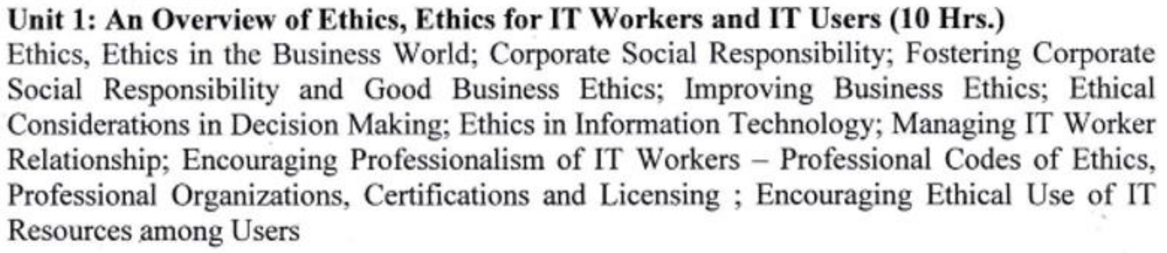
Unit 1: Introduction

Syllabus:



Unit 1: An Overview of Ethics, Ethics for IT Workers and IT Users (10 Hrs.)
Ethics, Ethics in the Business World; Corporate Social Responsibility; Fostering Corporate Social Responsibility and Good Business Ethics; Improving Business Ethics; Ethical Considerations in Decision Making; Ethics in Information Technology; Managing IT Worker Relationship; Encouraging Professionalism of IT Workers – Professional Codes of Ethics, Professional Organizations, Certifications and Licensing ; Encouraging Ethical Use of IT Resources among Users

===

Ethics

Ethics is a code of behaviour that is defined by the group to which an individual belongs. Ethical behaviour conforms to generally accepted norms, which may change over time to meet the evolving needs of the society or a group of people who share similar laws, traditions, and values that provide structure to enable them to live in an organized manner. Ethics help members of a group understand their roles and responsibilities so they can work together to achieve mutual benefits such as security, access to resources, and the pursuit of life goals.

Ethics is based on well-founded standards of right and wrong that prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, or specific virtues.

Some years ago, sociologist Raymond Baumhart asked business people, "What does ethics mean to you?" Among their replies were the following:

"Ethics has to do with what my feelings tell me is right or wrong."
"Ethics has to do with my religious beliefs."
"Being ethical is doing what the law requires."
"Ethics consists of the standards of behaviour our society accepts."
"I don't know what the word means."

Like Baumhart's first respondent, many people tend to equate ethics with their feelings. But being ethical is clearly not a matter of following one's feelings. A person following his or her feelings may recoil from doing what is right. In fact, feelings frequently deviate from what is ethical.

Nor should one identify ethics with religion. Most religions, of course, advocate high ethical standards. Yet if ethics were confined to religion, then ethics would apply only to religious people. But ethics applies as much to the behaviour of the atheist as to that of the devout religious person. Religion can set high ethical standards and can provide intense motivations for ethical behaviour. Ethics, however, cannot be confined to religion nor is it the same as religion.

Being ethical is also not the same as following the law. The law often incorporates ethical standards to which most citizens subscribe. But laws, like feelings, can deviate from what is ethical. Our own pre-Civil War slavery laws and the old apartheid laws of present-day South Africa are grotesquely obvious examples of laws that deviate from what is ethical.

Finally, being ethical is not the same as doing "whatever society accepts." In any society, most people accept standards that are, in fact, ethical. But standards of behaviour in society can deviate from what is ethical. An entire society can become ethically corrupt. Nazi Germany is a good example of a morally corrupt society.

Moreover, if being ethical were doing "whatever society accepts," then to find out what is ethical, one would have to find out what society accepts. To decide what we should think about abortion, for example, we would have to take a survey of Our society and then conform our beliefs to whatever society accepts. But no one ever tries to decide an ethical issue by doing a survey. Further, the lack of social consensus on many issues makes it impossible to equate ethics with whatever society accepts. Some people accept abortion but many others do not. If being ethical were doing whatever society accepts, one would have to find an agreement on issues which does not, in fact, exist.

What, then, is ethics?

Ethics is two things. First, ethics refers to well-founded standards of right and wrong that prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, or specific virtues.

Ethics, for example, refers to those standards that impose the reasonable obligations to refrain from rape, stealing, murder, assault, slander, and fraud. Ethical standards also include those that enjoin virtues of honesty, compassion, and loyalty. And, ethical standards include standards relating to rights, such as the right to life, the right to freedom from injury, and the right to privacy. Such standards are adequate standards of ethics because they are supported by consistent and well-founded reasons.

Secondly, ethics refers to the study and development of one's ethical standards. As mentioned above, feelings, laws, and social norms can deviate from what is ethical. So, it is necessary to constantly examine one's standards to ensure that they are reasonable and well-founded. Ethics also means, then, the continuous effort of studying our own moral beliefs and our moral conduct, and striving to ensure that we, and the institutions we help to shape, live up to standards that are reasonable and solidly-based.

Morals

Morals are the personal principles upon which an individual bases his or her decisions about what is right and what is wrong. They are core beliefs formed and adhered to by an individual. For example, many of us have a core belief that all people should be treated with respect and this belief governs our actions toward others. Your moral principles are statements of what you believe to be rules of right conduct. As a child, you may have been taught not to lie, cheat, or steal. As an adult facing more complex decisions, you often reflect on your moral principles when you consider what to do in different situations: Is it okay to lie to protect someone's feelings? Should you intervene with a co-worker who seems to have a chemical dependency problem? Is it acceptable to exaggerate your work experience on a résumé? Can you cut corners on a project to meet a tight deadline?

As children grow, they learn complicated tasks—such as walking, talking, swimming, riding a bike, and writing the alphabet—that they perform out of habit for the rest of their lives. People also develop habits that make it easier for them to choose between good and bad.

virtue

A **virtue** is a habit that inclines people to do what is acceptable, and a **vice** is a habit of unacceptable behaviour. Fairness, generosity, and loyalty are examples of virtues, while vanity, greed, envy, and anger are considered **vices**. People's virtues and vices help define their personal value system—the complex scheme of moral values by which they live.

Although nearly everyone would agree that certain behaviours—such as lying and cheating—are wrong, opinions about what constitutes right and wrong behaviours can vary dramatically. For example, attitudes toward software piracy—a form of copyright infringement that involves making copies of software or enabling others to access software to which they are not entitled—range from strong opposition to acceptance of the practice as a standard approach to conducting business. According to the Business Software Alliance (BSA), the global rate of software piracy stands at around 42 percent. The piracy rate is nearly 80 percent across the continent of Africa, where many consumers simply cannot afford software licenses and pirated copies are readily available at cut-rate prices.

Individual views of what behaviour is moral may be impacted by a person's age, cultural group, ethnic background, religion, life experiences, education, and gender along with many other factors. There is widespread agreement on the immorality of murder, theft, and arson, but other behaviours that are accepted in one culture might be unacceptable in another. Even within the same society, people can have strong disagreements over important moral issues.

Figure below illustrates the relationship between ethics and morals and identifies some of the many factors that help define them.

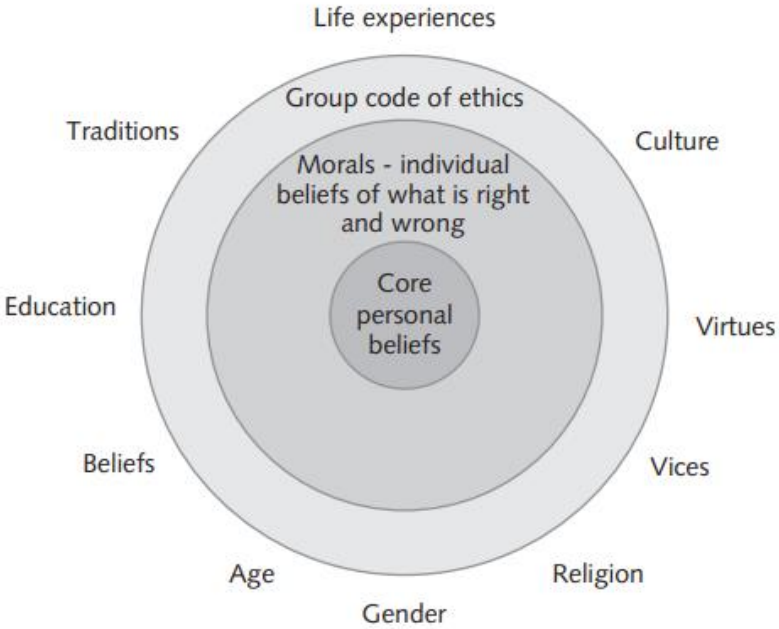


Figure: The relationship between ethics and morals

The Difference Between Morals, Ethics, and Laws

Law is a system of rules that tells us what we can and cannot do. Laws are enforced by a set of institutions (the police, courts, law-making bodies). Violation of a law can result in censure, fines, and/or imprisonment. Laws in the United States are made by the various local, state, and federal legislatures. Sometimes the laws of these various jurisdictions are in conflict, creating confusion and uncertainty. In addition, laws are not static; new laws are constantly being introduced and existing laws repealed or modified. As a result, the precise meaning of a particular law may be different in the future from what it is today.

Legal acts are acts that conform to the law. Moral acts conform to what an individual believes to be the right thing to do. Laws can proclaim an act as legal, although many people may consider the act immoral—for example, abortion. Laws may also proclaim an act as illegal, although many people may consider the act moral—for example, using marijuana to relieve stress and nausea for people undergoing chemotherapy treatment for cancer.

Laws raise important and complex issues concerning equality, fairness, and justice, but do not provide a complete guide to ethical behaviour. Just because an activity is defined as legal does not mean that it is ethical as shown in figure below.

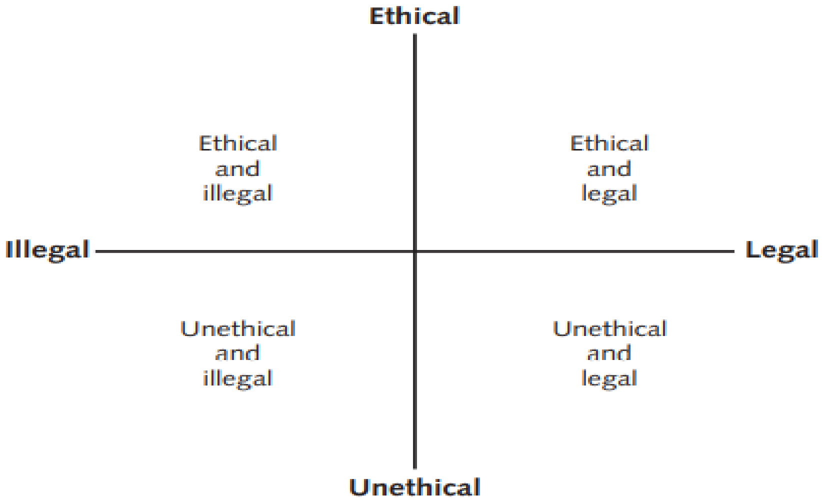


Figure: Legal versus ethical

As a result, practitioners in many professions subscribe to a code of ethics that states the principles and core values that are essential to their work and, therefore, govern their behaviour. The code can become a reference point for helping an individual determine what is legal and what is ethical; however, an individual will also be guided by his or her set of morals.

Ethics in the Business World

Ethics has risen to the top of the business agenda because the risks associated with inappropriate behaviour have increased, both in their likelihood and in their potential negative impact. We have seen the collapse of financial institutions such as Bank of America, CitiGroup, Countrywide Financial, Fannie Mae, Freddie Mac, Lehman Brothers, and American International Group (AIG) due to unwise and/or unethical decision making regarding the approval of mortgages, loans, and lines of credit to unqualified individuals and organizations.

We have also witnessed numerous corporate officers and senior managers sentenced to prison terms for their unethical behaviour, including former investment broker Bernard Madoff, who bilked his clients out of an estimated $65 billion, and Stewart Parnell, former CEO of Peanut Corporation of America, who was sentenced to 28 years in prison for knowingly shipping contaminated food product, resulting in a salmonella outbreak that killed nine people and sickened more than 700. Clearly, unethical behaviour in the business world can lead to serious negative consequences for both organizations and individuals.

Several trends have increased the likelihood of unethical behaviour. First, for many organizations, greater globalization has created a much more complex work environment that spans diverse cultures and societies, making it more difficult to apply principles and codes of ethics consistently. Numerous U.S. companies have moved operations to developing countries, where employees or contractors work in conditions that would not be acceptable in the most developed parts of the world. For example, it was reported in 2016 that employees of the Pegatron factory in

China, where the Apple iPhone is produced, are often forced to work excessive amounts of overtime—up to 90 overtime hours per month—while their overall wages have been cut from $1.85 to $1.60 per hour.

Second, in today’s challenging and uncertain economic climate, many organizations are finding it more difficult to maintain revenue and profits. Some organizations are sorely tempted to resort to unethical behaviour to maintain profits. Tesco, Britain’s largest supermarket chain, admitted its first half-year of profits for 2013 were overstated by $400 million. Fiat Chrysler Automobiles admitted its U.S. auto sales were overstated by hundreds of cars each month starting as far back as 2011.

Employees, shareholders, and regulatory agencies are increasingly sensitive to violations of accounting standards, failures to disclose substantial changes in business conditions, nonconformance with required health and safety practices, and production of unsafe or substandard products. Such heightened vigilance raises the risk of financial loss for businesses that do not foster ethical practices or that run afoul of required standards. There is also a risk of criminal and civil lawsuits resulting in fines and/or incarceration for individuals.

A classic example of the many risks associated with unethical decision making can be found in the Enron accounting scandal. In 2000, Enron—a Texas-based energy company—employed over 22,000 people, and it reported an annual revenue of $101 billion. However, in 2001, it was revealed that much of Enron’s revenue was the result of deals with limited partnerships, which it controlled. In addition, as a result of actions taken contrary to generally accepted accounting practices (GAAP), many of Enron’s debts and losses were not reported in its financial statements. As the accounting scandal unfolded, Enron shares dropped from $90 per share to less than $1 per share, and the company was forced to file for bankruptcy. The Enron case was notorious, but many other corporate scandals have occurred in spite of safeguards enacted as a result of the Enron debacle.

