CHAPTER 2

ETHICS FOR IT WORKERS AND IT USERS

QUOTE

> *This above all: to thine own self be true.*
> —William Shakespeare, playwright

VIGNETTE

New York City Payroll Project Riddled with Fraud

The CityTime project was meant to replace a largely manual, paper-based payroll system for the city of New York (NYC). The goal was to provide a tool that would help city administrators manage a workforce of over 100,000 employees spread across 63 departments. It was also intended to simplify the employee time-reporting process, which was complicated by numerous union timekeeping rules, and to identify employees who tried to fraudulently inflate their paychecks. The project was initiated in 1998 when the city awarded the contract to a subsidiary of MCI, a telecommunications company that later ran into financial scandals and, ultimately, filed for bankruptcy.[1]

In 2001, the CityTime contract was reassigned to Science International Applications Incorporated (SAIC), a defense company. In an unusual move, the handoff to SAIC occurred without the contract going through the normal competitive bidding process required for contracts of this size. Around the same time, Spherion Atlantic Enterprises was hired as a subcontractor to provide quality assurance on the CityTime project, with an initial contract of $3.4 million. The city's contract with Spherion was eventually revised 11 times, with a resulting cost of $48 million.[2]

Richard Valcich, the NYC payroll office executive director during the initial years of the project, accused SAIC of dragging its feet on the project and was skeptical of the company's ability to deliver a quality product. However, Valcich retired in 2004 and was replaced by Joel Bondy, a staunch advocate of the project.[3] In this role, Bondy was responsible for overseeing and re-awarding Spherion's contract. It was later discovered that Bondy worked for Spherion for two years prior to joining the city.

In another questionable move, the CityTime contract was switched from a fixed-price contract to a "time and materials" contract, and the project costs spiraled out of control—from $224 million in 2006 to $628 million by 2009. This switch in the terms of the contract plus lack of project oversight made it even easier for those involved with the project to commit fraud.[4]

At a city hearing in December 2010, Bondy revealed that Spherion employees were billing the city at a rate of $236.25 per hour and that a number of former city employees had become Spherion employees.[5] Mr. Bondy resigned shortly after this meeting.[6]

That same month, federal prosecutors charged several consultants for the CityTime project with a multimillion dollar fraud scheme, which allegedly started in 2005. The consultants were accused of manipulating the city into paying for contracts to businesses that the consultants controlled, and then redirecting part of the money to enrich themselves personally.[7]

In May 2011, federal investigators arrested Gerald Denault, the senior project manager at SAIC, for allegedly receiving over $5 million in kickbacks and for committing wire fraud and money laundering. Denault had convinced his employer to hire TechnoDyne LLC as the main subcontractor for the project. TechnoDyne eventually received $450 million out of the $600 million paid to SAIC and siphoned off millions to a bogus India-based consulting firm owned by Denault.[8] The two owners of TechnoDyne are now fugitives and their whereabouts are unknown. Six other defendants are scheduled to go to trial in 2013.[9]

In March 2012, SAIC agreed to pay $500 million to avoid prosecution for its role in the CityTime scandal; most of that money was to go back to the city of New York. By this time, it was estimated that NYC had paid out $652 million—with an outstanding bill of $41 million—owed on the project, which was originally estimated to cost $63 million and to be completed in 2003.[10]

Questions to Consider

1. What were some early warning signs that signaled things were not going well with the City-Time project?
2. What steps should city managers and SAIC have taken at an early stage of the project to identify and prevent fraud?

LEARNING OBJECTIVES

As you read this chapter, consider the following questions:

1. What key characteristics distinguish a professional from other kinds of workers, and is an IT worker considered a professional?
2. What factors are transforming the professional services industry?
3. What relationships must an IT worker manage, and what key ethical issues can arise in each?
4. How do codes of ethics, professional organizations, certification, and licensing affect the ethical behavior of IT professionals?
5. What is meant by compliance, and how does it help promote the right behaviors and discourage undesirable ones?

IT PROFESSIONALS

A **profession** is a calling that requires specialized knowledge and often long and intensive academic preparation. Over the years, the United States government adopted labor laws and regulations that required a more precise definition of what is meant by a *professional* employee. The United States Code of federal regulations defines a "professional employee" as one who is engaged in the performance of work:

> "(i) requiring knowledge of an advanced type in a field of science or learning customarily acquired by a prolonged course of specialized intellectual instruction and study in an institution of higher learning or a hospital (as distinguished from knowledge acquired by a general academic education, or from an apprenticeship, or from training in the performance of routine mental, manual, mechanical, or physical activities);
> (ii) requiring the consistent exercise of discretion and judgment in its performance;
> (iii) which is predominantly intellectual and varied in character (as distinguished from routine mental, manual, mechanical, or physical work); and
> (iv) which is of such character that the output produced or the result accomplished by such work cannot be standardized in relation to a given period of time."[11]

In other words, professionals such as doctors, lawyers, and accountants require advanced training and experience; they must exercise discretion and judgment in the course of their work; and their work cannot be standardized. Many people would also expect professionals to contribute to society, to participate in a lifelong training program (both formal and informal), to keep abreast of developments in their field, and to assist other professionals in their development. In addition, many professional roles carry special rights and responsibilities. Doctors, for example, prescribe drugs, perform surgery, and request confidential patient information while maintaining doctor–patient confidentiality.

✓ Are IT Workers Professionals?

Many business workers have duties, backgrounds, and training that qualify them to be classified as professionals, including marketing analysts, financial consultants, and IT specialists such as mobile application developers, software engineers, systems analysts, and network administrators. One could argue, however, that not every IT role requires "knowledge of an advanced type in a field of science or learning customarily acquired by a prolonged course of specialized intellectual instruction and study," to quote again from the United States Code. From a *legal* perspective, IT workers are not recognized as professionals because they are not licensed by the state or federal government. This distinction is important, for example, in malpractice lawsuits, as many courts have ruled that IT workers are not liable for malpractice because they do not meet the legal definition of a professional.

✓ Professional Relationships That Must Be Managed

IT workers typically become involved in many different relationships, including those with employers, clients, suppliers, other professionals, IT users, and society at large—as illustrated in Figure 2-1. In each relationship, an ethical IT worker acts honestly and appropriately. These various relationships are discussed in the following sections.

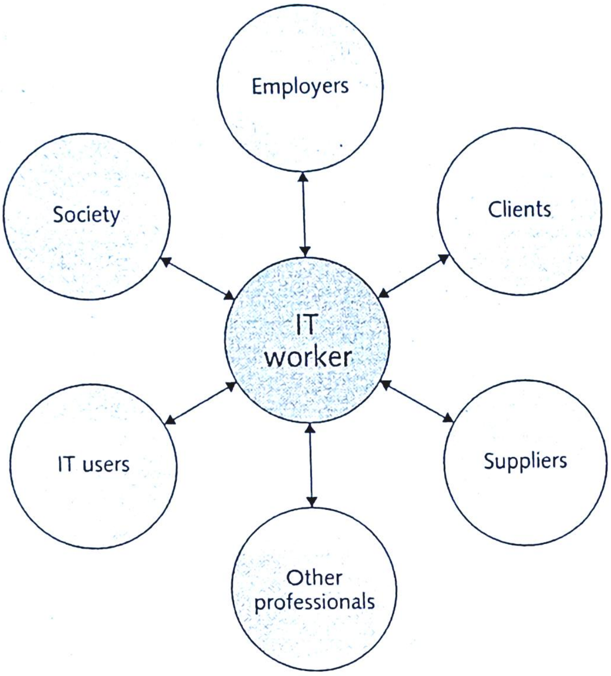

FIGURE 2-1 Professional relationships IT workers must manage
Credit: Course Technology/Cengage Learning.

✓ Relationships Between IT Workers and Employers

IT workers and employers have a critical, multifaceted relationship that requires ongoing effort by both parties to keep it strong. An IT worker and an employer typically agree on fundamental aspects of this relationship before the worker accepts an employment offer. These issues may include job title, general performance expectations, specific work responsibilities, drug-testing requirements, dress code, location of employment, salary, work hours, and company benefits. Many other aspects of this relationship may be addressed in a company's policy and procedures manual or in the company's code of conduct, if one exists. These issues may include protection of company secrets; vacation policy; time off for a funeral or an illness in the family; tuition reimbursement; and use of company resources, including computers and networks.

Other aspects of this relationship develop over time as the need arises (for example, whether the employee can leave early one day if the time is made up another day). Some aspects are addressed by law—for example, an employee cannot be required to do anything illegal, such as falsify the results of a quality assurance test. Some aspects are specific to the role of the IT worker and are established based on the nature of the work or project—for example, the programming language to be used, the type and amount of documentation to be produced, and the extent of testing to be conducted.

As the stewards of an organization's IT resources, IT workers must set an example and enforce policies regarding the ethical use of IT. IT workers often have the skills and knowledge to abuse systems and data or to enable others to do so. Software piracy is an area in which IT workers may be tempted to violate laws and policies. Although end users often get the blame when it comes to using illegal copies of commercial software, software piracy in a corporate setting is sometimes directly traceable to IT staff members—either they allow it to happen or they actively engage in it, often to reduce IT-related spending.

The **Business Software Alliance (BSA)** is a trade group that represents the world's largest software and hardware manufacturers. Its mission is to stop the unauthorized copying of software produced by its members. BSA is funded both through dues based on member companies' software revenues and through settlements from companies that commit piracy. BSA membership includes two dozen or so members such as Adobe, Apple, Intel, McAfee, Microsoft, Symantec, and The Math Works.

More than 100 BSA lawyers and investigators prosecute thousands of cases of software piracy each year. BSA investigations are usually triggered by calls to the BSA hotline (1-888-NO-PIRACY), reports sent to the BSA Web site (*www.nopiracy.org*), and referrals from member companies. Many of these cases are reported by disgruntled employees or former employees. For 2011, the commercial value of software piracy in the United States was estimated to be nearly $10 billion with 31 percent of computer users participating in this illegal activity.[12] When BSA finds cases of software piracy, it assesses heavy monetary penalties.

Failure to cooperate with the BSA can be extremely expensive. The cost of criminal or civil penalties to a corporation and the people involved can easily be many times more expensive than the cost of "getting legal" by acquiring the correct number of software licenses. Software manufacturers can file a civil suit against software pirates with penalties of up to $150,000 per copyrighted work. Furthermore, the government can criminally prosecute violators and fine them up to $250,000, incarcerate them for up to five years, or both.

