person would act
- **Professional malpractice:** The liability of professionals who breach the duty of care, resulting in negligent care and injuries
- Professional negligence can only occur if there are uniform standards against which to compare their professional behavior.

Common Ethical Issues for IT Users

- Software piracy
  - Has a negative impact on future software development
  - Android operating system has contributed to the software piracy problem
- Inappropriate use of computing resources
  - Erodes(reduce) worker productivity and wastes time
  - Could lead to workplace racial/sexual harassment lawsuits
- Inappropriate sharing of information
  - Private personal data: Privacy violation
  - Confidential company data: Could fall into the hands of competitors

Supporting the Ethical Practices of IT Users

- Establish guidelines for the use of company hardware and software
- Define an acceptable use policy (AUP)
- Structure information systems to protect data and information
- Install and maintain a company firewall
  - **Firewall:** Hardware or software that serves as the first line of defense between an organization's network and the Internet; also limits access to the company's network
    based on an Internet-usage policy
- Compliance

Acceptable Use Policy (AUP)

- AUP: Stipulates(identify) restrictions and practices that a user must agree to in order to use organizational computing and network resources
- An effective AUP contains five elements:
  - Purpose
  - Scope
  - Policy
  - Compliance
  - Sanctions
- An organization's information security (infosec) group is responsible for monitoring compliance to the AUP

Manager's Checklist For Establishing an Acceptable Use Policy, Part 1

QUESTION	YES	NO

• Is there a statement that explains the need for an acceptable use policy?
• Is it clear how the policy applies to the following types of workers?
  • Full-time employees
  • Part-time employees
  • Temps
  • Contractors
• Does the policy address the following issues?
  • Protection of the data privacy rights of employees, customers, suppliers, and others
  • Control of access to proprietary company data and information
  • Use of unauthorized or pirated software		

Manager's Checklist For Establishing an Acceptable Use Policy, Part 2

QUESTION	YES	NO

• Does the policy address the following issues? *(continued)*
  • Employee monitoring, including email, wiretapping and eavesdropping on phone conversations, computer monitoring, and surveillance by video
  • Respect of the intellectual rights of others, including trade secrets, copyrights, patents, and trademarks
  • Inappropriate use of IT resources, such as web surfing, excessive use of social networks, blogging, personal emailing, and other use of computers for purposes other than business
  • The need to protect the security of IT resources through adherence to good security practices, such as not sharing user IDs and passwords, using hard-to-guess passwords, and frequently changing passwords		

Manager's Checklist For Establishing an Acceptable Use Policy, Part 3

QUESTION	YES	NO
• Does the policy address the following issues? *(continued)* • The use of the computer to intimidate, harass, or insult others through abusive language in emails and by other means • Are disciplinary actions defined for IT-related abuses? • Is there a process for communicating the policy to employees? • Is there a plan to provide effective, ongoing training relative to the policy?		

Compliance

- **Compliance:** To be in accordance with established policies, guidelines, specifications, or legislation
- Failure to be in compliance with legislation can lead to lawsuits or government fines.
- Demonstrating compliance with multiple government and industry regulations can be challenging.

Audit Committee

- Provides assistance to the board of directors with respect to:
  - Quality and integrity of accounting and reporting practices and controls
  - Compliance with legal and regulatory requirements
  - Qualifications, independence, and performance of the organization’s independent auditor
  - Performance of the company’s internal audit team

Internal Audit Department

- Primary responsibilities:
  - Determine that internal systems and controls are effective
  - Verify existence of company assets and maintain proper safeguards over their protection
  - Measure organization's compliance with its own policies and procedures
  - Ensure that institutional policies and procedures, appropriate laws, and good practices are followed
  - Evaluate adequacy and reliability of information available for management decision making

Summary, Part 1

- **What can be done to encourage the professionalism of IT workers?**
  - Professionals:
    - Possess the skills, good judgment, and work habits expected from a person who has the training and experience to do a job well
    - Contribute to society, participate in lifelong training, and help develop other professionals
  - IT workers can improve their profession's reputation for professionalism:
    - Subscribe to a professional code of ethics
    - Join professional organizations
    - Obtain appropriate certifications
    - Support government licensing

Summary, Part 2

- **What can be done to encourage the professionalism of IT workers?**
  - Professional code of ethics: States the principles and core values essential to the work of a particular occupational group
  - Benefits of a code of ethics: Ethical decision making, high standards of ethical behavior, trust and respect with the general public, and access to an evaluation benchmark for self-assessment
  - IT-related professional organizations with a code of ethics:
    - ACM, IEEE-CS, AITP, and SANS

Summary, Part 3

- **What can be done to encourage the professionalism of IT workers?**
  - Certification and licensing of IT workers:
    - Proponents argue that certification and licensing would increase the reliability and effectiveness of information systems.
    - Certification indicates a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization.
    - Most states support the licensing of software engineers.
    - State licensing boards have responsibility over specific requirements in their jurisdiction.

Summary, Part 4

- **What ethical issues do IT users face, and what can be done to encourage their ethical behavior?**
  - Ethical issues faced by IT users: Software piracy, inappropriate use of computing resources, and inappropriate sharing of data
  - Actions to encourage ethical behavior: Establish guidelines for the use of technology, define an AUP; structure information systems to protect data, maintain a firewall, and ensure compliance
  - The audit committee of a board of directors and the internal audit team: Ensure that the IT organization and IT users are in compliance with organizational policies, laws, and regulations