Here are just a few examples of lapses in business ethics by employees in IT organizations:

1. Volkswagen has admitted that 11 million of its vehicles were equipped with software that was used to cheat on emissions tests. The company is now contending with the fallout.

2. Toshiba, the Japanese industrial giant whose diversified products and services include information technology and communications equipment and systems, disclosed that it overstated its earnings over a seven-year period by more than $1.2 billion.

3. Amazon has the second highest employee turnover rate of companies in the Fortune 500 and has been criticized by some for creating a high-pressure work environment in which bosses’ expectations were almost impossible to satisfy and jobs were threatened if illness or other personal issues encroached on work.

It is not unusual for powerful, highly successful individuals to fail to act in morally appropriate ways, as these examples illustrate. Such people are often aggressive in striving for what they want and are used to having privileged access to information, people, and other resources. Furthermore, their success often inflates their belief that they have the ability and the right to manipulate the outcome of any situation.

The moral corruption of people in power, which is often facilitated by a tendency for people to look the other way when their leaders act inappropriately has been given the name Bathsheba syndrome—a reference to the biblical story of King David, who became corrupted by his power and success. According to the story, David became obsessed with Bathsheba, the wife of one of his generals, and eventually ordered her husband on a mission of certain death so that he could marry Bathsheba.

Even lower-level employees and ordinary individuals can find themselves in the middle of ethical dilemmas, as these examples illustrate:

- Edward Snowden, working as a Dell contractor at the National Security Agency (NSA), copied thousands of classified and unclassified documents that revealed details about the capabilities and scope of operations of the NSA and other foreign intelligence agencies. The documents were then handed over to reporters who published many of the disclosures in the Guardian and Washington Post newspapers. Snowden felt he acted as a patriot in exposing the behaviour of the NSA, which he thought was overreaching and counter to the U.S. Constitution. Some consider him a whistle-blower and a hero, while others see him as a traitor.

- Mark Lillie, a former Takata Corporation engineer, warned the company of the potential deadly consequences of using the propellant ammonium nitrate to inflate its airbags. The use of ammonium nitrate enabled Takata to earn a greater profit than other designs, however, it also resulted in devices that can deploy with too much force, causing them to rupture and shoot metal fragments at motorists. Unfortunately, Lillie was unable to convince management at Takata to choose an alternative design. He eventually left the firm in disagreement over this fatal manufacturing decision. In the United States, at least 10 deaths and more than 100 injuries have been attributed to the flawed devices, and over 100 million cars with Takata inflators have been recalled worldwide.

Corporate Social Responsibility

Corporate social responsibility (CSR) is the concept that an organization should act ethically by taking responsibility for the impact of its actions on its shareholders, consumers, employees, community, environment, and suppliers as shown in figure below.

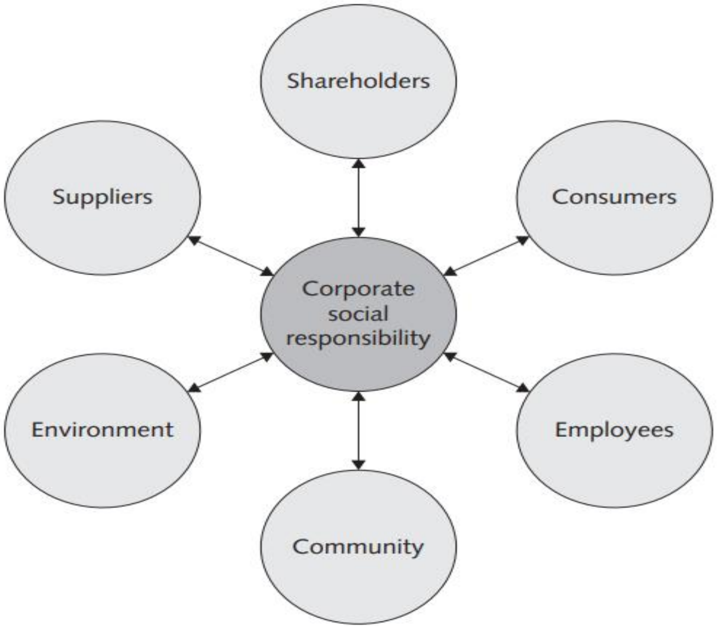


Figure: - An organization's program CSR affects its shareholders, consumers, employees, community, environment, and suppliers

An organization's approach to CSR can encompass a wide variety of tactics—from donating a portion of net profit to charity to implementing more sustainable business operations or encouraging employee education through tuition reimbursement. Setting CSR goals encourages an organization to achieve higher moral and ethical standards.

Supply chain sustainability is a component of CSR that focuses on developing and maintaining a supply chain that meets the needs of the present without compromising the ability of future generations to meet their needs. Supply chain sustainability takes into account issues such as fair labour practices, energy and resource conservation, human rights, and community responsibility.

Many IT equipment manufacturers have made supply chain sustainability a priority, in part, because they must adhere to various European Union directives and regulations—including the Restriction of Hazardous Substances Directive, the Waste Electrical and Electronic Equipment Directive, and the Registration, Evaluation, Authorization, and Restriction of Chemicals (REACH) Regulation—to be permitted to sell their products in the European Union countries.

In many cases, meeting supply chain sustainability goals can also lead to lower costs. For example, in fiscal year 2015, Dell launched its closed-loop plastics supply chain and by year end had recycled 2.2 million pounds of those plastics back into new Dell products. In addition, its global takeback program has made Dell the world's largest technology recycler, collecting more than 1.4 billion pounds of e-waste since 2007.

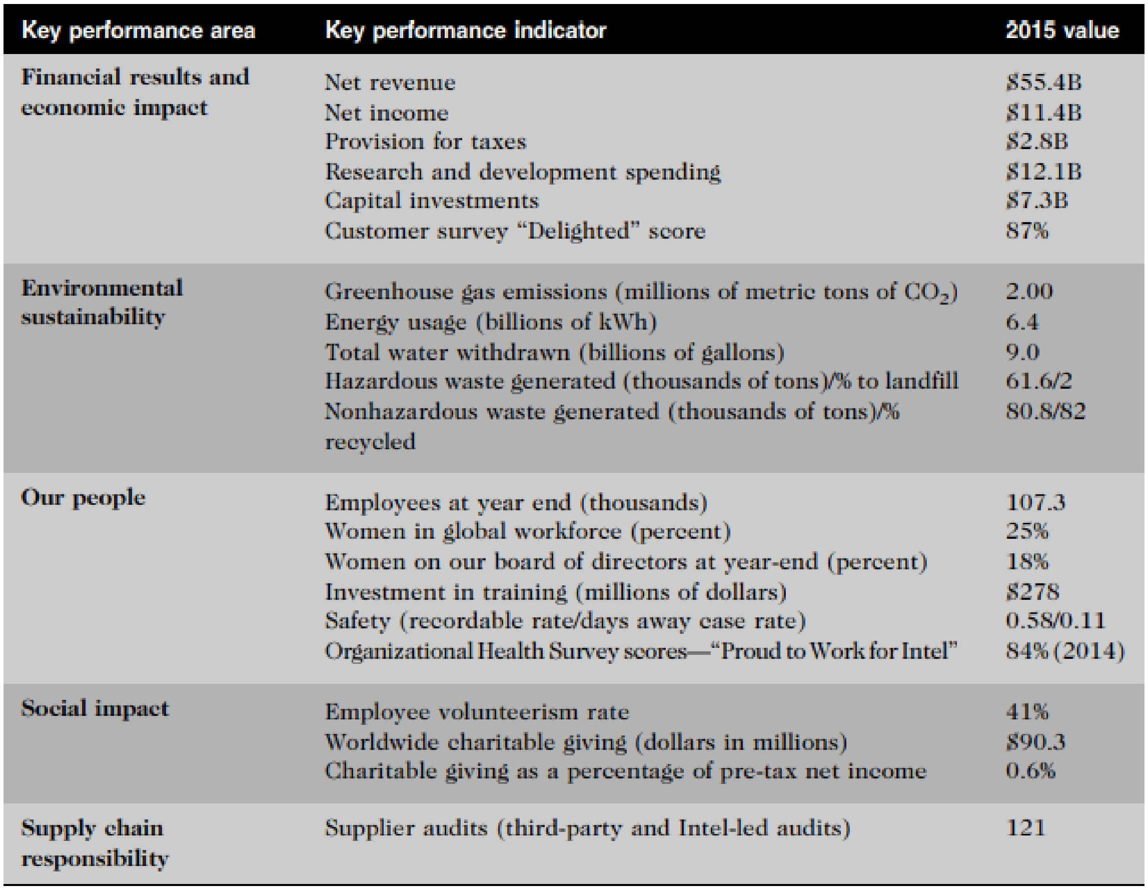
Each organization must decide if CSR is a priority and, if so, what its specific CSR goals are. The pursuit of some CSR goals can lead to increased profits, making it easy for senior company management and stakeholders to support the organization's goals in this arena. However, if striving to meet a specific CSR goal leads to a decrease in profits, senior management may be challenged to modify or drop that CSR goal entirely.

For example, most U.S. auto manufacturers have introduced models that run on clean, renewable electric power as part of a corporate responsibility goal of helping to end U.S. dependence on oil. However, Americans have been slow to embrace electric cars, and many manufacturers have had to offer low-interest financing, cash discounts, sales bonuses, and subsidized leases to get the autos off the sales floor. Manufacturers and dealers are struggling to increase profits on the sale of these electric cars, and senior management at the automakers must consider how long they can continue with their current strategies.

Many organizations define a wide range of corporate responsibility areas that are important to them, their customers, and their community. In order for a CSR program to be effective, a senior executive should be placed in charge of corporate responsibility results for each area, with strategic initiatives defined, staffed, and well-funded. Key indicators of progress in these areas should be defined and the results tracked and reported to measure progress.

Table 1-2 shows a summary of the 2015 corporate responsibility report for Intel. An example of one strategic initiative at Intel is its diversity and inclusion initiative launched in early 2015 whose goal is to achieve full representation of women and underrepresented minorities in Intel's workforce by 2020.

TABLE 1-2 Intel Corporate Responsibility Report for 2015



Key performance area	Key performance indicator	2015 value
Financial results and economic impact	Net revenue Net income Provision for taxes Research and development spending Capital investments Customer survey "Delighted" score	$55.4B $11.4B $2.8B $12.1B $7.3B 87%
Environmental sustainability	Greenhouse gas emissions (millions of metric tons of CO_2) Energy usage (billions of kWh) Total water withdrawn (billions of gallons) Hazardous waste generated (thousands of tons)/% to landfill Nonhazardous waste generated (thousands of tons)/% recycled	2.00 6.4 9.0 61.6/2 80.8/82
Our people	Employees at year end (thousands) Women in global workforce (percent) Women on our board of directors at year-end (percent) Investment in training (millions of dollars) Safety (recordable rate/days away case rate) Organizational Health Survey scores—"Proud to Work for Intel"	107.3 25% 18% $278 0.58/0.11 84% (2014)
Social impact	Employee volunteerism rate Worldwide charitable giving (dollars in millions) Charitable giving as a percentage of pre-tax net income	41% $90.3 0.6%
Supply chain responsibility	Supplier audits (third-party and Intel-led audits)	121

Fostering Corporate Social Responsibility and Good Business Ethics

Organizations have at least five good reasons to pursue CSR goals and to promote a work environment in which employees are encouraged to act ethically when making business decisions:

- Gaining the goodwill of the community
- Creating an organization that operates consistently
- Fostering good business practices
- Protecting the organization and its employees from legal action
- Avoiding unfavourable publicity

<u>1.Gaining the Goodwill of the Community</u>

Although organizations exist primarily to earn profits or provide services to customers, they also have some fundamental responsibilities to society. As discussed in the previous section, companies often declare these responsibilities in specific CSR goals.

All successful organizations, including technology firms, recognize that they must attract and maintain loyal customers. Philanthropy is one way in which an organization can demonstrate its values in action and make a positive connection with its stakeholders. As a result, many organizations initiate or support socially responsible activities, which may include making contributions to charitable organizations and non-profit institutions, providing benefits for employees in excess of any legal requirements, and devoting organizational resources to initiatives that are more socially desirable than profitable. Here are a few examples of some of the CSR activities supported by major IT organizations:

- **Dell Inc.** has several initiatives aimed at reducing the number of natural resources it takes to create and ship its products, cutting the amount of energy it takes its customers to use its products, and curbing the effects its products have on people and the planet.
- **Google** agreed to invest more than $1.5 billion in renewable energy projects, such as large-scale wind farms and rooftop solar panels.
- **IBM** created a program to train transitioning service members to become certified as advanced data analysts. The company also launched the P-TECH program to help students from low-income families finish high school and obtain associate degrees. Several graduates of the program have taken entry-level jobs at IBM while continuing to work toward a four-year degree.
- **Microsoft** made $922 million in technology donations to more than 120,000 non-profit organizations globally, and its employees contributed $117 million to 20,000 non-profits through the company’s corporate giving program.
- **Oracle** delivered nearly $5 billion in resources (with a focus on computer science education) to help 2.2 million students in 100 countries become college-and-career ready.
- **SAP** (System Applications and Products in Data Processing) pledged over $1 billion toward immediate relief efforts, long-term education, and integration projects to assist refugees, and it initiated a program to provide internship opportunities for more than 100 refugees as well as humanitarian assistance.

The goodwill that CSR activities generate can make it easier for corporations to conduct their business. For example, a company known for treating its employees well will find it easier to compete for the top job candidates. On the other hand, businesses that are not socially responsible run the risk of alienating their customer base.

A recent study of more than 10,000 shoppers in 10 different countries revealed that more than 90 percent are likely to switch to brands that support a socially responsible cause, given similar price and quality. In addition, 90 percent of the shoppers surveyed would boycott a company if they learned that the firm engaged in socially irresponsible business practices. Indeed, 55 percent of the respondents had already done so in the previous year.