In 2012, the Alexander Automotive Group paid $325,000 to settle claims that it was using unlicensed Microsoft software on its computers. As part of the settlement agreement with BSA, the firm deleted all unlicensed copies of software from its computers, purchased the licenses required to become compliant, and agreed to implement more effective software management procedures. BSA was alerted to this situation by a report sent to its Web site.[13]

Trade secrecy is another area that can present challenges for IT workers and their employers. A **trade secret** is information, generally unknown to the public, that a company has taken strong measures to keep confidential. It represents something of economic value that has required effort or cost to develop and that has some degree of uniqueness or novelty. Trade secrets can include the design of new software code, hardware designs, business plans, the design of a user interface to a computer program, and manufacturing processes. Examples include the Colonel's secret recipe of 11 herbs and spices used to make the original KFC chicken, the formula for Coke, and Intel's manufacturing process for the i7 quad core processing chip. Employers worry that employees may reveal these secrets to competitors, especially if they leave the company. As a result, companies often require employees to sign confidentiality agreements and promise not to reveal the company's trade secrets.

Zynga is a provider of online social games such as ChefVille, CityVille, FarmVille, FrontierVille, and Zynga Poker that boast over 300 million active monthly users.[14] After just over a year with Zynga, the firm's general manager of CityVille left to become a vice president at Kixeye, a competitor. Zynga claimed that the employee stole files with data critical to the business—including financial projections, marketing plans, and game designs.[15] Zynga filed a request for a temporary restraining order barring its former employee from sharing or copying the information or from engaging in any actions using the information to develop online games employing these trade secrets.

Another issue that can create friction between employers and IT workers is whistle-blowing. **Whistle-blowing** is an effort by an employee to attract attention to a negligent, illegal, unethical, abusive, or dangerous act by a company that threatens the public interest. Whistle-blowers often have special information based on their expertise or position within the offending organization. For example, an employee of a chip manufacturing company may know that the chemical process used to make the chips is dangerous to employees and the general public. A conscientious employee would call the problem to management's attention and try to correct it by working with appropriate resources within the company. But what if the employee's attempt to correct the problem through internal channels was thwarted or ignored? The employee might then consider becoming a whistle-blower and reporting the problem to people outside the company, including state or federal agencies that have jurisdiction. Obviously, such actions could have negative consequences on the employee's job, perhaps resulting in retaliation and firing.

The H-1B visa is a work visa that allows foreigners to come to the United States and work full-time in specialty occupations that require at least a four-year bachelor's degree in a specific field. A U.S. consultant for India-based outsourcing firm Infosys filed a whistle-blower lawsuit against the firm for abusing H-1B program rules. The lawsuit alleged that at a management meeting in Bangalore, Infosys officials discussed the need to "creatively" circumvent the H-1B visa restrictions. The lawsuit further alleged that Infosys brought workers to the United States on B-1 visas (which are intended for workers coming to the United States for short-term work assignments only), but that these workers were assigned full-time jobs. It also claimed that Infosys was not paying the B-1 workers the prevailing wage and was not withholding federal and state income taxes.[16] The whistle-blower filed a separate lawsuit in which he claimed that Infosys retaliated against him for the filing of the visa-related lawsuit by lowering his bonuses, harassing him, and giving him no meaningful work to do.[17]

✓ Relationships Between IT Workers and Clients

IT workers provide services to clients; sometimes those "clients" are coworkers who are part of the same organization as the IT worker. In other cases, the client is part of a different organization. In relationships between IT workers and clients, each party agrees to provide something of value to the other. Generally speaking, the IT worker provides hardware, software, or services at a certain cost and within a given time frame. For example, an IT worker might agree to implement a new accounts payable software package that meets a client's requirements. The client provides compensation, access to key contacts, and perhaps a work space. This relationship is usually documented in contractual terms—who does what, when the work begins, how long it will take, how much the client pays, and so on. Although there is often a vast disparity in technical expertise between IT workers and their clients, the two parties must work together to be successful.

Typically, the client makes decisions about a project on the basis of information, the alternatives, and recommendations provided by the IT worker. The client trusts the IT worker to use his or her expertise and to act in the client's best interests. The IT worker must trust that the client will provide relevant information, listen to and understand what the IT worker says, ask questions to understand the impact of key decisions, and use the information to make wise choices among various alternatives. Thus, the responsibility for decision making is shared between client and IT worker.

One potential ethical problem that can interfere with the relationship between IT workers and their clients involves IT consultants or auditors who recommend their own products and services or those of an affiliated vendor to remedy a problem they have detected. Such a situation has the potential to undermine the objectivity of an IT worker due to a **conflict of interest**—a conflict between the IT worker's (or the IT firm's) self-interest and the interests of the client. For example, an IT consulting firm might be hired to assess a firm's IT strategic plan. After a few weeks of analysis, the consulting firm might provide a poor rating for the existing strategy and insist that its proprietary products and services are required to develop a new strategic plan. Such findings would raise questions about the vendor's objectivity and whether its recommendations can be trusted.

Problems can also arise during a project if IT workers find themselves unable to provide full and accurate reporting of the project's status due to a lack of information, tools, or experience needed to perform an accurate assessment. The project manager may want to keep resources flowing into the project and hope that problems can be corrected before anyone notices. The project manager may also be reluctant to share status information because of contractual penalties for failure to meet the schedule or to develop certain system functions. In such a situation, the client may not be informed about a problem until it has become a crisis. After the truth comes out, finger-pointing and heated discussions about cost overruns, missed schedules, and technical incompetence can lead to charges of fraud, misrepresentation, and breach of contract.

Fraud is the crime of obtaining goods, services, or property through deception or trickery. Fraudulent misrepresentation occurs when a person consciously decides to induce another person to rely and act on a misrepresentation. To prove fraud in a court of law, prosecutors must demonstrate the following elements:

- The wrongdoer made a false representation of material fact.
- The wrongdoer intended to deceive the innocent party.
- The innocent party justifiably relied on the misrepresentation.
- The innocent party was injured.

As an example of alleged fraud, consider the case of Paul Ceglia, who in 2010 sued Facebook claiming to own a majority of the company. Ceglia claimed that he signed a contract with Mark Zuckerberg in 2003 to design and develop the Web site that eventually became Facebook. He alleged that he paid Zuckerberg $1,000 for the programming work and also invested an additional $1,000 in Zuckerberg's Facebook project in exchange for a 50 percent interest in Facebook.[18] Facebook lawyers have asserted that the lawsuit is an outright fraud and have depositions alleging that "Ceglia manufactured evidence, including purported emails with Zuckerberg, to support his false claim to an interest in Facebook" and that "Ceglia destroyed evidence that was inconsistent with his false claim." Facebook's attorneys pointed out that Zuckerberg did not even conceive of Facebook until eight months after Zuckerberg did the contract work (which, they say, was completely unrelated to Facebook) for Ceglia. They further alleged that Ceglia's emails to Zuckerberg were manufactured to support his claims. Eventually, Ceglia was arrested on federal mail and wire fraud charges.[19]

Misrepresentation is the misstatement or incomplete statement of a material fact. If the misrepresentation causes the other party to enter into a contract, that party may have the legal right to cancel the contract or seek reimbursement for damages.

Siri, the voice-activated software that comes with the Apple iPhone, has delighted many iPhone users; however, not everyone has had a positive experience. Shortly after one user in New York purchased an iPhone 4S, he realized that Siri was not performing as expected. When he asked Siri for directions, it did not understand the question or after a long delay gave incorrect directions. As a result, the user filed a lawsuit against Apple claiming that advertising for the Siri amounted to "intentional misrepresentation" and that Apple's claims about the Siri software were "misleading and deceptive." Attorneys for this user are considering turning the case into a class action against Apple.[20]

Breach of contract occurs when one party fails to meet the terms of a contract. Further, a **material breach of contract** occurs when a party fails to perform certain express or implied obligations, which impairs or destroys the essence of the contract. Because there is no clear line between a minor breach and a material breach, determination is made on a case-by-case basis. "When there has been a material breach of contract, the nonbreaching party can either: (1) rescind the contract, seek restitution of any compensation paid under the contract to the breaching party, and be discharged from any further performance under the contract; or (2) treat the contract as being in effect and sue the breaching party to recover damages."[21]

In an out-of-court settlement of a breach of contract lawsuit brought by the General Services Administration (GSA), Oracle Corporation agreed to pay the federal agency $200 million. Oracle entered into a contract with the GSA for the sale of software and technical support to various departments of the federal government. The contract required Oracle to provide the government with its pricing policies. The lawsuit arose when the GSA claimed that Oracle "knowingly failed to meet its contractual obligations to provide GSA with current, accurate, and complete information about its commercial sales practices, including discounts offered to other customers, and that Oracle knowingly made false statements to GSA about its sales practices and discounts." The GSA further claimed that Oracle failed to disclose that other customers received greater discounts than the GSA and that, based on its contract with Oracle, those discounts should have been passed on to the GSA.[22]

When IT projects go wrong because of cost overruns, schedule slippage, lack of system functionality, and so on, aggrieved parties might charge fraud, fraudulent misrepresentation, and/or breach of contract. Trials can take years to settle, generate substantial legal fees, and create bad publicity for both parties. As a result, the vast majority of such disputes are settled out of court, and the proceedings and outcomes are concealed from the public. In addition, IT vendors have become more careful about protecting themselves from major legal losses by requiring that contracts place a limit on potential damages.

Most IT projects are joint efforts in which vendors and customers work together to develop a system. Assigning fault when such projects go wrong can be difficult; one side might be partially at fault, while the other side is mostly at fault. Clients and vendors often disagree about who is to blame in such circumstances. Consider the following frequent causes of problems in IT projects:

- The customer changes the scope of the project or the system requirements.
- Poor communication between customer and vendor leads to performance that does not meet expectations.
- The vendor delivers a system that meets customer requirements, but a competitor comes out with a system that offers more advanced and useful features.
- The customer fails to reveal information about legacy systems or databases that make the new system extremely difficult to implement.

Relationships Between IT Workers and Suppliers

IT workers deal with many different hardware, software, and service providers. Most IT workers understand that building a good working relationship with suppliers encourages the flow of useful communication as well as the sharing of ideas. Such information can lead to innovative and cost-effective ways of using the supplier's products and services that the IT worker may never have considered.

IT workers can develop good relationships with suppliers by dealing fairly with them and not making unreasonable demands. Threatening to replace a supplier who can't deliver needed equipment tomorrow, when the normal industry lead time is one week, is aggressive behavior that does not help build a good working relationship.

Suppliers strive to maintain positive relationships with their customers in order to make and increase sales. To achieve this goal, they may sometimes engage in unethical actions—for example, offering an IT worker a gift that is actually intended as a bribe. Clearly, IT workers should not accept a bribe from a vendor, and they must be careful when considering what constitutes a bribe. For example, accepting invitations to expensive dinners or payment of entry fees for a golf tournament may seem innocent to the recipient, but it may be perceived as bribery by an auditor.

Bribery is the act of providing money, property, or favors to someone in business or government in order to obtain a business advantage. An obvious example is a software supplier sales representative who offers money to another company's employee to get its business. This type of bribe is often referred to as a kickback or a payoff. The person who offers a bribe commits a crime when the offer is made, and the recipient is guilty of a crime if he or she accepts the bribe. Various states have enacted bribery laws, which have sometimes been used to invalidate contracts involving bribes but have seldom been used to make criminal convictions.