2.Creating an Organization That Operates Consistently

Organizations develop and abide by values to create an organizational culture and to define a consistent approach for dealing with the needs of their stakeholders— shareholders, employees, customers, suppliers, and the community. Such a consistency ensures that employees know what is expected of them and can employ the organization's values to help them in their decision making. Consistency also means that shareholders, customers, suppliers, and the community know what they can expect of the organization—that it will behave in the future much as it has in the past. It is especially important for multinational or global organizations to present a consistent face to their shareholders, customers, and suppliers, no matter where those stakeholders live or operate their business. Although each company's value system is different, many share the following values:

- Operate with honesty and integrity, staying true to organizational principles
- Operate according to standards of ethical conduct, in words and action
- Treat colleagues, customers, and consumers with respect
- Strive to be the best at what matters most to the organization
- Value diversity
- Make decisions based on facts and principles

3.Fostering Good Business Practices

In many cases, good ethics can mean good business and improved profits. Companies that produce safe and effective products avoid costly recalls and lawsuits. Companies that provide excellent service retain their customers instead of losing them to competitors. Companies that develop and maintain strong employee relations enjoy lower turnover rates and better employee morale. Suppliers and other business partners often place a priority on working with companies that operate in a fair and ethical manner. All these factors tend to increase revenue and profits while decreasing expenses. As a result, ethical companies tend to be more profitable over the long term than unethical companies.

On the other hand, bad ethics can lead to bad business results. Bad ethics can have a negative impact on employees, many of whom may develop negative attitudes if they perceive a difference between their own values and those stated or implied by an organization's actions. In such an environment, employees may suppress their tendency to act in a manner that seems ethical to them and instead act in a manner that will protect them against anticipated punishment. When such a discrepancy between employee and organizational ethics occurs, it destroys employee commitment to organizational goals and objectives, creates low morale, fosters poor performance, erodes employee involvement in organizational improvement initiatives, and builds indifference to the organization's needs.

4. Protecting the Organization and Its Employees from Legal Action

In a 1909 ruling (United States v. New York Central & Hudson River Railroad Co.), the U.S. Supreme Court established that an employer can be held responsible for the acts of its employees even if the employees act in a manner contrary to corporate policy and their employer's directions. The principle established is called respondent superior, or "let the master answer."

When it was uncovered that employees of Wells Fargo Bank opened over 2 million bogus credit card accounts not authorized by its customers, the bank was fined over $185 million and ordered to pay customers full restitution for any fees or charges they may have incurred. The practice began at least as early as 2011 and was an attempt by thousands of bank employees to achieve their sales targets for cross-selling and be rewarded with higher sales bonuses. Cross-selling is the practice of selling multiple products to the existing customers—savings account, checking account, auto loan, mortgage, credit card, etc. Cross-selling to existing customers is cheaper than locating and selling to brand new customers. It also tends to lock existing customers into your bank.

A coalition of several legal organizations, including the Association of Corporate Counsel, the U.S. Chamber of Commerce, the National Association of Manufacturers, the National Association of Criminal Défense Lawyers, and the New York State Association of Criminal Défense Lawyers, argues that organizations should "be able to escape criminal liability if they have acted as responsible corporate citizens, making strong efforts to prevent and detect misconduct in the workplace." One way to do this is to establish effective ethics and compliance programs. However, some people argue that officers of companies should not be given light sentences if their ethics programs fail to deter criminal activity within their firms.

5.Avoiding Unfavourable Publicity

The public reputation of a company strongly influences the value of its stock, how consumers regard its products and services, the degree of oversight it receives from government agencies, and the amount of support and cooperation it receives from its business partners. Thus, many organizations are motivated to build a strong ethics program to avoid negative publicity. If an organization is perceived as operating ethically, customers, business partners, shareholders, consumer advocates, financial institutions, and regulatory bodies will usually regard it more favourably.

Prominent ad buyers and marketers are angry with Facebook after finding out that the world's largest online social network service greatly exaggerated the average viewing time of video ads on its platform. This is a key metric used by advertisers in deciding how much to spend on Facebook video versus other video services such as YouTube, Twitter, and TV networks. It turns out that Facebook was not including views of three seconds or less in calculating its average view time, resulting in overestimating viewing time by 60 to 80 percent. Some advertising industry analysts believe that the new viewing time results and bad publicity associated with the incident will be impactful in the future placement of tens of billions of advertising dollars.

Improving Business Ethics

A well-implemented ethics and compliance program and a strong ethical culture can lead to less pressure on employees to misbehave and a decrease in observed misconduct. It also creates an environment in which employees are more comfortable reporting instances of misconduct, partly because there is less fear of potential retaliation by management against reporters. See Figure below.

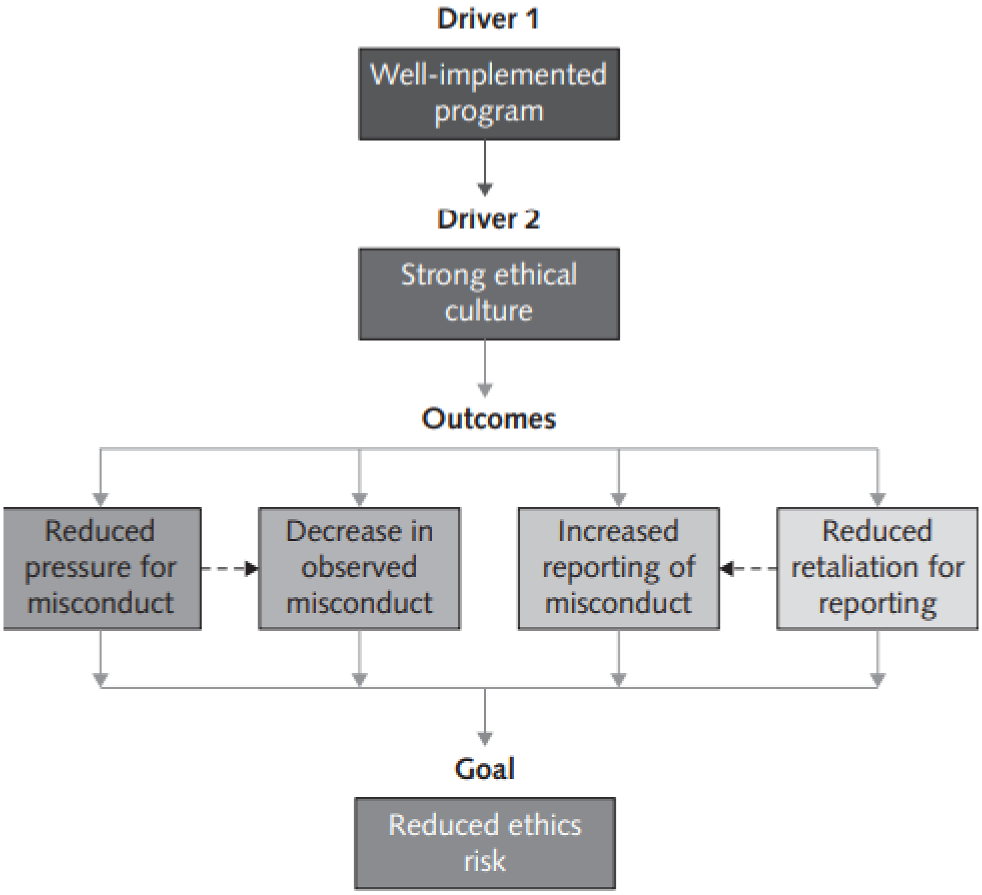

Driver 1
Well-implemented program
Driver 2
Strong ethical culture
Outcomes
Reduced pressure for misconduct
Decrease in observed misconduct
Increased reporting of misconduct
Reduced retaliation for reporting
Goal
Reduced ethics risk

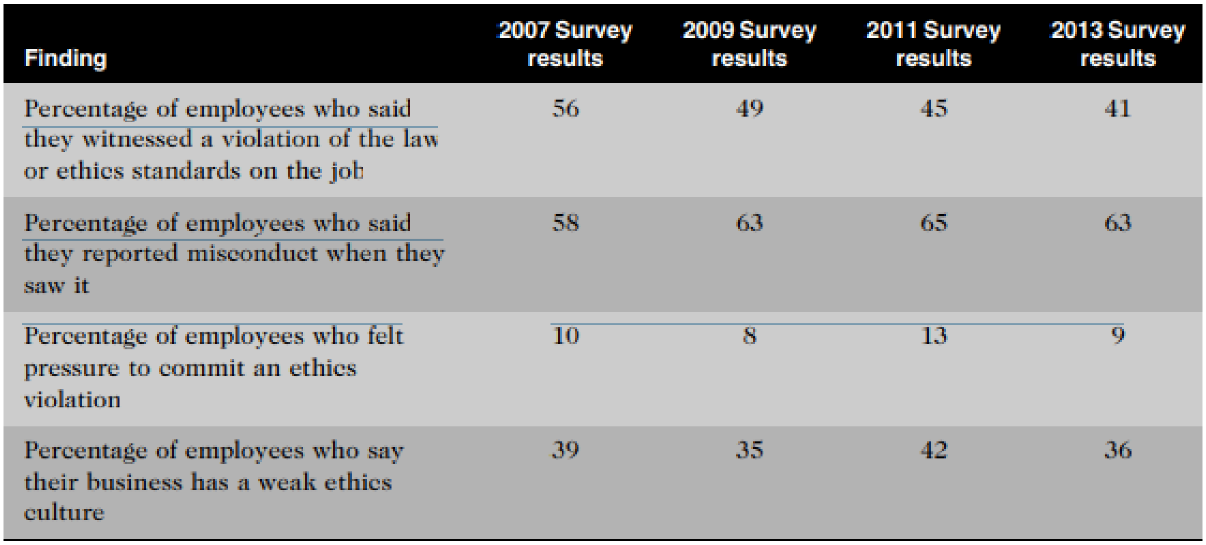
Figure: Reducing the risk of unethical behaviour

The Ethics Resource Centre has defined the following characteristics of a successful ethics program:

- Employees are willing to seek advice about ethics-related issues.
- Employees feel prepared to handle situations that could lead to misconduct.
- Employees are rewarded for ethical behaviour.
- The organization does not reward success obtained through questionable means.
- Employees feel positively about their company.

The 2013 National Business Ethics Survey found evidence of continuing improvement in ethics in the workplace, as summarized in Table 1-3. The survey results indicate that fewer employees witnessed misconduct on the job, but when they did, they were more willing to report it. They also show that there is a decrease in the percentage of employees who felt pressure to commit an unethical act and who feel their organization has a weak ethics culture.

TABLE 1-3 Conclusions from the 2013 National Business Ethics Survey



Finding	2007 Survey results	2009 Survey results	2011 Survey results	2013 Survey results
Percentage of employees who said they witnessed a violation of the law or ethics standards on the job	56	49	45	41
Percentage of employees who said they reported misconduct when they saw it	58	63	65	63
Percentage of employees who felt pressure to commit an ethics violation	10	8	13	9
Percentage of employees who say their business has a weak ethics culture	39	35	42	36

In addition to reporting on some positive trends in workplace ethics, however, the survey also highlighted some areas of concern. For instance, about 21 percent of those who reported misconduct stated that they suffered from some sort of retribution from their supervisor or negative reaction from their co-workers; that amounts to an estimated 6.2 million American workers who have faced a backlash for reporting misconduct.

The following sections explain some of the action's corporations can take to improve business ethics.

1. Appoint a Corporate Ethics Officer

A corporate ethics officer (also called a corporate compliance officer) provides an organization with vision and leadership in the area of business conduct. This individual "aligns the practices of a workplace with the stated ethics and beliefs of that workplace, holding people accountable to ethical standards."

Organizations send a clear message to employees about the importance of ethics and compliance in their decision about who will be in charge of the effort and to whom that individual will report. Ideally, the corporate ethics officer should be a well-respected, senior-level manager who reports directly to the CEO. Ethics officers come from diverse backgrounds, such as legal staff, human resources, finance, auditing, security, or line operations.

The ethics officer position has its critics. Many are concerned that if one person is appointed head of ethics, others in the organization may think they have no responsibility in this area. On the other hand, Odell Guyton—a long-time director of compliance at Microsoft—feels a point person for ethics is necessary, otherwise, “how are you going to make sure it’s being done, when people have other core responsibilities? That doesn’t mean it’s on the shoulders of the compliance person alone.”

Typically, the ethics officer tries to establish an environment that encourages ethical decision making through the actions. Specific responsibilities include the following:

- Responsibility for compliance—that is, ensuring that ethical procedures are put into place and consistently adhered to throughout the organization
- Responsibility for creating and maintaining the ethics culture envisioned by the highest level of corporate authority
- Responsibility for being a key knowledge and contact person on issues relating to corporate ethics and principles

Of course, simply naming a corporate ethics officer does not automatically improve an organization’s ethics; hard work and effort are required to establish and provide ongoing support for an organizational ethics program.

2. **Require the Board of Directors to Set and Model High Ethical Standards**

The board of directors is responsible for the careful and responsible management of an organization. In a for-profit organization, the board’s primary objective is to oversee the organization’s business activities and management for the benefit of all stakeholders, including shareholders, employees, customers, suppliers, and the community. In a non-profit organization, the board reports to a different set of stakeholders—in particular, the local community that the non-profit serves.

A board of directors fulfils some of its responsibilities directly and assigns others to various committees. The board is not normally responsible for day-to-day management and operations; these responsibilities are delegated to the organization’s management team. However, the board is responsible for supervising the management team.

Board members are expected to conduct themselves according to the highest standards for personal and professional integrity while setting the standard for company-wide ethical conduct and ensuring compliance with laws and regulations. Employees will “get the message” if board members set an example of high-level ethical behaviour. If they don’t set a good example, employees will get that message as well. Importantly, board members must create an environment in which employees feel they can seek advice about appropriate business conduct, raise issues, and report misconduct through appropriate channels.

The board of directors must set an example of high-level ethical behaviour and may need intervention in order to stop unethical behaviour, as illustrated by a recent ethics scandal at the Wounded Warrior Project (WWP), a charity and veterans service non-profit. In 2016, the CEO and COO of WWP were fired by the organization's board of directors over allegations by many current and former employees regarding ineffective and wasteful spending of the more than $372 million the organization received in 2015.

The non-profit spent over 40 percent of its funds on overhead—including luxurious employee retreats and first-class airfare, while creating programs for veterans that were effective for marketing purposes but often failed to address the real needs of veterans. Several months after the scandal became public, the WWP board of directors hired a new CEO who ultimately fired more than half of the non-profit's executives, closed several offices, and redirected millions of dollars in spending to programs, including those that provide mental healthcare services, which more directly serve veterans.

3. Establish a Corporate Code of Ethics

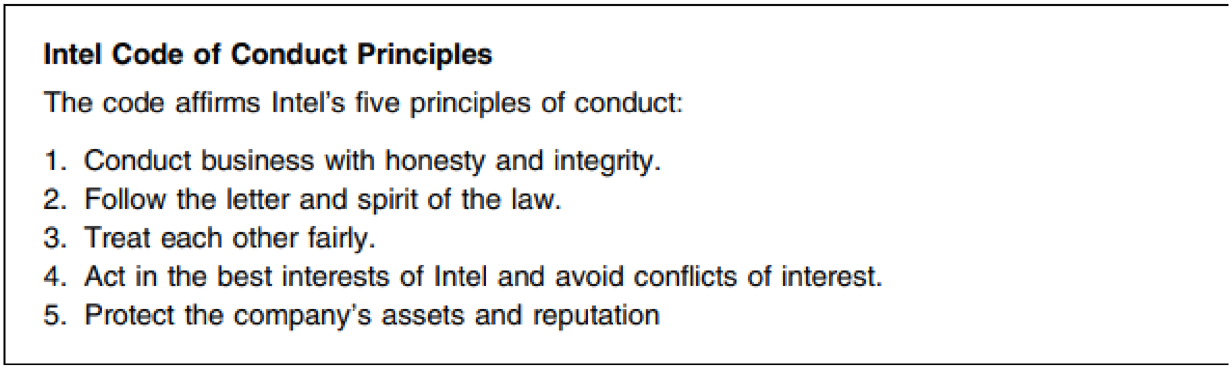
A code of ethics is a statement that highlights an organization's key ethical issues and identifies the overarching values and principles that are important to the organization and its decision making. Codes of ethics frequently include a set of formal, written statements about the purpose of an organization, its values, and the principles that should guide its employees' actions.

An organization's code of ethics applies to its directors, officers, and employees, and it should focus employees on areas of ethical risk relating to their role in the organization, offer guidance to help them recognize and deal with ethical issues, and provide mechanisms for reporting unethical conduct and fostering a culture of honesty and accountability within the organization. An effective code of ethics helps ensure that employees abide by the law, follow necessary regulations, and behave in an ethical manner.

A code of ethics cannot gain company-wide acceptance unless it is developed with employee participation and fully endorsed by the organization's leadership. It must also be easily accessible by employees, shareholders, business partners, and the public. The code of ethics must continually be applied to a company's decision making and emphasized as an important part of its culture.

Each year, Corporate Responsibility magazine rates publicly held U.S. companies, using a statistical analysis of corporate ethical performance in several categories. (For 2016, the categories were environment, climate change, human rights, employee relations, corporate governance, philanthropy and community support, and financial performance.)

Intel Corporation, the world’s largest chip maker, has been ranked in the top 25 every year since the list began in 2000, and was ranked second in 2016. As such, Intel is recognized as one of the most ethical companies in the IT industry. A summary of Intel’s code of ethics is provided below.



Intel Code of Conduct Principles

The code affirms Intel’s five principles of conduct:

1. Conduct business with honesty and integrity.
2. Follow the letter and spirit of the law.
3. Treat each other fairly.
4. Act in the best interests of Intel and avoid conflicts of interest.
5. Protect the company’s assets and reputation

FIGURE 1-6 Intel Code of Conduct Principles

Intel’s Code of Conduct shown in Figure 1-6 applies to all employees and sets expectations for Intel Corporation and its subsidiaries as well as its nonemployee members of the Board of Directors regarding their Intel-related activities.

The Code of Conduct also applies to independent contractors, consultants, suppliers, and others who do business with Intel. Each employee is responsible for reading, understanding, and following the Code. Employees who violate the Code are subject to discipline, up to and including termination of employment. Anyone who violates the law may also be subject to civil and criminal penalties.

4. Conduct Social Audits

An increasing number of organizations conduct regular social audits of their policies and practices. In a social audit, an organization reviews how well it is meeting its ethical and social responsibility goals and communicates its new goals for the upcoming year. This information is shared with employees, shareholders, investors, market analysts, customers, suppliers, government agencies, and the communities in which the organization operates.

In an ongoing effort to engrain socially responsible business behaviour into all business activities, key Dell suppliers undergo a review of their social and environmental progress on a quarterly basis. These reviews include audit performance data, assessment of policy compliance and specific implementation plans for suppliers’ own programs for compliance, and environmental stewardship.

5. **Require Employees to Take Ethics Training**

The ancient Greek philosophers believed that personal convictions about right and wrong behaviour could be improved through education. Today, most psychologists agree with them. Lawrence Kohlberg, the late Harvard psychologist, found that many factors stimulate a person's moral development, but one of the most crucial is education. Other researchers have repeatedly supported the idea that people can continue their moral development through further education, such as working through case studies and examining contemporary issues.

Thus, an organization's code of ethics must be promoted and continually communicated within the organization, from the top to the bottom. Organizations can do this by showing the employees examples of how to apply the code of ethics in real life. One approach is through a comprehensive ethics education program that encourages employees to act responsibly and ethically. Such programs are often presented in small workshop formats in which employees apply the organization's code of ethics to hypothetical but realistic case studies. Employees may also be given examples of recent company decisions based on principles from the code of ethics.

A critical goal of such training is to increase the percentage of employees who report incidents of misconduct; thus, employees must be shown effective ways of reporting such incidents. In addition, they must be reassured that such feedback will be acted on and that they will not be subjected to retaliation.

In its 2013 National Business Ethics Survey, the Ethics Resource Center reported that 81 percent of the surveyed organizations provide ethics training. At IBM, for example, employees around the world take part in the firm's online Business Conduct Guidelines course and certification. This training is available in two dozen languages and presents real-world scenarios that employees may face when conducting business. In addition, senior IBM business leaders sponsor integrity summits that emphasize the role of leaders in creating an ethical culture. The summits also help IBM employees to identify key compliance risks along with specific actions that can mitigate these risks. In addition, IBM provides online ethics and integrity training to almost 20,000 employees of IBM's partners and suppliers around the world.

Formal ethics training not only makes employees more aware of a company's code of ethics and how to apply it but also demonstrates that the company intends to operate in an ethical manner. The existence of formal training programs can also reduce a company's liability in the event of legal action.

6. Include Ethical Criteria in Employee Appraisals

Managers can help employees to meet performance expectations by monitoring employee behaviour and providing feedback; increasingly, managers are including ethical conduct as part of an employee's performance appraisal. Those that do so base a portion of their employees' performance evaluations on treating others fairly and with respect; operating effectively in a multicultural environment; accepting personal accountability for meeting business needs; continually developing others and themselves; and operating openly and honestly with suppliers, customers, and other employees. These factors are considered along with the more traditional criteria used in performance appraisals, such as an employee's overall contribution to moving the business ahead, successful completion of projects and tasks, and maintenance of good customer relations. In a recent survey, about two-thirds of organizations reported that they include ethical conduct as a performance measure in employee evaluations.

7. Create an Ethical Work Environment

Most employees want to perform their jobs successfully and ethically, but good employees sometimes make bad ethical choices. Employees in highly competitive workplaces often feel pressure from aggressive competitors, cutthroat suppliers, unrealistic budgets, unforgiving quotas, tight deadlines, and bonus incentives. Employees may also be encouraged to do "whatever it takes" to get the job done. In such environments, some employees may feel pressure to engage in unethical conduct to meet management's expectations, especially if the organization has no corporate code of ethics and no strong examples of senior management practicing ethical behaviour.

The most important influence on how employees act is their perception of their immediate boss's expectations. If the boss sets the expectation that compliance failures and ethical lapses will not be tolerated, then employees will be less likely to fail.

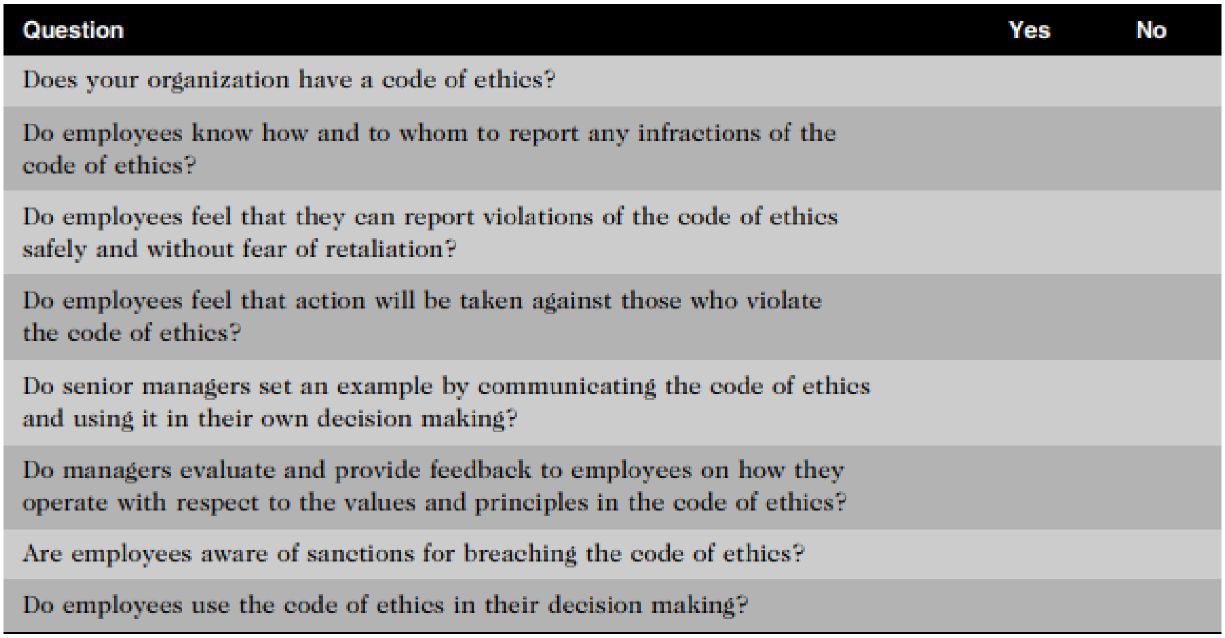
The following list includes several examples of how managerial behaviour can encourage unethical employee behaviour:

- A manager sets and holds people accountable to meet "stretch" goals, quotas, and budgets, causing employees to think, "My boss wants results, not excuses, so I have to cut corners to meet the goals my boss has set."
- A manager fails to provide a corporate code of ethics and operating principles to make decisions, so employees think, "Because the company has not established any guidelines, I don't think my conduct is really wrong or illegal."
- A manager fails to act in an ethical manner and instead sets a poor example for others to follow, so employees think, "I have seen other successful people take unethical actions and not suffer negative repercussions."
- Managers fail to hold people accountable for unethical actions, so employees think, "No one will ever know the difference, and if they do, so what?"

- Managers put a three-inch-thick binder entitled “Corporate Business Ethics, Policies, and Procedures” on the desks of new employees and tell them to “read it when you have time and sign the attached form that says you read and understand the corporate policy.” Employees think, “This is overwhelming. Can’t they just give me the essentials? I can never absorb all this.”

Table 1-4 provides a manager’s checklist for establishing an ethical workplace. The preferred answer to each question is yes.

TABLE 1-4 Manager’s checklist for establishing an ethical work environment



Question	Yes	No
Does your organization have a code of ethics?		
Do employees know how and to whom to report any infractions of the code of ethics?		
Do employees feel that they can report violations of the code of ethics safely and without fear of retaliation?		
Do employees feel that action will be taken against those who violate the code of ethics?		
Do senior managers set an example by communicating the code of ethics and using it in their own decision making?		
Do managers evaluate and provide feedback to employees on how they operate with respect to the values and principles in the code of ethics?		
Are employees aware of sanctions for breaching the code of ethics?		
Do employees use the code of ethics in their decision making?		

Employees must have a knowledgeable resource with whom they can discuss perceived unethical practices. For example, Intel expects employees to report suspected violations of its code of conduct to a manager, the Legal or Internal Audit Departments, or a business unit’s legal counsel. Employees can also report violations anonymously through an internal website dedicated to ethics. Senior management at Intel has made it clear that any employee can report suspected violations of corporate business principles without fear of reprisal or retaliation.

Ethical Considerations in Decision Making

We are all faced with difficult decisions in our work and in our personal life. Most of us have developed a decision-making process that we execute automatically, without thinking about the steps we go through. For many of us, the process generally follows the steps outlined in Figure 1-7 below.

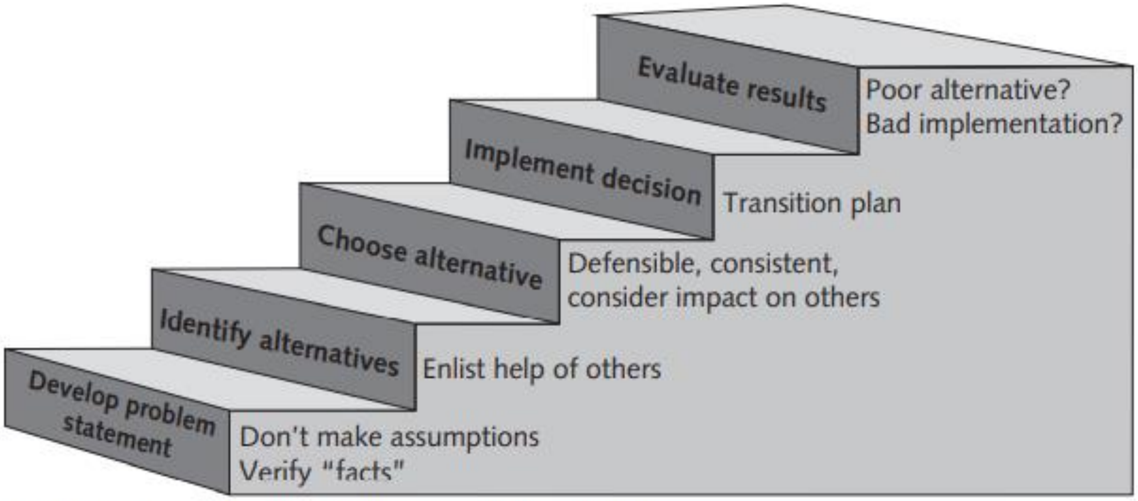


FIGURE 1-7 A five-step ethical decision-making process

The following sections discuss this decision-making process further and point out where and how ethical considerations need to be brought into the process.