A former midlevel supply chain manager at Apple pled guilty in 2011 to taking over $1 million in payments from certain iPhone, iPad, and iPod suppliers in China, Singapore, South Korea, and Taiwan. The kickbacks took place over several years and were in exchange for the employer providing confidential information about Apple's production plans, enabling the suppliers to negotiate more favorable deals with Apple. He now faces 20 years in prison on charges of money laundering, receiving kickbacks, and wire fraud.[23]

The 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. The act applies to any U.S. citizen or company and to any company with shares listed on any U.S. stock exchange. However, a bribe is not a crime if the payment was lawful under the laws of the foreign country in which it was paid. Penalties for violating the FCPA are severe—corporations face a fine of up to $2 million per violation, and individual violators may be fined up to $100,000 and imprisoned for up to five years.

The FCPA also requires corporations whose securities are listed in the United States to meet U.S. accounting standards by having an adequate system of internal controls, including maintaining books and records that accurately and fairly reflect their transactions. The goal of these standards is to prevent companies from using slush funds or other means to disguise payments to foreign officials. A firm's business practices and its accounting information systems must be frequently audited by both internal and outside auditors to ensure that they meet these standards.

The FCPA permits facilitating payments that are made for "routine government actions," such as obtaining permits or licenses; processing visas; providing police protection; providing phone services, power, or water supplies; or facilitating actions of a similar nature. Thus, it is permissible under the FCPA to pay an official to perform some official function faster (for example, to speed customs clearance) but not to make a different substantive decision (for example, to award business to one's firm).[24]

There is growing global recognition of the need to prevent corruption. The United Nations Convention Against Corruption is a legally binding global treaty designed to fight bribery and corruption. During its November 2010 meeting, Finance Ministers and Central Bank Ministers of members of the Group of 20 (G20), which includes Argentina, China, India, Japan, Russia, the United Kingdom, the United States, and 13 other countries, pledged to implement this treaty effectively. In particular, the countries pledged to put in place mechanisms for the recovery of property from corrupt officials through international cooperation in tracing, freezing, and confiscating assets. Members also pledged to adopt and enforce laws against international bribery and put in place rules to protect whistle-blowers.[25]

In some countries, gifts are an essential part of doing business. In fact, in some countries, it would be considered rude not to bring a present to an initial business meeting. In the United States, a gift might take the form of free tickets to a sporting event from a personnel agency that wants to get on your company's list of preferred suppliers. But, at what point does a gift become a bribe, and who decides?

The key distinguishing factor is that no gift should be hidden. A gift may be considered a bribe if it is not declared. As a result, most companies require that all gifts be declared and that everything but token gifts be declined. Some companies have a policy of pooling the gifts received by their employees, auctioning them off, and giving the proceeds to charity.

When it comes to distinguishing between bribes and gifts, the perceptions of the donor and the recipient can differ. The recipient may believe he received a gift that in no way obligates him to the donor, particularly if the gift was not cash. The donor's intentions, however, might be very different. Table 2-1 shows some distinctions between bribes and gifts.

TABLE 2-1 Distinguishing between bribes and gifts

Bribes	Gifts
Are made in secret, as they are neither legally nor morally acceptable	Are made openly and publicly, as a gesture of friendship or goodwill
Are often made indirectly through a third party	Are 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

Source Line: Course Technology/Cengage Learning.

Relationships Between IT Workers and Other Professionals

Professionals often feel a degree of loyalty to the other members of their profession. As a result, they are often quick to help each other obtain new positions but slow to criticize each other in public. Professionals also have an interest in their profession as a whole, because how it is perceived affects how individual members are viewed and treated. (For example, politicians are not generally thought to be very trustworthy, but teachers are.) Hence, professionals owe each other an adherence to the profession's code of conduct. Experienced professionals can also serve as mentors and help develop new members of the profession.

A number of ethical problems can arise among members of the IT profession. One of the most common is **résumé inflation**, which involves lying on a résumé by, for example, claiming competence in an IT skill that is in high demand. Even though an IT worker might benefit in the short term from exaggerating his or her qualifications, such an action can hurt the profession and the individual in the long run. Many employers consider lying on a résumé as grounds for immediate dismissal.

Yahoo! hired Scott Thompson, the president of eBay's PayPal electronic payments unit, as its new CEO in January 2012.[26] Just four months later, Thompson left the company, due, at least in part, to revelations that his résumé falsely claimed that he had earned a bachelor's degree in computer science.[27]

Some studies have shown that around 30 percent of all U.S. job applicants exaggerate their accomplishments, while roughly 10 percent "seriously misrepresent" their backgrounds.[28] Résumé inflation is an even bigger problem in Asia. According to a recent survey conducted by the University of Hong Kong and a Hong Kong–based company specializing in preemployment screening, over 62 percent of respondents confessed to exaggerating their years of experience, previous positions held, and job responsibilities; 33 percent confessed to having exaggerated even more.[29] Table 2-2 lists the areas of a résumé that are most prone to exaggeration.

TABLE 2-2 Most frequent areas of résumé falsehood or exaggeration

Area of exaggeration	How to uncover the truth
Dates of employment	Thorough reference check
Job title	Thorough reference check
Criminal record	Criminal background check
Inflated salary	Thorough reference check
Education	Verification of education claims with universities and other training organizations
Professional licenses	Verification of license with accrediting agency
Working for fictitious company	Thorough background check

Source Line: Lisa Vaas, "Most Common Resume Lies," The Ladders, July 17, 2009, www.theladders.com/career-advice/most-common-resume-lies.

Another ethical issue that can arise in relationships between IT workers and other professionals is the inappropriate sharing of corporate information. Because of their roles, IT workers may have access to corporate databases of private and confidential information about employees, customers, suppliers, new product plans, promotions, budgets, and so on. It might be sold to other organizations or shared informally during work conversations with others who have no need to know.

Relationships Between IT Workers and IT Users

The term **IT user** refers to a person who uses a hardware or software product; the term distinguishes end users from the IT workers who develop, install, service, and support the product. IT users need the product to deliver organizational benefits or to increase their productivity.

IT workers have a duty to understand a user's needs and capabilities and to deliver products and services that best meet those needs—subject, of course, to budget and time constraints. IT workers also have a key responsibility to establish an environment that supports ethical behavior by users. Such an environment discourages software piracy, minimizes the inappropriate use of corporate computing resources, and avoids the inappropriate sharing of information.

Relationships Between IT Workers and Society

Regulatory laws establish safety standards for products and services to protect the public. However, these laws are less than perfect, and they cannot safeguard against all negative side effects of a product or process. Often, professionals can clearly see the effect their work will have and can take action to eliminate potential public risks. Thus, society expects members of a profession to provide significant benefits and to not cause harm through their actions. One approach to meeting this expectation is to establish and maintain professional standards that protect the public.

Clearly, the actions of an IT worker can affect society. For example, a systems analyst may design a computer-based control system to monitor a chemical manufacturing process. A failure or an error in the system may put workers or residents near the plant at risk. As a result, IT workers have a relationship with members of society who may be affected by their actions. There is currently no single, formal organization of IT workers that takes responsibility for establishing and maintaining standards that protect the public. However, as discussed in the following sections, there are a number of professional organizations that provide useful professional codes of ethics to guide actions that support the ethical behavior of IT workers.

Professional Codes of Ethics

A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group. Practitioners in many professions subscribe to a code of ethics that governs their behavior. For example, doctors adhere to varying versions of the 2,000-year-old Hippocratic oath, which medical schools offer as an affirmation to their graduating classes. Most codes of ethics created by professional organizations have two main parts: The first outlines what the organization aspires to become, and the second typically lists rules and principles by which members of the organization are expected to abide. Many codes also include a commitment to continuing education for those who practice the profession.

Laws do not provide a complete guide to ethical behavior. Just because an activity is not defined as illegal does not mean it is ethical. Nor can a professional code of ethics be expected to provide an answer to every ethical dilemma—no code can be a definitive collection of behavioral standards. However, following a professional code of ethics can produce many benefits for the individual, the profession, and society as a whole:

- *Ethical decision making*—Adherence to a professional code of ethics means that practitioners use a common set of core values and beliefs as a guideline for ethical decision making.
- *High standards of practice and ethical behavior*—Adherence to a code of ethics reminds professionals of the responsibilities and duties that they may be tempted to compromise to meet the pressures of day-to-day business. The code also defines acceptable and unacceptable behaviors to guide professionals in their interactions with others. Strong codes of ethics have procedures for censuring professionals for serious violations, with penalties that can include the loss of the right to practice. Such codes are the exception, however, and few exist in the IT arena.
- *Trust and respect from the general public*—Public trust is built on the expectation that a professional will behave ethically. People must often depend on the integrity and good judgment of a professional to tell the truth, abstain from giving self-serving advice, and offer warnings about the potential negative side effects of their actions. Thus, adherence to a code of ethics enhances trust and respect for professionals and their profession.
- *Evaluation benchmark*—A code of ethics provides an evaluation benchmark that a professional can use as a means of self-assessment. Peers of the professional can also use the code for recognition or censure.

Professional Organizations

No one IT professional organization has emerged as preeminent, so there is no universal code of ethics for IT workers. However, the existence of such organizations is useful in a field that is rapidly growing and changing. In order to stay on top of the many new developments in their field, IT workers need to network with others, seek out new ideas, and continually build on their personal skills and expertise. Whether you are a freelance programmer or the CIO of a *Fortune* 500 company, membership in an organization of IT workers enables you to associate with others of similar work experience, develop working relationships, and exchange ideas. These organizations disseminate information through email, periodicals, Web sites, meetings, and conferences. Furthermore, in recognition of the need for professional standards of competency and conduct, many of these organizations have developed codes of ethics. Four of the most prominent IT-related professional organizations are highlighted in the following sections.