1.Develop Problem Statement

A problem statement is a clear, concise description of the issue that needs to be addressed. A good problem statement answers the following questions:

- What do people observe that causes them to think there is a problem?
- Who is directly affected by the problem?
- Is anyone else affected?
- How often does the problem occur?
- What is the impact of the problem?
- How serious is the problem?

Development of a problem statement is the most critical step in the decision-making process. Without a clear statement of the problem or the decision to be made, it is useless to proceed. If the problem is stated incorrectly, the chances of solving the real problem are greatly diminished.

The following list includes good problem statement and poor problem statements:

- **Good problem statement:** Our product supply organization is continually running out of stock of finished products, creating an out-of-stock situation on over 15 percent of our customer orders, resulting in over $300,000 in lost sales per month.
- **Poor problem statement:** We need to implement a new inventory control system. (This is a possible solution, not a problem statement. Pursuing this course of action will surely be expensive and time consuming and, may or may not, solve the underlying problem.)
- **Poor problem statement:** We need to install cameras and monitoring equipment to put an end to theft of finished product in the warehouse. (Again, this is a possible solution, not a problem statement. And are there sufficient facts to support the hypothesis of theft in the warehouse?)

You must gather and analyse facts to develop a good problem statement. Seek information and opinions from a variety of people to broaden your frame of reference. During this process, you must be extremely careful not to make assumptions about the situation and carefully check key facts for validity. Simple situations can sometimes turn into complex controversies because no one takes the time to gather and analyse the real facts.

2. Identify Alternatives

During this stage of decision making, it is ideal to enlist the help of others, including stakeholders, to identify several alternative solutions to the problem. Brainstorming with others will increase your chances of identifying a broad range of alternatives and determining the best solution.

On the other hand, there may be times when it is inappropriate to involve others in solving a problem that you are not at liberty to discuss. In providing participants information about the problem to be solved, offer just the facts, without your opinion, so you don’t influence others to accept your solution.

During any brainstorming process, try not to be critical of ideas, as any negative criticism will tend to shut down the discussion, and the flow of ideas will dry up. Simply write down the ideas as they are suggested and ask questions only to gain a clearer understanding of the proposed solution.

3. Choose Alternative

Once a set of alternatives has been identified, the group must evaluate them based on numerous criteria, such as effectiveness of addressing the issue, the extent of risk associated with each alternative, cost, and time to implement. An alternative that sounds attractive but that is not feasible will not help solve the problem.

As part of the evaluation process, weigh various laws, guidelines, and principles that may apply. You certainly do not want to violate a law that can lead to a fine or imprisonment for yourself or others. Do any corporate policies or guidelines apply? Does the organizational code of ethics offer guidance? Do any of your own morals apply?

Consider the likely consequences of each alternative from several perspectives: What is the impact on you, your organization, other stakeholders (including your suppliers and customers), and the environment? Does this alternative do less harm than other alternatives?

The alternative selected should be ethically and legally defensible to a collection of your co-workers, peers, and your profession's governing body of ethics; be consistent with the organization's policies and code of ethics; take into account the impact on others; and, of course, provide a good solution to the problem.

5.Implement the Decision

Once an alternative is selected, it should be implemented in an efficient, effective, and timely manner. This is often much easier said than done, because people tend to resist change. In fact, the bigger the change, the greater is the resistance to it. Communication is the key to helping people accept a change. It is imperative that someone whom the stakeholders trust and respect answer the following questions

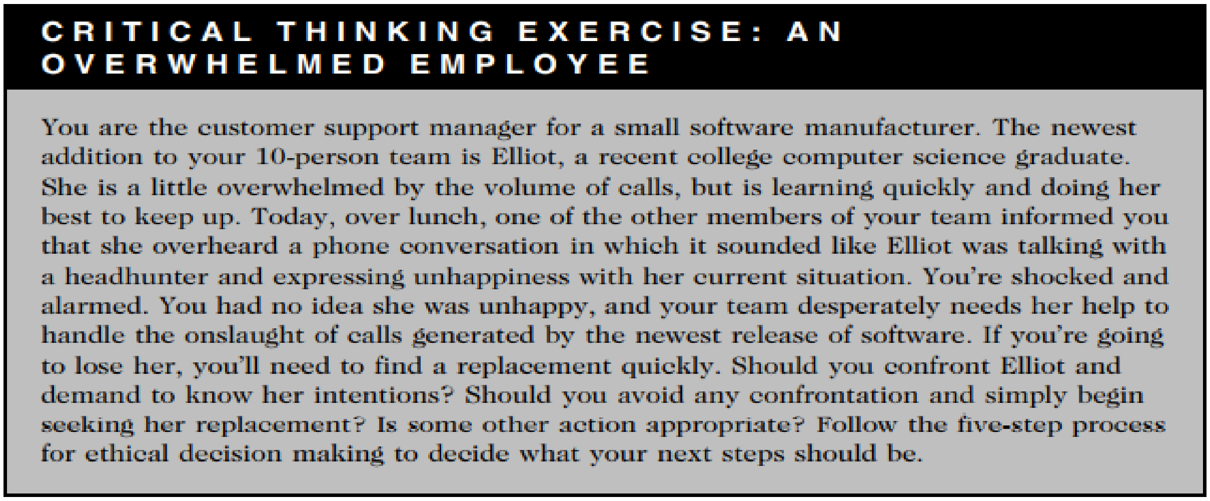
- Why are we doing this?
- What is wrong with the current way we do things?
- What are the benefits of the new way for you?

A transition plan must be defined to explain to people how they will move from the old way of doing things to the new way. It is essential that the transition be seen as relatively easy and pain free. It may be necessary to train the people affected, provide incentives for making the change in a successful fashion, and modify the reward system to encourage new behaviours consistent with the change.

6.Evaluate the Results

After the solution to the problem has been implemented, monitor the results to see if the desired effect was achieved and observe its impact on the organization and the various stakeholders. Were the success criteria fully met? Were there any unintended consequences? This evaluation may indicate that further refinements are needed. If so, return to the problem development step, refine the problem statement as necessary, and work through the process again.

On the other hand, the proper alternative may have been selected, but it was implemented in a poor fashion so the desired results were not achieved. This may require redoing some of the implementation steps.



CRITICAL THINKING EXERCISE: AN OVERWHELMED EMPLOYEE

You are the customer support manager for a small software manufacturer. The newest addition to your 10-person team is Elliot, a recent college computer science graduate. She is a little overwhelmed by the volume of calls, but is learning quickly and doing her best to keep up. Today, over lunch, one of the other members of your team informed you that she overheard a phone conversation in which it sounded like Elliot was talking with a headhunter and expressing unhappiness with her current situation. You're shocked and alarmed. You had no idea she was unhappy, and your team desperately needs her help to handle the onslaught of calls generated by the newest release of software. If you're going to lose her, you'll need to find a replacement quickly. Should you confront Elliot and demand to know her intentions? Should you avoid any confrontation and simply begin seeking her replacement? Is some other action appropriate? Follow the five-step process for ethical decision making to decide what your next steps should be.

Ethics in Information Technology

The growth of the Internet and social networks; the ability to capture, store, and analyse vast amounts of personal data; and a greater reliance on information systems in all aspects of life have increased the risk that information technology will be used unethically. In the midst of the many IT breakthroughs in recent years, the importance of ethics and human values has been underemphasized—with a range of consequences.

Here are some examples that raise public concern about the ethical use of information technology:

- Governments around the world have implemented various systems that enable the surveillance of their citizens and are struggling to achieve the proper balance between privacy and security.

- Many employees have their email and Internet access monitored while at work, as employers struggle to balance their need to manage important company assets and work time with employees' desire for privacy and self-direction.

- Millions of people have downloaded music and movies at no charge and in apparent violation of copyright laws at tremendous expense to the owners of those copyrights.

- Organizations contact millions of people worldwide through unsolicited email and text messages in an extremely low cost, but intrusive marketing approach.

- Hackers break into databases of financial and retail institutions to steal customer information and then use it to commit identity theft—opening new accounts and charging purchases to unsuspecting victims.

- Students around the world have been caught downloading material from the web and plagiarizing content for their term papers.

- Websites plant cookies or spyware on visitors' hard drives to track their online purchases and activities.

Managing IT Worker Relationship

IT workers typically become involved in many different work relationships, including those with employers, clients, suppliers, other professionals, IT users, and society at large. In each relationship, an ethical IT worker acts honestly and appropriately. These various relationships are discussed as follows.

1.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 the 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. Topics addressed in such a manual or code of conduct might include protection of company secrets; vacation policy; time off allowed 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, depending on circumstances (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 issues 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 **Software & Information Industry Association (SIIA) and the Business Software Alliance (BSA)** are trade groups that represent the world's largest software and hardware manufacturers. Part of their mission is to stop the unauthorized copying of software produced by its members. North America has the lowest regional rate of software piracy at 17 percent, which represents a commercial value of $10 billion in lost revenue for software development companies. The global software theft rate for personal computer software is around 43 percent, which equates to a commercial value of $62.7 billion.

SIIA promotes the common interests of the software and digital content industry. It protects the intellectual property of member companies and advocates a legal and regulatory environment that benefits the entire industry. SIIA informs the industry and the broader public by serving as a resource on trends, technologies, policies, and related issues that affect member firms and demonstrate the contribution of the industry to the broader economy. It also provides global services in government relations, business development, corporate education, and intellectual property protection. Over 200 organizations are members of SIIA, including 21st Century Fox, Accenture, Adobe Systems, Bank of America Merrill Lynch, Blackboard, Cengage Learning, Fidelity Investments, Google, Scottrade, Thomson Reuters, and Wells Fargo Bank.

BSA is funded both through dues based on member companies' software revenue and through settlements from companies that commit piracy. BSA membership includes about two dozen global members such as Adobe, Apple, Dell, IBM, Intuit, Microsoft, Oracle, and SAS Institute. BSA investigations are usually triggered by calls to the BSA hotline (1-888-NO-PIRACY), reports sent to the BSA website (www.nopiracy.org), and referrals from member companies. Many of these cases are reported by disgruntled employees or former employees who can receive a monetary reward of thousands of dollars. In 2012 alone, BSA investigated over 15,000 reports of unlicensed software use around the globe.

When the BSA receives what it believes to be a credible tip, it contacts the company and informs it that a tip has been received. It then requests a detailed inventory of all software used by the company, plus evidence of the appropriate licenses for each piece of software. Should the company have insufficient licenses, it has two choices: purchase the required number of licenses and pay BSA a fine, or stonewall and risk the BSA working with the U.S. Marshall's office to obtain a search warrant to search its premises. Strong probable cause evidence is required to obtain the search warrant, but it has been done in the past resulting in expensive and time-consuming litigation, as well as significant business interruption.

Shortly after its one IT staff member left the company, a Texas automotive repair company received a letter from the BSA accusing it of using unlicensed copies of Microsoft software. The company was threatened with a multimillion-dollar fine, one it could not pay and that would force it out of business. To stave off bankruptcy, the company froze salaries and put off the purchase of needed equipment. The dispute was eventually settled for a fraction of the initial amount after the company sought out legal counsel.

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 Core i7-6950K 10-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.

Zillow is an online real estate and rental marketplace that provides information for people interested in buying, selling, renting, financing, and remodelling homes and apartments. Through the company's website and app, users can access a database of more than 110 million U.S. homes—including homes for sale, homes for rent, and even homes not currently on the market.

Zillow also provides a range of services, including one it calls Zestimate, which provides an estimated market value for a house, and a similar service call Rent Zestimate, which estimates the current market rate for rent for a particular property.

Move is a rival company offering similar services. In early 2014, Move's chief strategy officer resigned and, on the same day, joined Zillow as its second highest paid executive. Move filed suit against Zillow, alleging that its former employee, and by extension Zillow, stole trade secrets and proprietary information by copying thousands of document and deleting texts and emails from his company-issued computer and smartphone before resigning. Further, Move alleged that Zillow attempted to cover up the theft. Following more than two years of legal wrangling, Zillow agreed to pay Move a total of $130 million to settle the allegations, with the stipulation that Zillow is not admitting liability in the settlement.

Another issue that can create friction between employers and IT workers is **whistleblowing.** 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 computer 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.

2.Relationships Between IT Workers and Clients

IT workers provide services to clients; sometimes those “clients” are co-workers who are part of the same company as the IT worker. In other cases, the client is part of a different company. 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, 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 the client and the 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 client’s interests.

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 the trustworthiness of its recommendations.

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.

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.

Affinity Gaming, a Las Vegas-based casino with 11 properties located across four states, suffered a data breach in 2013 that enabled hackers to gain access to customers' credit card data. Affinity hired Trustwave, an information security company that provides on-demand threat, vulnerability, and compliance-management services to investigate and contain the breach. Following its investigation, Trustwave claimed that it had identified how the data breach had occurred and had contained the malware responsible for it. However, a year later, Affinity was hit with a second customer data breach. This time, Affinity hired Mandiant, a Trustwave competitor, to conduct an investigation. Mandiant concluded that Trustwave's original work was incomplete and had failed to identify the means by which the attacker had breached Affinity's data security. Affinity sued Trustwave for conducting an allegedly "woefully inadequate" investigation that missed key details of the network breach and enabled subsequent attacks. Affinity alleged that Trustwave made misrepresentations when it claimed that its examination would analyze and help remedy the data breach, when it represented that the data breach was "contained," and when it claimed that its recommendations would address the data breach.

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 non-breaching 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.".

In 2016, Hewlett-Packard Enterprise (HPE) was awarded $3 billion in damages from Oracle after a court determined that Oracle had breached its contract with HPE by dropping support for all Oracle database software being run on HP systems using Intel's Itanium processor chip. HPE argued that Oracle's actions dramatically reduced the sale of HPE's Itanium-based products. HPE also alleged that Oracle's actions were intended to boost sales of Oracle's own Sun hardware. The jury ultimately agreed with HPE and awarded it the full amount it was seeking, compensating the company for both lost sales and damages, as well as requiring Oracle to continue supporting Itanium based systems.

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. Frequent causes of problems in IT projects include the following …

- **Scope creep**—Changes to the scope of the project or the system requirements can result in cost overruns, missed deadlines, and a project that fails to meet end-user expectations.
- **Poor communication**—Miscommunication or a lack of communication between customer and vendor can lead to a system whose performance does not meet expectations.
- **Delivery of an obsolete solution**—The vendor delivers a system that meets customer requirements, but a competitor comes out with a system that offers more advanced and useful features.
- **Legacy systems**—If a customer fails to reveal information about legacy systems or databases that must connect with the new hardware or software at the start of a project, implementation can become extremely difficult.

3.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.

Foxconn Technology, the world's largest electronics contract manufacturer, is headquartered in New Taipei City, Taiwan. The company assembles products for top international brands such as Apple, Nokia, and Sony, and it procures supplies for those products from a wide range of suppliers. In 2014, five former Foxconn employees, including two former senior managers, were charged with bribery for accepting kickbacks from 10 suppliers in exchange for purchasing contracts and assistance clearing Foxconn's quality control checks. Foxconn officials detected the problem and alerted authorities in both Taiwan and China following an internal audit.

Internal control is the process established by an organization's board of directors, managers, and IT systems people to provide reasonable assurance for the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations. An organization's internal control resources include all the people, policies, processes, procedures, and systems controlled by management that enable it to meet these goals .

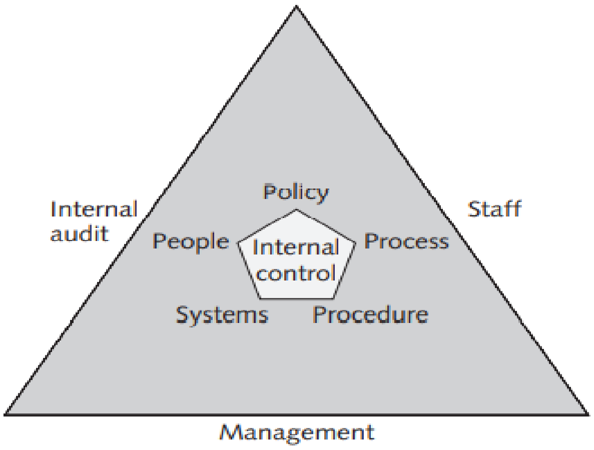


FIGURE 2-2 Internal control

Policies are the guidelines and standards by which the organization must abide. The guidelines and standards are often in response to some law. Policies drive processes and procedures. Processes are a collection of tasks designed to accomplish a stated objective. A procedure defines the exact instructions for completing each task in a process. An organization might have a policy that defines the credit terms and collection guidelines to be followed when handling a customer order. The processes associated with handling customer orders could include creating a new customer account, accepting a new order from an existing customer, and planning shipment of a customer order, among others. Procedures for each process define how to complete each task in the process. The process and procedures must be designed and executed to conform to the credit terms and collection guidelines policy.

Management is responsible for ensuring that an adequate system of internal control is set up, documented with written procedures, and implemented. Management must also decide the proper level of control over various aspects of the business so that the cost of implementing control does not outweigh the benefits. Employees are responsible for following the documented procedures and reporting to management if the controls are not effective in meeting the needs of the organization. The internal audit organization is responsible for assessing whether the internal controls have been implemented correctly and are functioning as designed; the internal audit organization reports its findings to management.

A fundamental concept of good internal controls is the careful separation of duties associated with any process that involves the handling of financial transactions so that different aspects of the process are handled by different people. With proper separation of duties, fraud would require the collusion of two or more parties. When designing an accounts receivable system, for instance, the principal of separation of duties dictates that you separate responsibility for the receipt of customer payments, approving write-offs, depositing cash, and reconciling bank statements. Ideally, no one person should be allowed to perform more than one of these tasks. Internal controls play a key role in preventing and detecting fraud and protecting the organization's resources. Proper separation of duties is frequently reviewed during the audit of a business operation.

In small organizations, it is common for employees to have multiple responsibilities. Separation of duties is often not practical, and internal controls are more likely to be informal and carried out by one or a few people. Such a lack of separation of duties raises concerns that fraud could go undetected. Monitoring and reviewing cash receipt and disbursement activities by supervisory personnel not directly involved with the daily processing is one way to improve internal control within a small organization.

The Foreign Corrupt Practices Act 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 5 years.

Importantly, 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 control, including maintaining books and records that accurately and fairly reflect all transactions—the so-called books and records provision of the act. 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 audited by both internal and outside auditors to ensure that they meet these standards. Thus, it is not enough for an organization to simply direct its employees or agents to not accept or offer bribes; rather, it must also keep a set of books and establish a system of internal control to prevent bribery from occurring.

Hewlett-Packard (HP) agreed to pay $108 million to resolve FCPA-related investigations by the U.S. Department of Justice and the Securities and Exchange Commission into whether HP subsidiaries in Mexico, Poland, and Russia bribed government officials to obtain highly profitable contracts. The investigation revealed that HP's "subsidiaries created a slush fund for bribe payments, employed two sets of books to track bribe recipients, and used anonymous email accounts and prepaid mobile telephones to arrange covert meetings to hand over bags of cash," according to Deputy Assistant Attorney General Bruce Swartz. In a statement issued when the settlement was announced, HP executive vice president and general counsel John Schultz said HP fully cooperated with the investigation and that the misconduct was limited to a small number of people who were no longer employed by the company.

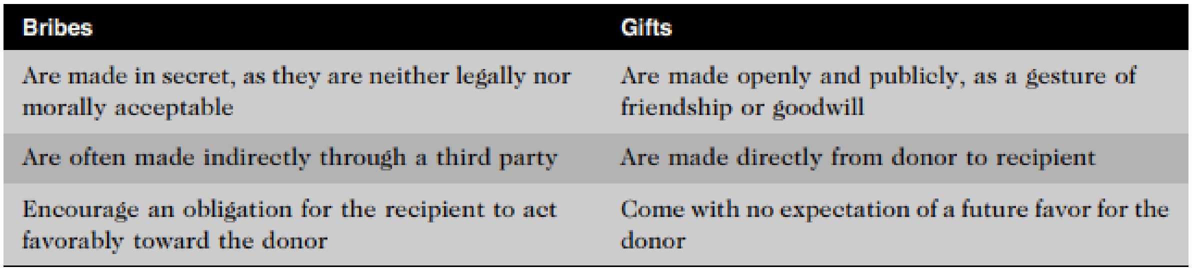
In some countries, gifts are an essential part of doing business. In fact, in some countries, it would be considered rude not to bring a present to an initial business meeting. In the United States, a gift might take the form of free tickets to a sporting event from a personnel agency that wants to get 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 the key 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

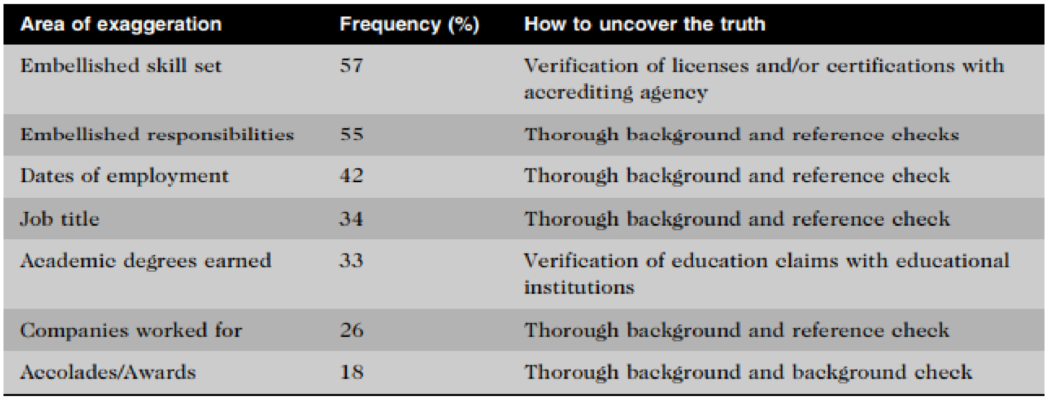
4.Relationships Between IT Workers and Other Professionals

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. For instance, Yahoo hired Scott Thompson, the president of eBay's PayPal electronic payments unit, as its new CEO in January 2012; however, Thompson resigned less than a year later over discrepancies in his academic record summarized on his résumé.17 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.

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	Frequency (%)	How to uncover the truth
Embellished skill set	57	Verification of licenses and/or certifications with accrediting agency
Embellished responsibilities	55	Thorough background and reference checks
Dates of employment	42	Thorough background and reference check
Job title	34	Thorough background and reference check
Academic degrees earned	33	Verification of education claims with educational institutions
Companies worked for	26	Thorough background and reference check
Accolades/Awards	18	Thorough background and background check

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. Revealing such private or confidential information is grounds for termination in many organizations and could even lead to criminal charges.

The Office of Communications (aka Ofcom) is the regulatory and competition authority for the broadcasting, telecommunications, and postal industries in the United Kingdom. In 2016, Ofcom made headlines when one of its former short-term contract employees offered his new employer (UKTV, a multichannel broadcaster jointly owned by BBC Worldwide and Scripps Networks Interactive), six years of confidential income and spending data of competing broadcasters that had been submitted to Ofcom in its regulatory capacity. The data were stolen from Ofcom's market intelligence database and would have provided valuable insights into competitors' programming budgets and revenue streams. UKTV management acted quickly to fire the individual and reported the incident to Ofcom. In a letter to other broadcasters, UKTV promised that it had removed all the data from its systems, assuring its rivals that the data had not been used.

5.Relationships Between IT Workers and IT Users

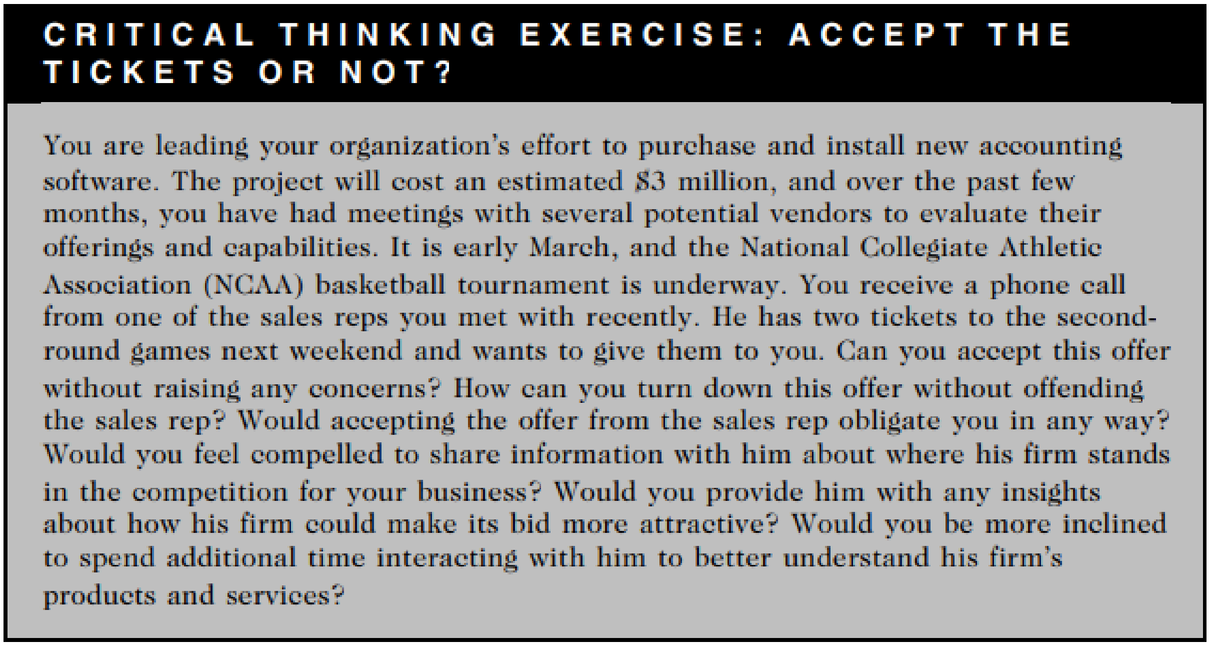
The term IT user refers to a person who uses a hardware or software product; the term distinguishes end users from the IT workers who develop, install, service, and support the product. IT users need the product to deliver organizational benefits or to increase their productivity.

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. They also have a key responsibility to establish an environment that supports ethical behaviors by users. Such an environment discourages software piracy, minimizes the inappropriate use of corporate computing resources, and avoids the inappropriate sharing of information.

6.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 people who live 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.



CRITICAL THINKING EXERCISE: ACCEPT THE TICKETS OR NOT?

You are leading your organization's effort to purchase and install new accounting software. The project will cost an estimated $3 million, and over the past few months, you have had meetings with several potential vendors to evaluate their offerings and capabilities. It is early March, and the National Collegiate Athletic Association (NCAA) basketball tournament is underway. You receive a phone call from one of the sales reps you met with recently. He has two tickets to the second-round games next weekend and wants to give them to you. Can you accept this offer without raising any concerns? How can you turn down this offer without offending the sales rep? Would accepting the offer from the sales rep obligate you in any way? Would you feel compelled to share information with him about where his firm stands in the competition for your business? Would you provide him with any insights about how his firm could make its bid more attractive? Would you be more inclined to spend additional time interacting with him to better understand his firm's products and services?

Encouraging Professionalism of IT Workers

A professional is one who possesses the skill, good judgment, and work habits expected from a person who has the training and experience to do a job well. Organizations including many IT organizations are desperately seeking workers who have the following characteristics of a professional:

- They are an expert in the tools and skills needed to do their job.
- They adhere to high ethical and moral standards.
- They produce high quality results.
- They meet their commitments.
- They communicate effectively.
- They train and develop others who are less skilled or experienced.

IT workers of all types can improve their profession's reputation for professionalism by…

1. Subscribing to a professional code of ethics,
2. Joining and participating in professional organizations,
3. Obtaining appropriate certifications, and
4. Supporting government licensing where available.

Each of these topics is discussed in the following sections.

1.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 behaviour. 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 behaviour. 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 behavioural 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 behaviour**
  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 behaviours 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 census.

2.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 the 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, websites, social media, 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), a computing society founded in New York in 1947, is “dedicated to advancing the art, science, engineering, and application of information technology, serving both professional and public interests by fostering the open interchange of information and by promoting the highest professional and ethical standards.”