Association for Computing Machinery (ACM)

The Association for Computing Machinery (ACM) is a computing society founded in 1947 with over 97,000 student and professional members in more than 100 countries. It is international in scope—with an ACM Europe, ACM India, and ACM China organization. ACM currently publishes over 50 journals and magazines and 30 newsletters—including *Communications of the ACM* (ACM's primary publication), *ACM Tech News* (coverage of timely topics for IT professionals), *XRDS* (for both graduate and undergraduate students considering computing careers), *RISKS Forum* (a moderated dialogue on risks to the public from computers and related systems), and *eLearn* (an online magazine about online education and training). The organization also offers a substantial digital library of bibliographic information, citations, articles, and journals. The ACM sponsors 37 special-interest groups (SIGs) representing major areas of computing. Each group provides publications, workshops, and conferences for information exchange.[30]

Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS)

1(a)

The Institute of Electrical and Electronics Engineers (IEEE) covers the broad fields of electrical, electronic, and information technologies and sciences. The IEEE-CS is one of the oldest and largest IT professional associations, with about 85,000 members. Founded in 1946, the IEEE-CS is the largest of the 38 societies of the IEEE. The IEEE-CS helps meet the information and career development needs of computing researchers and practitioners with technical journals, magazines, books, conferences, conference publications, and online courses. It also offers a Certified Software Development Professional (CSDP) program for experienced professionals and a Certified Software Development Associate (CSDA) credential for recent college graduates. The society sponsors many conferences, applications-related and research-oriented journals, local and student chapters, technical committees, and standards working groups.[31]

In 1993, the ACM and IEEE-CS formed a Joint Steering Committee for the Establishment of Software Engineering as a Profession. The initial recommendations of the committee were to define ethical standards, to define the required body of knowledge and recommended practices in software engineering, and to define appropriate curricula to acquire knowledge. The "Software Engineering Code of Ethics and Professional Practice" documents the ethical and professional responsibilities and obligations of software engineers. After a thorough review process, version 5.2 of the Software Engineering Code of Ethics was adopted by both the ACM and IEEE-CS in 1999.[32]

Association of Information Technology Professionals (AITP)

The Association of Information Technology Professionals (AITP) started in Chicago in 1951, when a group of machine accountants got together and decided that the future was bright for the IBM punched-card tabulating machines they were operating—a precursor of the modern electronic computer. They were members of a local group called the Machine Accountants Association (MAA), which first evolved into the Data Processing Management Association in 1962 and finally the AITP in 1996.[33]

The AITP provides IT-related seminars and conferences, information on IT issues, and forums for networking with other IT workers. Its mission is to provide superior leadership and education in information technology, and one of its goals is to help members make themselves more marketable within their industry. The AITP also has a code of ethics and standards of conduct. The standards of conduct are considered to be rules that no true IT professional should violate.

SysAdmin, Audit, Network, Security (SANS) Institute

The SysAdmin, Audit, Network, Security (SANS) Institute provides information security training and certification for a wide range of individuals, such as auditors, network administrators, and security managers. Each year, its programs train some 12,000 people, and a total of more than 165,000 security professionals around the world have taken one or more of its courses. SANS publishes a semiweekly news digest (NewsBites), a weekly security vulnerability digest (@Risk), and flash security alerts.[34]

At no cost, SANS makes available a collection of some 1,200 research documents about various topics of information security. SANS also operates Internet Storm Center—a program that monitors malicious Internet activity and provides a free early warning service to Internet users—and works with Internet service providers to thwart malicious attackers.

Table 2-3 provides the URL for the codes of ethics for the above IT professional organizations.

TABLE 2-3 Code of ethics for popular IT professional organizations

Organization	URL for code of ethics
Association for Computing Machinery	www.acm.org/about/code-of-ethics
Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS)	http://seeri.etsu.edu/Codes/TheSECode.htm
Association of Information Technology Professionals (AITP)	www.aitp.org/?page=Ethics
SysAdmin, Audit, Network, Security (SANS) Institute	www.sans.org/security-resources/ethics.php

Source Line: Course Technology/Cengage Learning.

Certification

Certification indicates that a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization. Unlike licensing, which applies only to people and is required by law, certification can also apply to products (e.g., the Wi-Fi CERTIFIED logo assures that the product has met rigorous interoperability testing to ensure that it will work with other Wi-Fi-certified products) and is generally voluntary. IT-related certifications may or may not include a requirement to adhere to a code of ethics, whereas such a requirement is standard with licensing.

Numerous companies and professional organizations offer certifications, and opinions are divided on their value. Many employers view them as a benchmark that indicates mastery of a defined set of basic knowledge. On the other hand, because certification is no substitute for experience and doesn't guarantee that a person will perform well on the job, some hiring managers are rather cynical about the value of certifications. Most IT employees are motivated to learn new skills, and certification provides a structured way of doing so. For such people, completing a certification provides clear recognition and correlates with a plan to help them continue to grow and advance in their careers. Others view certification as just another means for product vendors to generate additional revenue with little merit attached.

Deciding on the best IT certification—and even whether to seek a certification—depends on the individual's career aspirations, existing skill level, and accessibility to training. Is certification relevant to your current job or the one to which you aspire? Does the company offering the certification have a good reputation? What is the current and potential future demand for skills in this area of certification?

Vendor Certifications

Many IT vendors—such as Cisco, IBM, Microsoft, SAP, and Oracle—offer certification programs for those who use their products. Workers who successfully complete a program can represent themselves as certified users of a manufacturer's product. Depending on the job market and the demand for skilled workers, some certifications might substantially improve an IT worker's salary and career prospects. Certifications that are tied to a vendor's product are relevant for job roles with very specific requirements or certain aspects of broader roles. Sometimes, however, vendor certifications are too narrowly focused on the technical details of the vendor's technology and do not address more general concepts.

To become certified, one must pass a written exam. Because of legal concerns about whether other types of exams can be graded objectively, most exams are presented in a multiple-choice format. A few certifications, such as the Cisco Certified Internetwork Expert (CCIE) certification, also require a hands-on lab exam that demonstrates skills and knowledge. It can take years to obtain the necessary experience required for some certifications. Courses and training material are available to help speed up the preparation process, but such support can be expensive. Depending on the certification, study materials can cost $1,000 or more, and in-class formal training courses often cost more than $10,000.

Industry Association Certifications

There are many available industry certifications in a variety of IT-related subject areas. Their value varies greatly depending on where people are in their career path, what other certifications they possess, and the nature of the IT job market. Table 2-4 lists several of the certifications most in demand by employers.

TABLE 2-4 Certifications in high demand

Certification	Subject matter
Microsoft Certified Technology Specialist	Designing and optimizing solutions based on Microsoft products and technologies
Cisco Certified Internetwork Expert	Managing and troubleshooting large networks
Cisco Certified Network Professional Security	Configuring and designing firewalls and the security settings on routers and switches
CompTIA A+	Performing computer and network maintenance, troubleshooting, and installation—including addressing security issues
Project Management Institute's Project Management Professional (PMP)	Leading and directing projects

Source Line: Course Technology/Cengage Learning.

Certification requirements generally oblige an individual to have the prerequisite education and experience, and to sit for and pass an exam. In order to remain certified, the individual must typically pay an annual certification fee, earn continuing education credits, and—in some cases—pass a periodic renewal test.

Certifications from industry associations generally require a higher level of experience and a broader perspective than vendor certifications; however, industry associations often lag in developing tests that cover new technologies. The trend in IT certification is to move from purely technical content to a broader mix of technical, business, and behavioral competencies, which are required in today's demanding IT roles. This trend is evident in industry association certifications that address broader roles, such as project management and network security.

* Government Licensing

In the United States, a **government license** is government-issued permission to engage in an activity or to operate a business. It is generally administered at the state level and often requires that the recipient pass a test of some kind. Some professionals must be licensed, including certified public accountants (CPAs), lawyers, doctors, various types of medical and daycare providers, and some engineers.

States have enacted legislation to establish licensing requirements and protect public safety in a variety of fields. For example, Texas passed the Engineering Registration Act after a tragic school explosion at New London, Texas, in 1937. Under the act and subsequent revisions, only duly licensed people may legally perform engineering services for the public, and public works must be designed and constructed under the direct supervision of a licensed professional engineer. People cannot call themselves engineers or professional engineers unless they are licensed, and violators are subject to legal penalties. Most states have similar laws.

The Case for Licensing IT Workers

The days of simple, stand-alone information systems are over. Modern systems are highly complex, interconnected, and critically dependent on one another. Highly integrated enterprise resource planning (ERP) systems help multibillion-dollar companies control all of their business functions, including forecasting, production planning, purchasing, inventory control, manufacturing, and distribution. Complex computers and information systems manage and control the nuclear reactors of power plants that generate electricity. Medical information systems monitor the vital statistics of hospital patients on critical life support. Every year, local, state, and federal government information systems are entrusted with generating and distributing millions of checks worth billions of dollars to the public.

As a result of the increasing importance of IT in our everyday lives, the development of reliable, effective information systems has become an area of mounting public concern. This concern has led to a debate about whether the licensing of IT workers would improve information systems. Proponents argue that licensing would strongly encourage IT workers to follow the highest standards of the profession and practice a code of ethics. Licensing would also allow for violators to be punished. Without licensing, there are no clear, well-defined requirements for heightened care and no concept of professional malpractice.

Issues Associated with Government Licensing of IT Workers

Australia, Great Britain, and the Canadian provinces of Ontario and British Columbia have adopted licensing for software engineers. In the United States, the National Council of Examiners for Engineering and Surveying (NCEES) has developed a professional exam for electrical engineers and computer engineers. However, there are many reasons why there are few international or national licensing programs for IT workers in the United States:

- *There is no universally accepted core body of knowledge*. The core **body of knowledge** for any profession outlines agreed-upon sets of skills and abilities that all licensed professionals must possess. At present, however, there are no universally accepted standards for licensing programmers, software engineers, and other IT workers. Instead, various professional societies, state agencies, and federal governments have developed their own standards.
- *It is unclear who should manage the content and administration of licensing exams*. How would licensing exams be constructed, and who would be responsible for designing and administering them? Would someone who passes a license exam in one state or country be accepted in another state or country? In a field as rapidly changing as IT, workers must commit to ongoing, continuous education. If an IT worker's license were to expire every few years (like a driver's license), how often would practitioners be required to prove competence in new practices in order to renew their license? Such

Inappropriate Use of Computing Resources

Some employees use their computers to surf popular Web sites that have nothing to do with their jobs, participate in chat rooms, view pornographic sites, and play computer games. These activities eat away at worker productivity and waste time. Furthermore, activities such as viewing sexually explicit material, sharing lewd jokes, and sending hate email could lead to lawsuits and allegations that a company allowed a work environment conducive to racial or sexual harassment. A survey by the Fawcett Society found that one in five men admit to viewing porn at work, while a separate study found that 30 percent of mobile workers are viewing porn on their Web-enabled phones.[36,37] Organizations typically fire frequent pornography offenders and take disciplinary action against less egregious offenders.

Recently, the executive director of the Pentagon's Missile Defense Agency issued a memo to its 8,000 employees warning them to stop using their work computers to access Internet porn sites. One concern of government officials is that many pornography sites are infected with computer viruses and other malware; criminals and foreign intelligence agencies often use such sites as a means to gain access to government and corporate computer networks. For example, a foreign agent can embed malware capable of stealing data or opening computer communications ports whenever certain photos or videos are downloaded to a computer.[38]

Inappropriate Sharing of Information

Every organization stores vast amounts of information that can be classified as either private or confidential. Private data describes individual employees—for example, their salary information, attendance data, health records, and performance ratings. Private data also includes information about customers—credit card information, telephone number, home address, and so on. Confidential information describes a company and its operations, including sales and promotion plans, staffing projections, manufacturing processes, product formulas, tactical and strategic plans, and research and development. An IT user who shares this information with an unauthorized party, even inadvertently, has violated someone's privacy or created the potential that company information could fall into the hands of competitors. For example, if an employee accessed a coworker's payroll records via a human resources computer system and then discussed them with a friend, it would be a clear violation of the coworker's privacy.