ACM is the world’s largest educational and scientific society and is international in scope, with ACM councils established in Europe, India, and China. Over half the organization’s 100,000 student and professional members reside outside the United States in more than 100 countries. Its leading magazine, Communications of the ACM, provides industry news, commentary, observations, and practical research. In addition, the ACM sponsors 37 special-interest groups (SIGs) representing major areas of computing. Each group provides publications, workshops, and conferences for information exchange.

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

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 60,000 members. Founded in 1946, the IEEE-CS is the largest of the 38 societies of the IEEE. The society sponsors many conferences, applications-related and research-oriented journals, local and student chapters, technical committees, and standards working groups.

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.

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.

At no cost, SANS makes available a collection of some 1,200 research documents about various information security topics. 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.

3.Certifications and Licensing

Certification

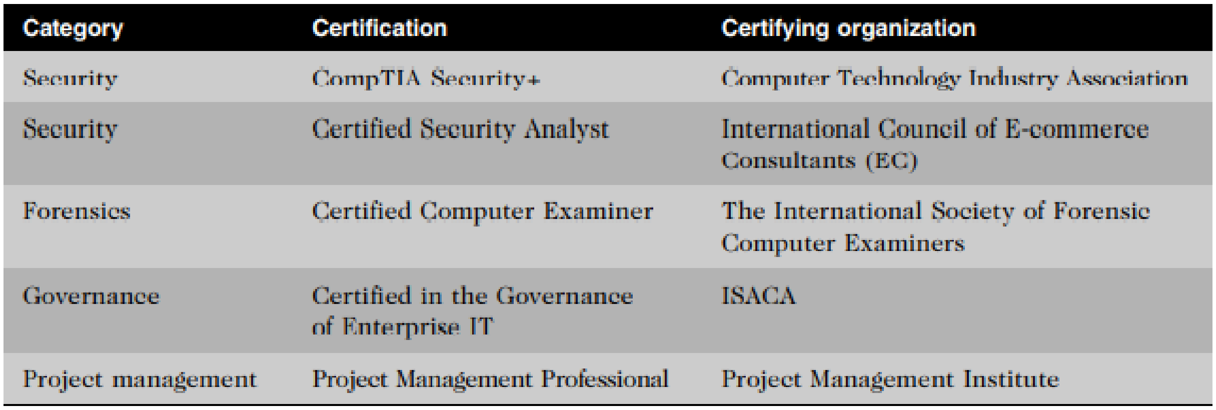
Certification indicates that a professional possesses a particular set of skills, knowledge, or abilities, in the opinion of the certifying organization. Unlike licensing, which applies only to people and is required by law, certification can also apply to products (for example, the Wi-Fi CERTIFIED logo 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?

TABLE 2-3 Common IT industry certifications



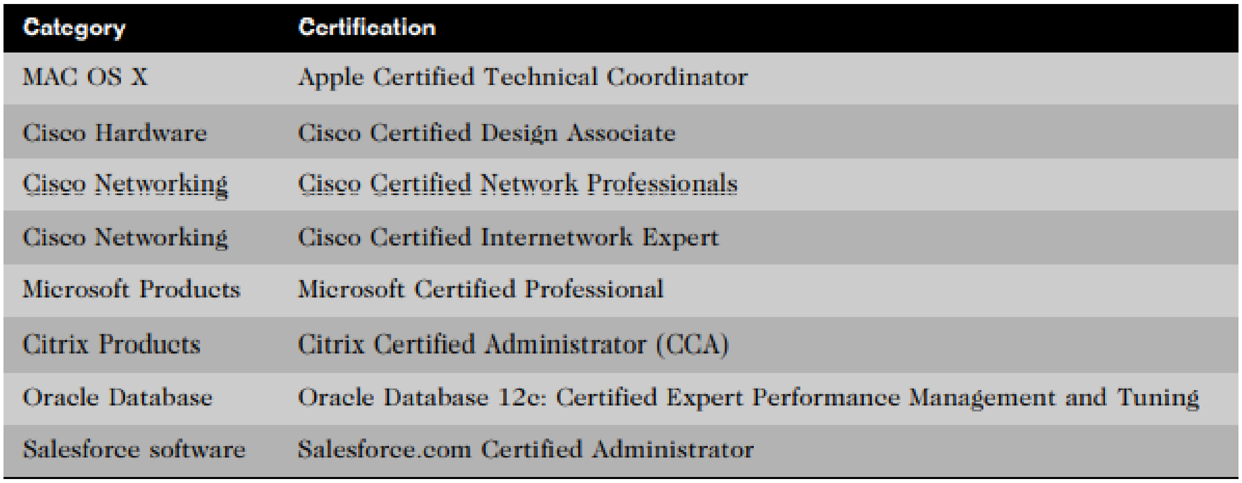
Category	Certification	Certifying organization
Security	CompTIA Security+	Computer Technology Industry Association
Security	Certified Security Analyst	International Council of E-commerce Consultants (EC)
Forensics	Certified Computer Examiner	The International Society of Forensic Computer Examiners
Governance	Certified in the Governance of Enterprise IT	ISACA
Project management	Project Management Professional	Project Management Institute

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. Table below lists some of the common vendor certifications.

TABLE 2-4 Common vendor-specific certifications for IT workers



Category	Certification
MAC OS X	Apple Certified Technical Coordinator
Cisco Hardware	Cisco Certified Design Associate
Cisco Networking	Cisco Certified Network Professionals
Cisco Networking	Cisco Certified Internetwork Expert
Microsoft Products	Microsoft Certified Professional
Citrix Products	Citrix Certified Administrator (CCA)
Oracle Database	Oracle Database 12c: Certified Expert Performance Management and Tuning
Salesforce software	Salesforce.com Certified Administrator

4.Licensing of IT Professionals

In the United States, a government license is government-issued permission to engage in an activity or to operate a business. Most states license activities that could result in damage to public health, safety, or welfare—if practiced by an individual who has no demonstrated minimal competence. Licensing 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 day-care providers, and some engineers.

The Case for Licensing IT Workers

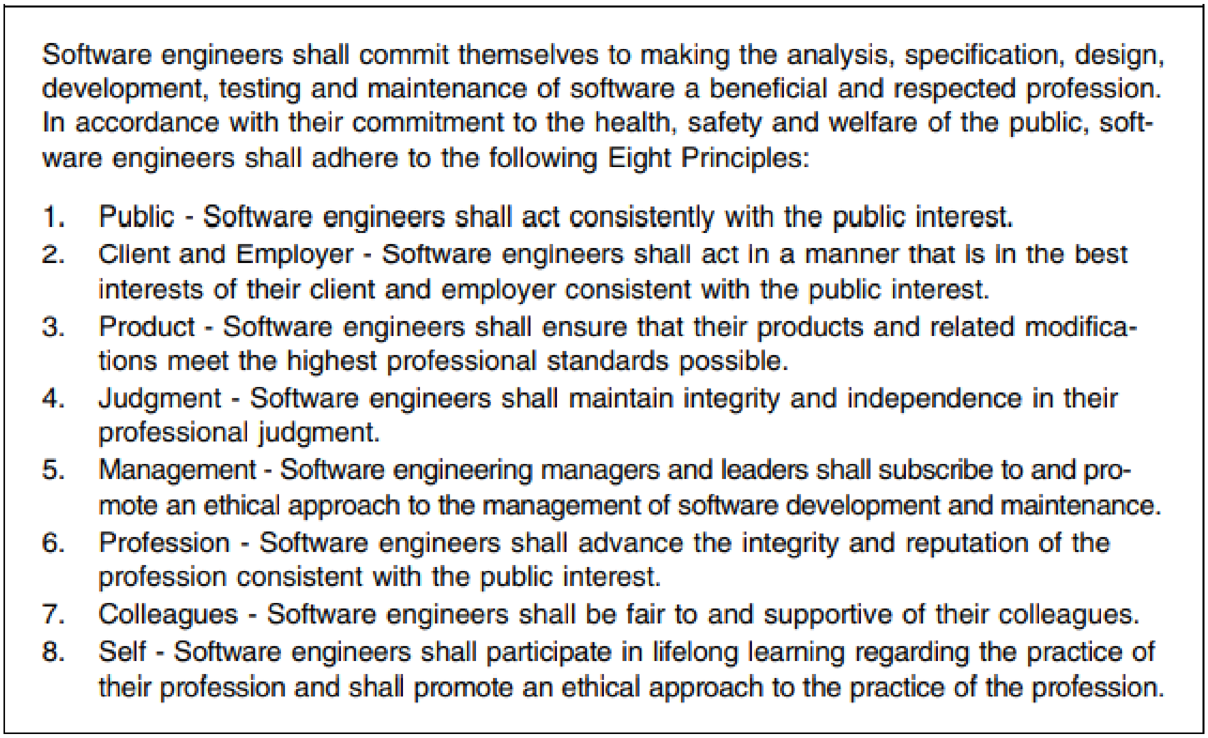
The days of simple, stand-alone information systems are over. Modern systems are highly complex, interconnected, and critically dependent on one another, and every day, the public entrust their health, safety, and welfare to these systems. Software systems are embedded in the vehicles we drive, controlling functions such as braking, cruise control, airbag deployment, navigation, and parking. Even more advanced systems are being designed and built for “self-driving” vehicles.

Complex computers and information systems manage and control the autopilot functions of passenger planes, the nuclear reactors of power plants, and the military’s missile launch and guidance systems. Complex medical information systems monitor hospital patients on critical life support. Failure of any of these systems can result in human injury or even death.

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. Without licensing, there are no clear, well-defined requirements for heightened care and no concept of professional malpractice. State licensing boards have ultimate authority over the specific requirements for licensing in their jurisdiction, and also decide whether or not to even offer a given exam.

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 core body of knowledge for any profession outlines agreed-upon sets of skills and abilities that all licensed professionals must possess.

The "Software Engineering Code of Ethics and Professional Practice" documents the ethical and professional responsibilities and obligations of software engineers. (A software engineer is defined as one who applies engineering principles and practices to the design, development, implementation, testing, and maintenance of software.) After a thorough review process, version 5.2 of the Software Engineering Code of Ethics and Professional Practice was adopted by both the ACM and IEEE-CS as shown in figure below.



Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:

1. Public - Software engineers shall act consistently with the public interest.
2. Client and Employer - Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.
3. Product - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
4. Judgment - Software engineers shall maintain integrity and independence in their professional judgment.
5. Management - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
6. Profession - Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
7. Colleagues - Software engineers shall be fair to and supportive of their colleagues.
8. Self - Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

FIGURE 2-3 Software Engineering Code of Ethics and Professional Practice

Source: Software Engineering Code of Ethics and Professional Practice. © acm.org, 2015. http://www.acm.org/about/se-code

The code contains eight principles related to the behaviour of and decisions made by software engineers, including practitioners, educators, managers, supervisors, and policy makers, as well as trainees and students of the profession.

The non-profit organization National Council of Examiners for Engineering and Surveying (NCEES) develops, administers, and scores the examinations used for engineering and surveying licensure in the United States. Members of NCEES include the licensing boards for all 50 states. In 2013, NCEES began offering testing for software engineers. The eight-hour exam consisting of 80 multiple-choice questions was produced in collaboration with the Institute of Electrical and Electronic Engineers (IEEE).

The software engineering license certifies that the license holder has:

- completed an appropriate engineering education from a program accredited by the Accreditation Board for Engineering and Technology/Engineering Accreditation.
- at least four years of software engineering experience in his or her field (the required years of experience varies by state) working under the supervision of qualified engineers. (This could be a sticking point because there are so few licensed software engineers.)
- passed the following two NCEES engineering exams:
  (1) the Fundamentals of Engineering exam, which is a broad-based exam and
  (2) an eight-hour software engineering Principles and Practices exam, which covers topics such as software requirements, design, construction, testing, maintenance, configuration management, engineering processes, quality assurance, safety, security, and privacy.
- kept current by meeting his or her state's minimum continuing education requirements.

IT Professional Malpractice

For most IT workers, becoming licensed as a software engineer is optional because they practice under the "industrial exemption" clause of their state's licensing laws that permits them to work internally for an organization without licensure so long as they are not making final decisions to release product to the public or offering engineering services directly to the public (for example, software engineering consultant). However, to open a software engineering consulting practice or to claim that one is a software engineer in a formal context may now require a license in some states. For an IT worker to become licensed raises some potential legal issues, as discussed in the following paragraphs.

Negligence is defined as not doing something that a reasonable person would do or doing something that a reasonable person would not do. Duty of care refers to the obligation to protect people against any unreasonable harm or risk. For example, people have a duty to keep their pets from attacking others and to operate their cars safely. Similarly, businesses must keep dangerous pollutants out of the air and water, make safe products, and maintain safe operating conditions.

The courts decide whether parties owe a duty of care by applying a reasonable person standard to evaluate how an objective, careful, and conscientious person would have acted in the same circumstances. Likewise, defendants who have particular expertise or competence are measured against a reasonable professional standard. For example, in a medical malpractice suit based on improper treatment of a broken bone, the standard of measure would be higher if the defendant were an orthopedic surgeon rather than a general practitioner.

In the IT arena, consider a hypothetical negligence case in which an employee inadvertently destroyed millions of customer records in an Oracle database. The standard of measure would be higher if the defendant were a licensed software engineer certified as an Oracle database administrator (DBA) with 10 years of experience rather than an unlicensed systems analyst with no DBA experience or specific knowledge of the Oracle software.

If a court finds that a defendant actually owed a duty of care, it must then determine whether the duty was breached. A breach of the duty of care is the failure to act as a reasonable person would act. A breach of duty might consist of an action, such as throwing a lit cigarette into a fireworks factory and causing an explosion, or a failure to act when there is a duty to do so—for example, a police officer not protecting a citizen from an attacker. Professionals who breach the duty of care are liable for injuries that their negligence causes. This liability is commonly referred to as professional malpractice. For example, a CPA who fails to use reasonable care, knowledge, skill, and judgment when auditing a client's books is liable for accounting malpractice.

Professionals who breach this duty are liable to their patients or clients and possibly to some third parties. In the past, courts have consistently rejected attempts to sue individual parties for computer-related malpractice .

Professional negligence can occur only when people fail to perform within the standards of their profession, and software engineering, until recently, was not a licensed profession in the United States. Because there were no uniform standards against which to compare a software engineer's professional behaviour, he or she could not be subject to malpractice lawsuits.