In late 2010, hundreds of thousands of leaked State Department documents were posted on the WikiLeaks Web site. As of this writing, it appears that the source of the leaks was a low-level IT user (an Army private) with access to confidential documents. The documents revealed details of behind-the-scenes international diplomacy, often divulging candid comments from world leaders and providing particulars of U.S. tactics in Afghanistan, Iran, and North Korea.[39] The leaked documents strained relations between the United States and some of its allies. It is also possible that the incident will lead to less sharing of sensitive information with the United States because of concerns over further disclosures.

Supporting the Ethical Practices of IT Users

The growing use of IT has increased the potential for new ethical issues and problems; thus, many organizations have recognized the need to develop policies that protect against abuses. Although no policy can stop wrongdoers, it can set forth the general rights and responsibilities of all IT users, establish boundaries of acceptable and unacceptable behavior, and enable management to punish violators. Adherence to a policy can improve services to users, increase productivity, and reduce costs. Companies can take several of the following actions when creating an IT usage policy.

Establishing Guidelines for Use of Company Software

Company IT managers must provide clear rules that govern the use of home computers and associated software. Some companies negotiate contracts with software manufacturers and provide PCs and software so that IT users can work at home. Other companies help employees buy hardware and software at corporate discount rates. The goal should be to ensure that employees have legal copies of all the software they need to be effective, regardless of whether they work in an office, on the road, or at home.

Defining the Appropriate Use of IT Resources

Companies must develop, communicate, and enforce written guidelines that encourage employees to respect corporate IT resources and use them to enhance their job performance. Effective guidelines allow some level of personal use while prohibiting employees from visiting objectionable Internet sites or using company email to send offensive or harassing messages.

Structuring Information Systems to Protect Data and Information

Organizations must implement systems and procedures that limit data access to just those employees who need it. For example, sales managers may have total access to sales and promotion databases through a company network, but their access should be limited to products for which they are responsible. Furthermore, they should be prohibited from accessing data about research and development results, product formulas, and staffing projections if they don't need it to do their jobs.

Installing and Maintaining a Corporate Firewall

A **firewall** is hardware or software that serves as a barrier between an organization's network and the Internet; a firewall also limits access to the company's network based on the organization's Internet-usage policy. A firewall can be configured to serve as an effective deterrent to unauthorized Web surfing by blocking access to specific objectionable Web sites. (Unfortunately, the number of such sites is continually growing, so it is difficult to block them all.) A firewall can also serve as an effective barrier to incoming email from certain Web sites, companies, or users. It can even be programmed to block email with certain kinds of attachments (for example, Microsoft Word documents), which reduces the risk of harmful computer viruses.

Table 2-5 provides a manager's checklist for establishing an IT usage policy. The preferred answer to each questions is *yes*.

TABLE 2-5 Manager's checklist for establishing an IT usage policy

Question	Yes	No
Is there a statement that explains the need for an IT usage policy?		
Does the policy provide a clear set of guiding principles for ethical decision making?		
Is it clear how the policy applies to the following types of workers? • Employees • Part-time workers • 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 • 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, 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 • 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?		
Has a corporate firewall been implemented?		
Is the corporate firewall maintained and kept up to date?		

Source Line: Course Technology/Cengage Learning.

Compliance

Compliance means to be in accordance with established policies, guidelines, specifications, or legislation. Records management software, for example, may be developed in compliance with the U.S. Department of Defense's Design Criteria Standard for Electronic Management Software applications (known as *DoD 5015*) that defines mandatory functional requirements for records management software used within the Department of Defense. Commercial software used within an organization should be distributed in compliance with the vendor's licensing agreement.

In the legal system, compliance usually refers to behavior in accordance with legislation—such as the Sarbanes–Oxley Act of 2002, which established requirements for internal controls to govern the creation and documentation of accurate and complete financial statements, or the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), which requires employers to ensure the security and privacy of employee healthcare data. Failure to be in compliance to specific pieces of legislation can lead to criminal or civil penalties specified in that legislation.

Failure to be in compliance with legislation can also lead to lawsuits or government fines. For instance, the California Online Privacy Protection Act of 2003 requires "commercial operators of online services, including mobile and social apps, which collect personally identifiable information from Californians, to conspicuously post a privacy policy," according to the California Attorney General's office. Such a policy must outline what data is gathered, for what purposes the data is being collected, and with whom the data may be shared. Developers of mobile applications face fines of up to $2,500 for every noncompliant application that is downloaded. Several organizations, including Delta, United Airlines, and Open Table, were notified by the Attorney General's office in late 2012 that they were not in compliance and were given 30 days to provide specific plans and a timeline for becoming compliant with the law.[40]

Demonstrating compliance with multiple government and industry regulations, many with similar but sometimes conflicting requirements, can be a major challenge. As a result, many organizations have implemented specialized software to track and record compliance actions, hired management consultants to provide advice and training, and even created a new position, the chief compliance officer (CCO), to deal with the issues.

In 1972, the Securities and Exchange Commission (SEC) recommended that publicly held organizations establish audit committees.[41] The **audit committee** of a board of directors provides assistance to the board in fulfilling its responsibilities with respect to the oversight of the following areas of activity:

- The quality and integrity of the organization's accounting and reporting practices and controls, including the financial statements and reports
- The organization's compliance with legal and regulatory requirements
- The qualifications, independence, and performance of the company's independent auditor (a certified public accountant who provides a company with an accountant's opinion but who is not otherwise associated with the company)
- The performance of the company's internal audit team

In some cases, audit committees have uncovered violations of law and reported their findings to appropriate law enforcement agencies. For example, the audit committee of Sensata Technology (which designs, manufactures, and distributes electronic sensors and controls) conducted an investigation into whether certain company officials had violated foreign bribery laws in connection with a business deal in China. As a result of that investigation, the audit committee reported possible Foreign Corrupt Practices Act violations to the SEC and the Department of Justice.[42]

In addition to an audit committee, most organizations also have an internal audit department whose primary responsibilities are to

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

Although the members of the internal audit team are not typically experts in detecting and investigating financial statement fraud, they can offer advice on how to develop and test policies and procedures that result in transactions being recorded in accordance with generally accepted accounting principles (GAAP). This can go a long way toward deterring fraud related to an organization's financial statements. Quite often in cases of financial statement fraud, senior management (including members of the audit committee) ignored or tried to suppress the recommendations of the internal audit team, especially when red flags were raised.

The audit committee and members of the internal audit team have a major role in ensuring that both the IT organization and IT users are in compliance with the various organizational guidelines and policies as well as various legal and regulatory practices.

Summary

- The key characteristics that distinguish professionals from other kinds of workers are as follows: (1) They require advanced training and experience; (2) they must exercise discretion and judgment in the course of their work; and (3) their work cannot be standardized.
- A professional is expected to contribute to society, to participate in a lifelong training program, to keep abreast of developments in the field, and to help develop other professionals.
- From a legal standpoint, a professional has passed the state licensing requirements (if they exist) and earned the right to practice there.
- From a legal perspective, IT workers are not recognized as professionals because they are not licensed by the state or federal government. As a result, IT workers are not liable for malpractice.
- IT professionals typically become involved in many different relationships, each with its own set of ethical issues and potential problems.
- In relationships between IT professionals and employers, important issues include setting and enforcing policies regarding the ethical use of IT, the potential for whistle-blowing, and the safeguarding of trade secrets.
- In relationships between IT professionals and clients, key issues revolve around defining, sharing, and fulfilling each party's responsibilities for successfully completing an IT project.
- A major goal for IT professionals and suppliers is to develop good working relationships in which no action can be perceived as unethical.
- In relationships between IT workers, the priority is to improve the profession through activities such as mentoring inexperienced colleagues and demonstrating professional loyalty.
- Résumé inflation and the inappropriate sharing of corporate information are potential problems in relationships between IT workers.
- In relationships between IT professionals and IT users, important issues include software piracy, inappropriate use of IT resources, and inappropriate sharing of information.
- When it comes to the relationship between IT workers and society at large, the main challenge for IT workers is to practice the profession in ways that cause no harm to society and provide significant benefits.
- A professional code of ethics states the principles and core values that are essential to the work of an occupational group.
- A code of ethics serves as a guideline for ethical decision making, promotes high standards of practice and ethical behavior, enhances trust and respect from the general public, and provides an evaluation benchmark.
- Several IT-related professional organizations have developed a code of ethics, including ACM, IEEE-CS, AITP, and SANS.
- Codes of ethics usually have two main parts—the first outlines what the organization aspires to become, and the second typically lists rules and principles that members are expected to live by. The codes also typically include a commitment to continuing education for those who practice the profession.

- Many people believe that the licensing and certification of IT workers would increase the reliability and effectiveness of information systems.
- Licensing and certification raise many issues, including the following: (1) There is no universally accepted core body of knowledge on which to test people; (2) it is unclear who should manage the content and administration of licensing exams; (3) there is no administrative body to accredit professional education programs; and (4) there is no administrative body to assess and ensure competence of individual professionals.
- The audit committee and members of the internal audit team have a major role in ensuring that both the IT organization and IT users are in compliance with organizational guidelines and policies as well as various legal and regulatory practices.

Key Terms

audit committee
body of knowledge
breach of contract
breach of duty of care
bribery
Business Software Alliance (BSA)
certification
compliance
conflict of interest
duty of care
firewall
Foreign Corrupt Practices Act (FCPA)
fraud
government license
IT user
material breach of contract
misrepresentation
negligence
profession
professional code of ethics
professional malpractice
reasonable person standard
reasonable professional standard
résumé inflation
trade secret
whistle-blowing

Self-Assessment Questions

The answers to the Self-Assessment Questions can be found in Appendix B.

1. A professional is someone who:
   a. requires advanced training and experience
   b. must exercise discretion and judgment in the course of his or her work
   c. does work that cannot be standardized
   d. all of the above
2. Although end users often get the blame when it comes to using illegal copies of commercial software, software piracy in a corporate setting is sometimes directly traceable to members of the ______________ organization.
3. The mission of the Business Software Alliance is to ______________.

4. Whistle-blowing is an effort by an employee to attract attention to a negligent, illegal, unethical, abusive, or dangerous act by a company that threatens the public interest. True or False?
5. ______________ is the crime of obtaining goods, services, or property through deception or trickery.
6. ______________ means to be in accordance with established policies, guidelines, specifications, or legislation.
7. Society expects professionals to act in a way that:
   a. causes no harm to society
   b. provides significant benefits
   c. establishes and maintains professional standards that protect the public
   d. all of the above
8. Most organizations have a(n) ______________ team with primary responsibilities to determine that internal systems and controls are adequate and effective.
9. ______________ is a process that one undertakes voluntarily to prove competency in a set of skills.
   a. Licensing
   b. Certification
   c. Registration
   d. all of the above
10. Senior management (including members of the audit committee) has the option of ignoring or suppressing recommendations of the internal audit committee. True or False?
11. ______________ has been defined as not doing something that a reasonable person would do, or doing something that a reasonable person would not do.
12. A(n) ______________ states the principles and core values that are essential to the work of a particular occupational group.

Discussion Questions

1. Would you rather be known as a person of modest means with an impeccable ethical character or as an unscrupulous person of wealth? Why?
2. How do you distinguish between misrepresentation and embellishment of one's professional accomplishments on a résumé? Provide an example of an embellishment that would not be considered misrepresentation.
3. Do laws provide a complete guide to ethical behavior? Can an activity be legal but not ethical?
4. In filling an open position in a U.S.-based IT organization, do you think that preference should be shown for qualified candidates from the United States over qualified candidates from foreign countries? Why or why not?

5. Does charging by the hour encourage unethical behavior on the part of contract workers and consultants?
6. Describe a situation in which there could be a conflict of interest between an IT worker's self-interest and the interests of a client. How should this potential conflict be addressed?
7. Should all IT workers be either licensed or certified? Why or why not?
8. Go to two or more of the Web sites identified in Table 2-3, and read the code of ethics found there. What commonalities do you find among the IT professional codes of ethics that you read? What differences are there? Do you think there are any important issues not addressed by these codes of ethics?
9. You are caught in the middle of a dilemma. You have been subpoenaed to be a witness in a work-related sexual harassment case involving your boss and a coworker. On many occasions, you heard your boss make statements to this employee that could be interpreted as sexual advancements. Your boss has made it clear that he will make things difficult for you at work if you testify in favor of the employee. You could choose to testify in a manner that would make it appear that your boss was not serious and that the employee was overreacting. On the other hand, it was clear to you that your boss was not joking with the employee and that he was harassing her. What kind of repercussions could there be if you testify in favor of your coworker? Would you be willing to risk those repercussions? Does it really matter if the case is dismissed because of your testimony?
10. What is the difference between breach of contract and material breach of contract? In a breach of contract dispute, what recourse can the nonbreaching party take?
11. Under the Foreign Corrupt Practices Act, under what conditions is a bribe not unlawful? Explain, and provide an example.

What Would You Do?

Use the five-step decision-making process discussed in Chapter 1 to analyze the following situations and recommend a course of action.

1. You are a new salesperson at a large software manufacturing firm. It is three weeks from the end of the sales quarter and you and your sales manager are sitting pretty—you have both already met your sales quota for the quarter. In addition, you just closed another deal with a new customer for $100,000 of software and customer service. This order would put you way over your sales quota for the current quarter. Your manager suggests that you hold this new order so it gets recorded against next quarter. She explains that because sales during the next three months tend to slow down, salespeople frequently miss their quotas and associated sales bonuses for that quarter. Holding this large order to next quarter would help you get an excellent start and almost guarantee that you meet your quota. What would you do?
2. You work part-time evenings and weekends as a real estate salesperson. You also work full-time for an IT consulting group. When ordering business cards for your real estate business, you decided to include your full-time work email address. As a result, you frequently find yourself receiving and sending emails related to your real estate work from your computer at your IT consulting job. You try to limit this activity to your lunch hour, but

there are often urgent messages that require an immediate reply. Lately the number of such emails is increasing. Sometimes you worry what would happen if your manager found out about this activity, but cutting off the flow of emails from your clients could have a serious impact on your ability to serve them and earn commissions. What should you do?

3. Your old roommate from college was recently let go from his firm during a wave of employee terminations to reduce costs. You two have kept in touch over the six years since school, and he has asked you to help him get a position in the IT organization where you work. You offered to review his résumé, make sure that it gets to the "right person," and even put in a good word for him. However, as you read the résumé, it is obvious that your friend has greatly exaggerated his accomplishments at his former place of work and even added some IT-related certifications you are sure he never earned. What would you do?
4. The daughter of the firm's CEO is scheduled to participate in a job interview for an entry-level position in the IT organization next week. You are a second-year employee in your firm's IT organization who will participate in the interview process. You will be one of three people who will interview her to form an assessment and make a group decision about whether or not she will be offered the position. How do you handle this situation?
5. You are in charge of awarding all computer hardware service contracts (valued at over $2 million per year) for your employer. In recent emails with the company's current service contractor, you casually exchanged ideas about family vacations. You mentioned that your family is planning on vacationing in the Scottsdale, Arizona, area. You are surprised when the contractor emails you an offer to use his company's condominium at a plush Scottsdale resort, complete with golf and health club privileges. He assures you that the condo would normally be empty that time of year and that other customers frequently use the condo. The resort is one you are familiar with but have never used because the rental is well over $5,000 per week. You would really like for your family to experience staying at a five-star resort but you worry about the potential consequences of accepting the offer. If your manager saw a copy of the emails exchanged with the contractor, could it appear that you were soliciting a bribe? Could this offer be considered a bribe? What would you do?
6. Your organization is preparing to submit a bid for a multimillion-dollar contract in South America. The contract is extremely important to your firm and would represent its first contract in South America. While meeting with your South American contacts, you are introduced to a consultant who offers to help your firm prepare and submit its bid, as well as to negotiate with the prospective customer company. The consultant is quite impressive in his knowledge of local government officials and managers and executives at the customer's company. The fee requested is only 1 percent of the potential value of the contract, but it is unclear exactly what the consultant will do. Later that day, your local contacts tell you that the use of such consultants is common. They say that they are familiar with this particular consultant and that he has a good reputation for getting results. Your company has never worked with such consultants in the past, and you are uncertain on how to proceed. What would you do?
7. You are a new human resources manager assigned to your firm's IT organization. One of your responsibilities is to screen résumés for job openings in the organization. You are in

the process of reviewing more than 100 résumés you received for a position as a Cisco network specialist. Your goal is to trim the group down to the top five candidates to invite to an in-house interview. About half the résumés are from IT workers with less than three years of experience who claim to have one or more Cisco certifications. There are also a few candidates with over five years of impressive experience but no Cisco certifications listed on their résumés. You were instructed to include only candidates with a Cisco certification in the list of finalists. However, you are concerned about possible résumé inflation and the heavy emphasis on certification versus experience. What would you do?

Cases

1. Whistle-Blower Claims Accounting Shenanigans at SuccessFactors

SuccessFactors is a U.S. multinational company that provides cloud-based human resources-related software applications. Under its "software-as-a-service" business model, the company provides software resources to subscribers who access them via the Internet for a fee. Annual revenue for the firm was $206 million in 2010.[43]

SuccessFactors spreads its costs over a large number of subscribers to keep its subscription rates low and generate income. Subscribers, in turn, rely on SuccessFactors to manage their data and software in a secure and reliable manner. Subscribers avoid large capital outlays for computing equipment and eliminate the costs associated with the purchase of hardware and software and the hiring of numerous computer operations and support people.

SuccessFactors has not been profitable—incurring losses in each fiscal period since its inception in 2001, with a loss of $12.5 million for 2010 and an accumulated deficit of $231.3 million.[44] Nevertheless, SAP paid $3.4 billion (over 10 times its 2011 revenue of $327 million) to acquire SuccessFactors in early 2012. (This number compares very unfavorably with the median price—three times revenue—paid in the 32 software mergers that occurred in North America in the five years prior to SAP's purchase of SuccessFactors.)[45] SAP was willing to pay such a premium to gain significant market share and expertise in the rapidly growing human resources software-as-a-service arena. At the time, SuccessFactors had a customer base of some 15 million subscription seat licenses spread across 3,500 customers.[46]

As with many companies, SuccessFactors supplemented the financial results that it reported in accordance with GAAP (generally accepted accounting principles that form the basis for financial reporting), with non-GAAP financial measures. The manner in which such non-GAAP measures are defined and calculated differ from company to company.[47] One of these non-GAAP financial measures was a measure called "backlog." SuccessFactors, and many other cloud computing service firms, invoice subscribers on an annual basis even if the term of the subscription agreement is longer than one year. Amounts that have been invoiced, but that have not yet been recognized as revenue, are recorded as deferred revenue. SuccessFactors reported the portion of the total contract value not yet invoiced as backlog.[48] SuccessFactors had a backlog of about $90 million at the end of 2007 compared with a backlog of $43 million at the end of 2006—an increase the company attributed to an upsurge in new contracts and customers.[49] In 2009, SuccessFactors stopped reporting this backlog figure, and the omission caught the eye of the SEC. When the agency inquired about why the company was no longer reporting this figure, SuccessFactors responded that it felt investors did not consider this figure useful.[50]

In the third quarter of 2010, Success Factors stated that it had adopted a 2009 SEC rule that limited the manner in which revenue could be reported on multiyear contracts.[51] However, in its 2011 annual report, filed just after SAP announced its intent to acquire the firm, but before the deal was finalized, SuccessFactors admitted that its accounting controls suffered from "a material weakness" and that its "internal control over financial reporting was not effective as of December 31, 2011."[52] Indeed, a SuccessFactors salesperson turned whistle-blower claimed that from 2009 to 2011, accounting controls at SuccessFactors were so weak that salespeople were able to improperly rewrite existing multiyear contracts as new contracts to earn additional commissions. If true, this would also accelerate revenue, making the company look more financially sound, while also reducing the backlog number. SAP investigated these claims with an examination conducted by an outside law firm and found no merit to the claims.[53]

Discussion Questions

1. In the end, SuccessFactors investors were not hurt by this alleged improper accounting because SAP paid such a high premium to acquire the firm, which helped SAP jump-start its cloud computing business. Was anyone hurt by this alleged improper accounting and, if so, who and how?
2. Should management encourage the reporting of non-GAAP financial measures that may be useful to investors? Why or why not?
3. What sort of measures should the management teams of service companies put in place to ensure that there is no improper accounting of multiyear contracts?