Encouraging Ethical Use of IT Resources among Users

This section discusses some of the most common ethical issues that IT users face, as well as ways that organizations can encourage the ethical use of IT by their employees, an area of growing concern as more companies provide employees with smartphones, tablets, and laptops—along with PCs, and other devices—to access corporate information systems, data, and the Internet.

Common Ethical Issues for IT Users

1.Software Piracy

Software piracy in a corporate setting can sometimes be directly traceable to IT professionals—they might allow it to happen, or they might actively engage in it. Corporate IT usage policies and management should encourage users to report instances of piracy and to challenge its practice. The software piracy rates in Albania, Kazakhstan, Libya, Panama, and Zimbabwe exceed 70 percent, so it is clear that business managers and IT professionals in those countries do not take a strong stand against the practice.

Sometimes IT users are the ones who commit software piracy. A common violation occurs when employees copy software from their work computers for use at home. When confronted, the IT user's argument might be: "I bought a home computer partly so I could take work home and be more productive; therefore, I need the same software on my home computer as I have at work." However, if no one has paid for an additional license to use the software on the home computer, this is still piracy.

The increasing popularity of the Android smartphone operating system has created a serious software piracy problem. Some IT end users have figured out how to download applications from the Google Play store without paying for them, and then use the software or sell it to others. Indeed, the rate of software piracy for apps from Google's Play store is alarmingly high—exceeding 90 percent for some popular games such as Monument Valley.

The software piracy rate for that some game from Apple's App store is closer to 60 percent. Software piracy can have a negative impact on future software development if professional developers become discouraged watching revenue from legitimate sales sink while the sales of pirated software and games skyrocket.

2.Inappropriate Use of Computing Resources

Some employees use their computers to surf popular websites that have nothing to do with their jobs, participate in chat rooms, view pornographic sites, and play computer games. These activities eat away at a worker's 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. Organizations typically fire frequent pornography offenders and take disciplinary action against less egregious offenders.

3.Inappropriate Sharing of Information

Every organization stores vast amounts of information that can be classified as either private or confidential. Private data describe individual employees—for example, their salary information, attendance data, health records, and performance ratings. Private data also include 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 co-worker's payroll records via a human resources computer system and then discussed them with a friend, it would be a clear violation of the co-worker's privacy.

One of the most serious leaks of sensitive information in the U.S. history occurred in late 2010, when hundreds of thousands of leaked State Department documents were posted on the WikiLeaks' website. 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-scene international diplomacy, often divulging candid comments from world leaders and providing particulars of U.S. tactics in Afghanistan, Iran, and North Korea. The leaked documents strained relations between the United States and some of its allies. It is also possible that the incident will cause other countries to be less willing to share sensitive information with the United States because of concerns over further disclosures.

4.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 behaviour, and enable management to punish violators. Adherence to a policy can improve services to users, increase productivity, and reduce costs. Companies can take several actions when creating an IT usage policy, as discussed in the following sections.

5.Establishing Guidelines for Use of Company Hardware and 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.

6.Defining an Acceptable Use Policy

An acceptable use policy (AUP) is a document that stipulates restrictions and practices that a user must agree to in order to use organizational computing and network resources. It is an essential information security policy—so important that most organizations require that employees sign an acceptable use policy before being granted a user or network ID.

An effective acceptable use policy is clear and concise and contains the following five key elements:

1. Purpose of the AUP—Why is the policy needed and what are its goals?
2. Scope—Who and what is covered under the AUP?
3. Policy—How are both acceptable use and unacceptable use defined; what are some examples of each?
4. Compliance—Who is responsible for monitoring compliance and how will compliance will be measured?
5. Sanctions—What actions will be taken against an individual who violates the policy?

Members of the legal, human resources, and information security groups are involved in creating the AUP. It is the organization's information security group that is responsible for monitoring compliance to the AUP. Information security (infosec) group's responsibilities include managing the processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and nondigital information, whether it is in transit, being processed, or at rest in storage.

Table 2-5 provides a manager's checklist for establishing an effective acceptable use policy. The preferred answer to each question is yes.

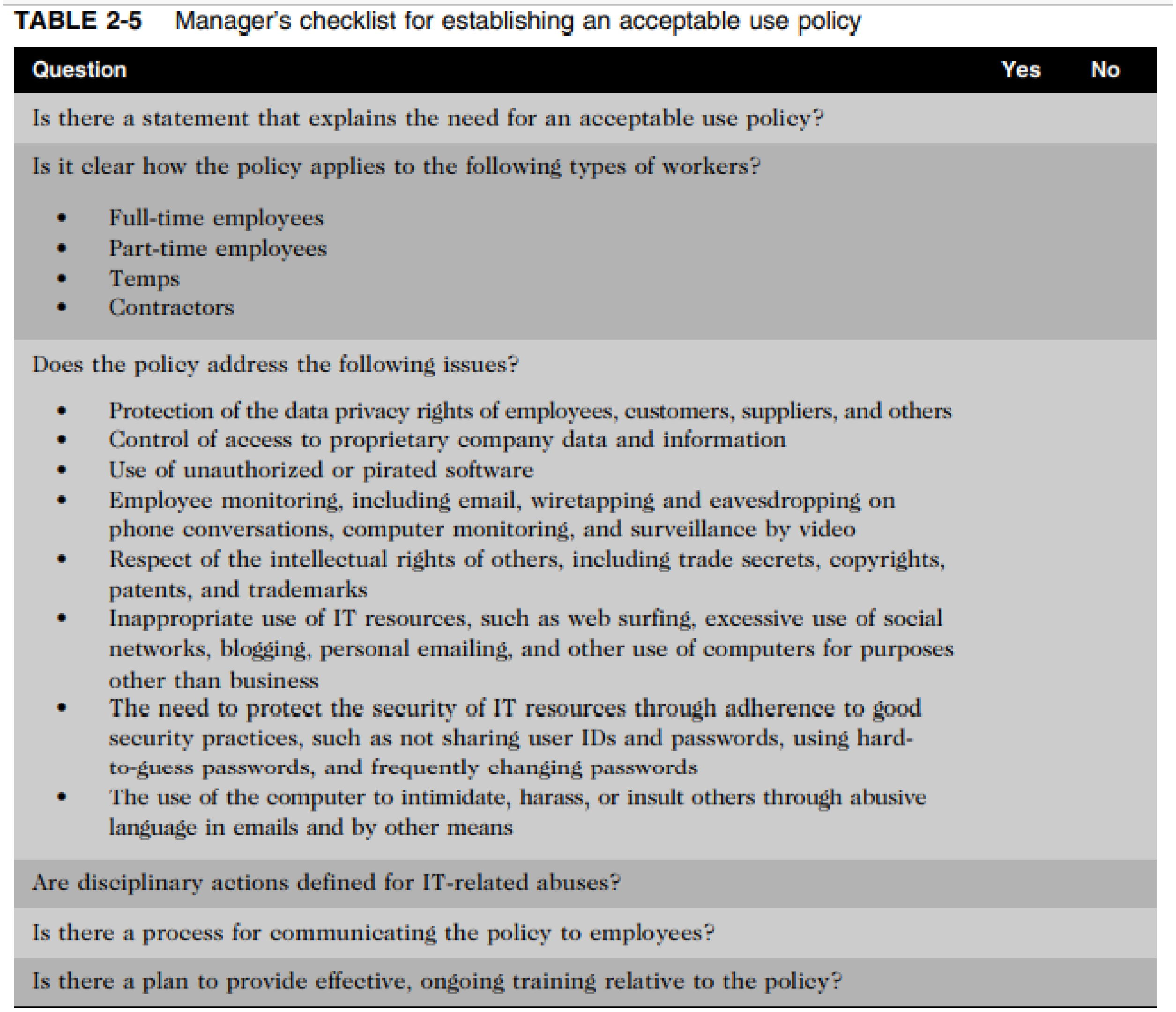


TABLE 2-5 Manager's checklist for establishing an acceptable use policy

Question	Yes	No
Is there a statement that explains the need for an acceptable use policy?		
Is it clear how the policy applies to the following types of workers? • Full-time employees • Part-time employees • Temps • Contractors		
Does the policy address the following issues? • Protection of the data privacy rights of employees, customers, suppliers, and others • Control of access to proprietary company data and information • Use of unauthorized or pirated software • Employee monitoring, including email, wiretapping and eavesdropping on phone conversations, computer monitoring, and surveillance by video • Respect of the intellectual rights of others, including trade secrets, copyrights, patents, and trademarks • Inappropriate use of IT resources, such as web surfing, excessive use of social networks, blogging, personal emailing, and other use of computers for purposes other than business • The need to protect the security of IT resources through adherence to good security practices, such as not sharing user IDs and passwords, using hard-to-guess passwords, and frequently changing passwords • 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?		

6. 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.

8.Installing and Maintaining a Corporate Firewall

A firewall is hardware or software (or a combination of both) that serves as the first line of defense 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 websites. (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 websites, 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.

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 a system of internal control 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 with 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 are gathered, for what purposes the data are 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.

It is a major challenge for many organizations to maintain compliance with multiple government and industry regulations, which are frequently updated and modified so that regulations have similar but sometimes conflicting requirements. For example, the California Online Privacy Protection Act of 2003 was amended in 2013 by Assembly Bill 370, which requires privacy policies to include information on how the operator responds to Do Not Track signals or similar mechanisms; the law also now requires privacy policies to state whether third parties can collect personally identifiable information about the site's users.36

As a result, many organizations have implemented specialized software to track and record compliance actions, hired management consultants to provide advice and training on compliance issues, and even created a new position, the chief compliance officer (CCO), to deal with compliance-related issues.

In 1972, the SEC recommended that publicly held organizations establish audit committees.37 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 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

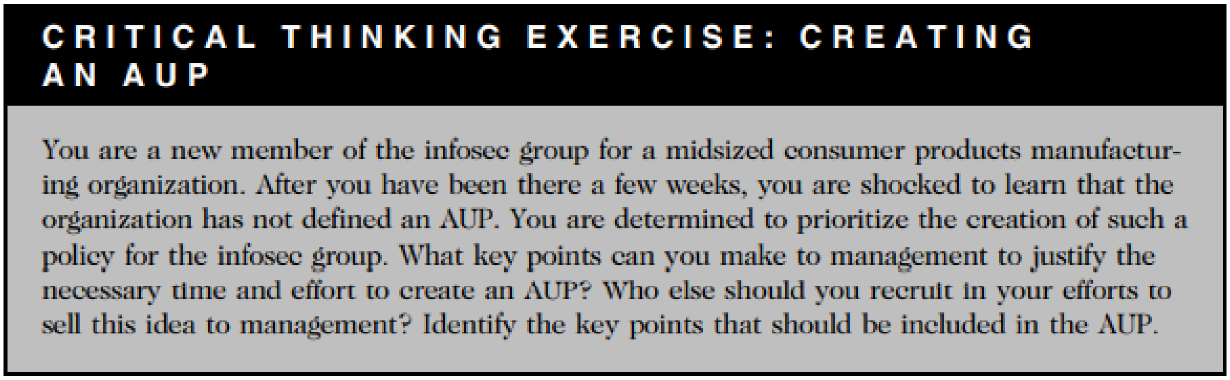
In some cases, audit committees have uncovered violations of law and have reported their findings to appropriate law enforcement agencies.

Marvell Technology Group LTD is a Silicon Valley-based producer of semiconductors and related products. In early 2016, the firm launched an audit committee investigation that scrutinized financial results for several quarters. The audit committee uncovered that in some cases Marvell personnel, IT users, would ask customers to accept delivery of products sooner than they had requested allowing the company to book revenue in earlier quarters. Such transactions were made in response to "significant pressure" from the management on sales teams to meet revenue targets. Such sales reporting accounted for about 9 percent of first quarter revenue in fiscal 2016 and 11 percent for the second quarter. Facing pressure from investors, both the firm's chief executive and its president were fired. In their first conference call with investors, the firm's new management team pledged to discontinue the practice of booking revenue prematurely.38

In addition to an audit committee, most organizations also have an internal audit department whose primary responsibilities include the following:

- ➢ Determine that internal systems and controls are adequate and effective
- ➢ Verify the existence of company's 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

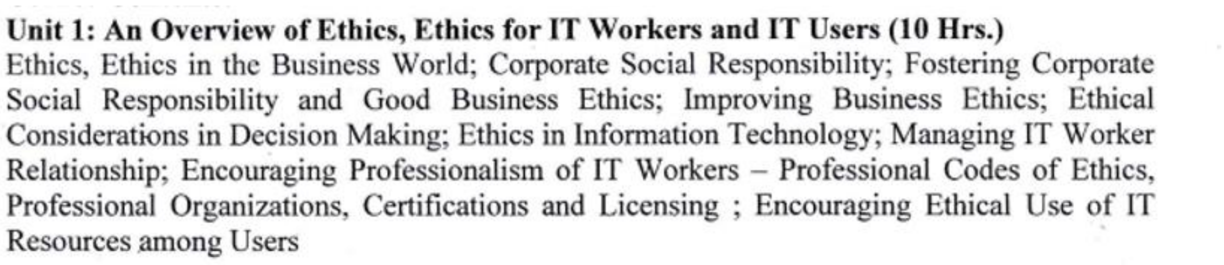
Although the members of the internal audit team are not typically experts in detecting and investigating financial statement fraud, they can offer advice on how to develop and test policies and procedures that result in transactions being recorded in accordance with generally accepted accounting principles (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.



CRITICAL THINKING EXERCISE: CREATING AN AUP

You are a new member of the infosec group for a midsized consumer products manufacturing organization. After you have been there a few weeks, you are shocked to learn that the organization has not defined an AUP. You are determined to prioritize the creation of such a policy for the infosec group. What key points can you make to management to justify the necessary time and effort to create an AUP? Who else should you recruit in your efforts to sell this idea to management? Identify the key points that should be included in the AUP.

========================= End of Unit-1 ================================



Unit 1: An Overview of Ethics, Ethics for IT Workers and IT Users (10 Hrs.)

Ethics, Ethics in the Business World; Corporate Social Responsibility; Fostering Corporate Social Responsibility and Good Business Ethics; Improving Business Ethics; Ethical Considerations in Decision Making; Ethics in Information Technology; Managing IT Worker Relationship; Encouraging Professionalism of IT Workers – Professional Codes of Ethics, Professional Organizations, Certifications and Licensing ; Encouraging Ethical Use of IT Resources among Users