2. IBM and the State of Indiana Involved in a Breach of Contract Dispute

In December 2006, IBM and the Indiana Family and Social Services Administration (FSSA) entered into a 10-year, $1.16 billion contract to modernize the state's processes and systems for determining welfare eligibility. The state expected to generate $500 million in administrative costs savings over the life of the contract.[54]

FSSA claims it began to notice problems in the new system as early as the project's initial rollout to 10 northern Indiana counties in October 2007. As a result, further expansion was delayed. The state's lawyers wrote: "IBM assured FSSA that if the Region 2 rollout was implemented, IBM would recognize some efficiencies and economies of scale that would improve performance." Accordingly, FSSA agreed to roll out the system to the next region.[55]

By May 2008, the system had expanded into 59 of Indiana's 92 counties. In January 2009, a new FSSA secretary Anne Murphy took over and halted any further expansion until IBM submitted a corrective action plan. She set a deadline of July 2009, and her request included the stipulation that the contract be canceled if IBM failed to improve the situation by September 2009.[56] IBM estimated that addressing the issues would cost $180 million. In October 2009, the state announced it had canceled the deal because IBM failed to make the proposed improvements to the satisfaction of the state.[57]

In May 2010, the state of Indiana sued IBM for $1.3 billion, claiming breach of contract. The Indiana FSSA claimed that system-processing errors resulted in incorrect denials of benefits and delays in processing claims bringing harm to in-need citizens. The claims mishandling rate had climbed from 4 percent to 18 percent under the new system.[58] FSSA spokesman Marcus Barlow stated that "there was more staff working on eligibility during IBM's tenure than before IBM came, yet the results show that once IBM put their system in place, timeliness got worse, error rates went higher. Backlogs got larger."[59]

When the FSSA defined the project in 2006, they told IBM that, for staffing flexibility and efficiency, they wanted a system that would not assign one citizen to a single caseworker. Thus, IBM designed a task-based process that involved outsourcing 1,500 former FSSA employees to IBM. These workers interacted with welfare applicants to gather the necessary data to apply for welfare. Once these workers completed their tasks, the application was turned over to some 700 FSSA state workers who used the accumulated data to determine benefits eligibility.[60]

An IBM spokesman asserted that while there were delays in the system, it was because there were an insufficient number of workers to handle the number of claims. In addition, IBM pointed out that during contract negotiations with IBM, FSSA specified that the system be able to handle up to 4,200 applications per month. However, during the severe recession of 2008–2010, the number of applications frequently exceeded 10,000 per month.[61] The IBM spokesman made it clear that changing from the assigned caseworker approach was Indiana's idea, and was not proposed by IBM.[62] FSSA has since implemented a hybrid system that incorporates the "successful elements of the old welfare delivery system" and a "modernized system." This system assigns caseworkers to welfare recipients and allows for more face-to-face contact.

In its lawsuit, Indiana is demanding that IBM refund the $437 million the state already paid to IBM. Indiana also wants reimbursement of all overtime pay state employees earned working longer hours due to problems with the system. In addition, Indiana insists that IBM be liable for any federal penalties or damages from any lawsuits filed by others because of delays in payments to citizens. IBM countersued Indiana to keep the $400 million it was already paid and for an additional $53 million for the equipment it left in place, which FSSA workers are now using.[63]

In a press release issued at the time the lawsuit was filed, IBM claimed that Indiana had acknowledged that the new system had reduced fraud that was estimated to cost over $100 million per year, led to creation of 1,000 new jobs, and reduced Indiana's operating expenses by $40 million per year for 2008 and 2009 with projected savings of hundreds of millions in upcoming years.[64]

In a 2012 court ruling, the judge ruled that IBM is not entitled to the more than $400 million it sought from Indiana. In the same ruling, the judge denied IBM's claim for damages, while ordering Indiana to pay $12 million for equipment provided by IBM.[65]

Discussion Questions

1. Experienced observers point out that the development of a state social services system is always exceedingly difficult. Multiagency interaction and interdependence often leads to delays and complications in getting requirements finalized and agreed upon. And even if that is accomplished, changes in welfare policies by the state or federal government can render those requirements invalid and require considerable rework. Given the problems that IBM encountered on this contract, should it decline the future opportunities it may have to propose a new solution for a state social services system?

2. Present a strong argument that the state of Indiana is entitled to reimbursement of all funds paid to IBM as well as reimbursement of all overtime employees were paid due to fixing problems associated with the new system. Now present a strong argument that IBM should be allowed to keep all funds it has received so far for this new system.
3. Read about the judge's recent ruling in this case (*www.govtech.com/health/Nobody-Wins-in-Indiana-vs-IBM-Lawsuit-Judge-Says.html*). Do you agree or disagree with the ruling? Provide three reasons to support your opinion.

3. When Certification Is Justified

When Don Tennant, former editor-in-chief of *Computerworld*, published an editorial in favor of IT certification, he was promptly hit with a barrage of angry responses from IT workers.[66] They argued that testable IT knowledge does not necessarily translate into quality IT work. A worker needs good communication and problem-solving skills as well as perseverance to get the job done well. Respondents explained that hardworking IT workers focus on skills and knowledge that are related to their current projects and don't have time for certifications that will quickly become obsolete. Many readers indicated they suspected that vendors offer certification simply as a marketing ploy and a source of revenue. They accused managers without technical backgrounds of using certification as "a crutch, a poor but politically defensible substitute for knowing what and how well one's subordinates are doing."[67]

Any manager would certainly do well to review these insightful points, yet they beg the question: What useful purposes *can* certification serve within an organization?

Some CIOs and vice presidents of technology assert that many employers use certification as a means of training employees and increasing skill levels within the company. Some companies are even using certification as a perk to attract and keep good employees. Such companies may also enhance their employee training programs by offering a job-rotation program through which workers can acquire certification and experience.

Employers are also making good use of certification as a hiring gate both for entry-level positions and for jobs that require specific core knowledge. For example, a company with a Windows Server network might run an ad for a systems integration engineer and require a Microsoft Certified Systems Engineer (MCSE) certification. A company that uses Siebel customer relationship management software might require a new hire to have a certification in the latest version of Siebel.

In addition, specific IT fields, such as project management and security, have a greater need for certification. As the speed and complexity of production increase within the global marketplace, workers in a variety of industries are showing an increasing interest in project management certification. With mottos like "Do It, Do It Right, Do It Right Now," the Project Management Institute has already certified more than 400,000 people. IT industry employers are beginning to encourage and sometimes require project management certification.

Calls for training in the field of security management go beyond certification. The demand for security workers is expected to continue to grow rapidly in the next few years in the face of growing threats. Spam, computer viruses, spyware, botnets, and identity theft have businesses and government organizations worried. They want to make sure that their security managers can protect their data, systems, and resources.

One of the best-recognized security certifications is the CISSP, awarded by the International Information Systems Security Certification Consortium. Yet the CISSP examination, like so many other IT certification examinations, is multiple choice. Employers and IT workers alike have begun to recognize the limitations of these types of examinations. They want to ensure that examinees not only have core knowledge but also know how to use that knowledge—and a multiple-choice exam, even a six-hour, 250-question exam like the CISSP, can't provide that assurance.

Other organizations are catching on. Sun Microsystems requires the completion of programming or design assignments for some of its certifications. So, while there is no universal call for certification or a uniform examination procedure that answers all needs within the IT profession, certifying bodies are beginning to adapt their programs to better fulfill the evolving needs for certification in IT.

Discussion Questions

1. How can organizations and vendors change their certification programs to test for skills as well as core knowledge? What issues might this introduce?
2. What are the primary arguments against certification, and how can certifying bodies change their programs to overcome these shortcomings?
3. What are the benefits of certification? How might certification programs need to change in the future to better serve the needs of the IT community?

End Notes

[1] "CityTime," *New York Times*, March 14, 2012, http://topics.nytimes.com/top/reference/timestopics/organizations/o/office_of_payroll_administration_nyc/citytime/index.html.

[2] "CityTime," *New York Times*, March 14, 2012, http://topics.nytimes.com/top/reference/timestopics/organizations/o/office_of_payroll_administration_nyc/citytime/index.html.

[3] "CityTime," *New York Times*, March 14, 2012, http://topics.nytimes.com/top/reference/timestopics/organizations/o/office_of_payroll_administration_nyc/citytime/index.html.

[4] "CityTime," *New York Times*, March 14, 2012, http://topics.nytimes.com/top/reference/timestopics/organizations/o/office_of_payroll_administration_nyc/citytime/index.html.

[5] Ali Winston, "Comptroller Moves to Rein in CityTime," *CityLimits*, February 26, 2012, www.citylimits.org/news/articles/3896/comptroller-moves.

[6] Serge F. Kovaleski and John Eligon, "New York City Payroll Chief Resigns," *New York Times*, December 23, 2010, www.nytimes.com/2010/12/24/nyregion/24citytime.html.

[7] Serge F. Kovaleski and John Eligon, "New York City Payroll Chief Resigns," *New York Times*, December 23, 2010, www.nytimes.com/2010/12/24/nyregion/24citytime.html.

[8] David W. Chen and William K. Rashbaum, "With Arrest, Criticism for Payroll Project Grows," *New York Times*, May 27, 2011, www.nytimes.com/2011/05/28/nyregion/criticism-for-citytime-project-grows-as-a-manager-is-arrested.html.

[9] Colin Moynihan, "Early Trial Planned for Defendants in CityTime Case," *New York Times*, March 15, 2012, http://cityroom.blogs.nytimes.com/2012/03/15/early-2013-trial-planned-for-defendants-in-citytime-case.

[10] "CityTime," *New York Times*, March 14, 2012, http://topics.nytimes.com/top/reference/timestopics/organizations/o/office_of_payroll_administration_nyc/citytime/index.html.

[11] U.S. Code, Title 5, Part III, Subpart F, Chapter 71, Subchapter 1, Section 7103, http://law.justia.com/us/codes/title5/5usc7103.html (accessed December 27, 2012).

[12] BSA I The Software Alliance, "Record Period of Settlements Underscores Persistent Software Piracy Problem in the US," August 21, 2012, www.bsa.org/country/News%20and%20Events/News%20Archives/en/2012/en-08212012-US.aspx.

[13] BSA I The Software Alliance, "Tennessee Automotive Dealer Pays Heavy Fines," March 7, 2012, www.bsa.org/country/News%20and%20Events/News%20Archives/en/2012/en-03072012-TN.aspx.

[14] Anthony Ha, "Zynga Falls Short of Analysts Estimate for Q2: $332 Million in Revenue, Bookings Decline From Last Quarter, Lowered Outlook," *Tech Crunch*, July 25, 2012, http://techcrunch.com/2012/07/25/zynga-earnings-q2.

[15] Tricia Duryee, "Zynga Files Suit Against Former Staffer, Claiming Theft of Trade Secrets," *AllThingsD.com*, October 14, 2012, http://allthingsd.com/20121014/zynga-files-suit-against-former-staffer-claiming-theft-of-trade-secrets.

[16] Paul McDougall, "Indian Outsourcer Infosys Eyed for Visa Fraud," *InformationWeek*, August 18, 2011, www.informationweek.com/services/outsourcing/indian-outsourcer-infosys-eyed-for-visa/231500239.

[17] Paul McDougall, "Infosys Wins Court Battle, But Visa Troubles Continue," *InformationWeek*, August 21, 2012, www.informationweek.com/global-cio/outsourcing/infosys-wins-court-battle-but-visa-troub/240005939.

[18] Steven Musil, "Man Suing for Half of Facebook Loses Lawyer," *CNET*, June 28, 2011, http://news.cnet.com/8301-1023_3-20075244-93/man-suing-for-half-of-facebook-loses-lawyer.

[19] Thomas Claburn, "Ceglia To Face Facebook Fraud Charges," *InformationWeek*, October 27, 2012, www.informationweek.com/internet/social-network/ceglia-to-face-facebook-fraud-charges/240010623.

[20] "Misleading and Deceptive: Apple Sued Over Siri," *Sydney Morning Herald*, March 14, 2012, www.smh.com.au/digital-life/mobiles/misleading-and-deceptive-apple-sued-over-siri-20120314-1uz3d.html.

[21] Henry R. Cheeseman, "*Contemporary Business Law*," 3rd ed. (Upper Saddle River, NJ: Prentice Hall, 2000), 292.

[22] Eli Segall, "Oracle to Pay $200M in Settlement," *Silicon Valley/San Jose Business Journal*, October 6, 2011, www.bizjournals.com/sanjose/news/2011/10/06/oracle-to-pay-200m-in-settlement.html?page=all.

[23] Paul McDougall, "Ex-Apple Manager Guilty In Kickback Scheme," *InformationWeek*, March 1, 2011, www.informationweek.com/hardware/apple-macintosh/ex-apple-manager-guilty-in-kickback-sche/229219586.

[24] United States Department of Justice, "Foreign Corrupt Practices Act: Antibribery Provisions," www.justice.gov/criminal/fraud/fcpa/docs/lay-persons-guide.pdf (accessed November 9, 2012).

[25] "G20 Throws Weight Behind Global Anti-Corruption Treaty," *TrustLaw*, November 12, 2010, www.trust.org/trustlaw/news/g20-throws-weight-behind-global-anti-corruption-treaty.

[26] Stu Woo, "New Chief Brings Affable Manner and A Boston Accent," *Wall Street Journal*, January 5, 2012, http://online.wsj.com/article/SB10001424052970203513604577140762129761548.html.

[27] Julianne Pepitone, "Yahoo Confirms CEO Is Out After Resume Scandal," *CNN Money*, May 14, 2002, http://money.cnn.com/2012/05/13/technology/yahoo-ceo-out/index.htm.

[28] Ropella, "Hiring Smart: How to Avoid the Top Ten Mistakes," www.ropella.com/index.php/knowledge/recruitingProcessArticles/hiring_smart, © 2012 Ropella Group Inc.

[29] Leo Ma, "Resume Exaggeration in Asia Pacific," *Ezine Articles*, http://ezinearticles.com/?Resume-Exaggeration-in-Asia-Pacific&id=4788569, August 6, 2010.

[30] Association for Computing Machinery, "Welcome," www.acm.org (accessed November 11, 2012).

[31] IEEE Computer Society, "About Us—About the Computer Society," www.computer.org/portal/web/about (accessed November 11, 2012).

[32] IEEE Computer Society, "Computer Society and ACM Approve Software Engineering Code of Ethics," *Computer Society Connection*, October 1999, www.computer.org/cms/Computer.org/Publications/code-of-ethics.pdf (accessed December 28, 2012).

[33] Association of Information Technology Professionals, "About AITP: History," www.aitp.org/organization/about/history/history.jsp (accessed November 11, 2012).

[34] SysAdmin, Audit, Network, Security (SANS) Institute, "Information Security Training, Certification & Research," www.sans.org/about/sans.php (accessed November 11, 2012).

[35] John Cox, "Android Software Piracy Rampant Despite Google's Efforts to Curb," *Network World*, September 29, 2010, www.networkworld.com/news/2010/092910-google-android-piracy.html.

[36] Andres Millington, "Porn in the Workplace is Now a Major Board-Level Concern for Business," *Business Computing World*, April 23, 2010, www.businesscomputingworld.co.uk/porn-in-the-workplace-is-now-a-major-board-level-concern-for-business.

[37] Dean Wilson, "Third of Mobile Workers Distracted by Porn, Report Finds," *TechEYE.net*, June 14, 2010, www.techeye.net/mobile/third-of-mobile-workers-distracted-by-porn-report-finds.

[38] Tony Capaccio, "Missile Defense Staff Warned to Stop Surfing Porn Sites," *Bloomberg*, August 2, 2012, www.bloomberg.com/news/2012-08-01/missile-defense-staff-warned-to-stop-surfing-porn-sites.html.

[39] Associated Press, "WikiLeaks Reveals Sensitive Diplomacy," *Cincinnati Enquirer*, November 28, 2010.

[40] Matthew J. Schwartz, "California Targets Mobile Apps for Missing Privacy Policies," *InformationWeek*, October 31, 2012, www.informationweek.com/government/mobile/california-targets-mobile-apps-for-missi/240012603.

[41] Annemarie K. Keinath and Judith C. Walo, "Audit Committees Responsibilities," *The CPA Journal Online*, www.nysscpa.org/cpajournal/2004/1104/essentials/p22.htm (accessed November 11, 2012).

[42] Shareholders Foundation, Inc. "Press Release: Sensata Technologies Holding N.V. Under Investor Investigation Over Possible Foreign Bribery," *PRLog*, October 26, 2010, www.prlog.org/11024869-sensata-technologies-holding-nv-under-investor-investigation-over-possible-foreign-bribery.html.

[43] SuccessFactors, "SuccessFactors 2010 Annual Report," http://phx.corporate-ir.net/phoenix.zhtml?c=214238&p=irol-reportsAnnual (accessed January 13, 2013).

[44] SuccessFactors, "SuccessFactors 2011 Annual Report," www.sap.com/corporate-en/investors/reports/pdf/SFSF-2011-Annual-Report.pdf (accessed January 13, 2013).

[45] The Linesch Firm, "Whistleblower Sheds Light on Fraud," November 2, 2012, http://lineschfirm.com/wp/whistleblower-sheds-light-on-fraud.

[46] Larry Dignan, "SAP Acquires SuccessFactors for $3.4 Billion: Cloud Consolidation Accelerates," *ZDNet*, December 3, 2011, www.zdnet.com/blog/btl/sap-acquires-successfactors-for-3-4-billion-cloud-consolidation-accelerates/64627.

[47] "Press Release: SuccessFactors Announces Preliminary Fourth Quarter Fiscal 2011 Results," *PRNewswire*, February 2, 2012, www.bizjournals.com/prnewswire/press_releases/2012/02/02/SF46931.

[48] SuccessFactors, "Annual Report 2008," http://media.corporate-ir.net/media_files/irol/21/214238/LetterAnnual08.pdf (accessed January 28, 2013).

[49] SuccessFactors, "Annual Report 2008," http://media.corporate-ir.net/media_files/irol/21/214238/LetterAnnual08.pdf (accessed January 28, 2013).

[50] Scott Priest, "Today in SAP: Allegations Build Over SuccessFactors' Accounting," *SAPexperts*, October 26, 2012, http://sapexperts.wispubs.com/IT/IT-Blog/2012/October/Today-in-SAP-10262012.

[51] Francine McKenna, "Is the SEC's Ponzi Crusade Enabling Companies to Cook the Books, Enron-Style?," *Forbes*, October 18, 2012, www.forbes.com/sites/francinemckenna/2012/10/18/is-the-secs-ponzi-crusade-enabling-companies-to-cook-the-books-enron-style.

[52] Julia Bort, "Whistleblower Explains One Way Cloud Companies Can Cook Their Books," *BusinessInsider*, October 25, 2012, www.businessinsider.com/successfactors-accounting-whistleblower-speaks-2012-10.

[53] Francine McKenna, "Is the SEC's Ponzi Crusade Enabling Companies to Cook the Books, Enron-Style?," *Forbes*, October 18, 2012.

[54] "IBM Closes In on $1.16bn Indiana Deal," *Computer Business Review*, November 29, 2006, www.cbronline.com/news/ibm_closes_in_on_116bn_indiana_deal (accessed November 12, 2010).

[55] Associated Press, "Indiana: IBM Welfare Intake Work Flawed from Start," *Indianapolis Business Journal*, July 21, 2010, www.ibj.com/indiana-ibm-welfare-intake-work-flawed-from-start/PARAMS/article/21227.

[56] Ken Kusmer, Associated Press, "IBM on Notice over Indiana Welfare Deal, *FortWayne.com*, www.newssentinel.com/apps/pbcs.dll/article?AID=/20090708/NEWS/907080335 (accessed December 19, 2010).

[57] Audrey B., "IBM vs. Indiana: Big Blue Makes Indiana See Red," *Seeking Alpha* (blog), May 18, 2010, http://seekingalpha.com/article/205668-ibm-vs-indiana-big-blue-makes-indiana-see-red.

[58] Robert Charette, "Indiana and IBM Sue Each Other Over Failed Outsourcing Contract," *IEEE Spectrum Risk Factor* (blog), May 14, 2010, http://spectrum.ieee.org/riskfactor/computing/it/indiana-and-ibm-sue-each-other-over-failed-outsourcing-contract.

[59] Andy Opsahl, "IBM and Indiana Suing Each Other Over Canceled Outsourcing Deal," *Government Technology*, May 13, 2010, www.govtech.com/health/IBM-and-Indiana-Suing-Each-Other.html.

[60] Andy Opsahl, "IBM and Indiana Suing Each Other Over Canceled Outsourcing Deal," *Government Technology*, May 13, 2010, www.govtech.com/health/IBM-and-Indiana-Suing-Each-Other.html.

[61] Andy Opsahl, "IBM and Indiana Suing Each Other Over Canceled Outsourcing Deal," *Government Technology*, May 13, 2010, www.govtech.com/health/IBM-and-Indiana-Suing-Each-Other.html.

[62] Andy Opsahl, "IBM and Indiana Suing Each Other Over Canceled Outsourcing Deal," *Government Technology*, May 13, 2010, www.govtech.com/health/IBM-and-Indiana-Suing-Each-Other.html.

[63] Andy Opsahl, "IBM and Indiana Suing Each Other Over Cancelled Outsourcing Deal," *Government Technology*, May 13, 2010, www.govtech.com/health/IBM-and-Indiana-Suing-Each-Other.html.

[64] IBM, "Press Release: IBM Seeks Enforcement of Indiana Welfare Contract," May 13, 2010, www-03.ibm.com/press/us/en/pressrelease/31641.wss.

[65] Colin Wood, "Nobody Wins in Indiana vs. IBM Lawsuit, Judge Says," *Government Technology*, July 19, 2012, www.govtech.com/health/Nobody-Wins-in-Indiana-vs-IBM-Lawsuit-Judge-Says.html.

[66] Don Tennant, "Certifiably Concerned," *Computerworld*, June 13, 2005, www.computerworld.com/s/article/102394/Certifiably_Concerned.

[67] Don Tennant, "Certifiably Mad?," *Computerworld*, June 20, 2005, www.computerworld.com/s/article/102564/Certifiably_Mad.