Professional Practice and Ethics Course Notes

Site:	Murang'a University E-learning Portal	Printed by:	Jane Njuki
Course:	Professional Practice and Ethics	Date:	Thursday, 23 June 2022, 1:59 PM
Book:	Professional Practice and Ethics Course Notes		

Table of contents

1. Introduction

Objectives:

i) Explain meaning Code of Conduct
ii) Explain Code of Conduct within IS
iii) Explain Functions of codes of conduct
iv) Explain Licensing
v) Explain Components

1.1. Code of Conduct

A code of conduct is the most common policy within an organization.

This policy lays out the company's principles, standards, and the moral and ethical expectations that employees and third parties are held to as they interact with the organization.

A code of conduct is an integral part of compliance efforts as it provides documentation that an employee or third party has violated company policy if illegal activity arises.

A company's code of conduct is a policy that outlines principles and standards that all employees and third parties acting on behalf of the company must follow.

The code of conduct reviews the organization's mission and values and ties these ideals to professional behavior standards.

In many workplaces, codes of conduct become benchmarks of performance.

A code of conduct serves as a reference point for employees to make better choices on a day-to-day basis.

While every possible ethical dilemma an employee might encounter won't be spelled out, the code should lay out the guiding principles by which employees should act and therefore lead there workforce to make the right decision.

These standards can have massive impacts on how the organization functions, how employees conduct themselves daily, and how the workforce interacts with others on behalf of the organization.

On top of ethical reasons, there are legal reasons for implementing a code of conduct as well. All public organizations in the U.S. (and in most countries)are required by law to have a code of conduct in place. Private organizations would be smart to take note of this as well.

Having a strong, ethical code of conduct is essential to building a culture of compliance throughout an organization.

A code of conduct is an excellent exercise to focus the leadership team on how employees should behave at work and the standards they should uphold.

Code of Conduct in IS

A code of ethics is one method for navigating new ethical waters. A code of ethics outlines a set of acceptable behaviors for a professional or social group.

Generally, it is agreed to by all members of the group. The document details different actions that are considered appropriate and inappropriate.

A good example of a code of ethics is the *Code of Ethics and Professional Conduct* of the Association for Computing Machinery, an organization of computing professionals that includes academics, researchers, and practitioners. Here is a quote from the preamble:

Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).

This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct. Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in Section 4.

In the ACM's code you will find many straightforward ethical instructions such as the admonition to be honest and trustworthy. But because this is also an organization of professionals that focuses on computing, there are more specific admonitions that relate directly to information technology:

- No one should enter or use another's computer system, software, or data files without permission. One must always have appropriate approval before using system resources, including communication ports, file space, other system peripherals, and computer time.
- Designing or implementing systems that deliberately or inadvertently demean individuals or groups is ethically unacceptable.
- Organizational leaders are responsible for ensuring that computer systems enhance, not degrade, the quality of working life. When implementing a computer system, organizations must consider the personal and professional development, physical safety, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

One of the major advantages of creating a code of ethics is that it clarifies the acceptable standards of behavior for a professional group. The varied backgrounds and experiences of the members of a group lead to a variety of ideas regarding what is acceptable behavior. While the guidelines may seem obvious, having these items detailed provides clarity and consistency. Explicitly stating standards communicates the common guidelines to everyone in a clear manner.

A code of ethics can also have some drawbacks. First, a code of ethics does not have legal authority. Breaking a code of ethics is not a crime in itself. What happens if someone violates one of the guidelines? Many codes of ethics include a section that describes how such situations will be handled. In many cases repeated violations of the code result in expulsion from the group.

In the case of ACM: "Adherence of professionals to a code of ethics is largely a voluntary matter. However, if a member does not follow this code by engaging in gross misconduct, membership in ACM may be terminated". Expulsion from ACM may not have much of an impact on many individuals since membership in ACM is usually not a requirement for employment. However, expulsion from other organizations, such as a state bar organization or medical board, could carry a huge impact.

Another possible disadvantage of a code of ethics is that there is always a chance that important issues will arise that are not specifically addressed in the code. Technology is quickly changing and a code of ethics might not be updated often enough to keep up with all of the changes. A good code of ethics, however, is written in a broad enough fashion that it can address the ethical issues of potential changes to technology while the organization behind the code makes revisions.

Finally, a code of ethics could also be a disadvantage in that it may not entirely reflect the ethics or morals of every member of the group. Organizations with a diverse membership may have internal conflicts as to what is acceptable behavior. For example, there may be a difference of opinion on the consumption of alcoholic beverages at company events. In such cases the organization must make a choice about the importance of addressing a specific behavior in the code.

1.2. Elements of a code of Conduct

There are a few common elements that every code of conduct should feature.

i) An ethical code of conduct should include a letter from the CEO, reiterate the company’s values, and outline how violations are handled.

The letter from the CEO should emphasize the organization’s commitment to these standards.

The note is an opportunity to express the leadership team’s prioritization of compliance and ethics.

The code of conduct is a great place to drive the organization’s values home with employees and third parties because they will be signing and therefore agreeing to uphold these standards. Selecting your organization’s values is a critical step in building a flourishing business, and establishing a culture of compliance.

Finally, a code of conduct should inform how violations of the code of conduct are handled internally at the organization and mention the external legal risks. The code should also review the proper channels for reporting misconduct if out-of-line behavior is witnessed.

Best-in-class codes of conduct have a few traits in common.

First, they are regularly reviewed. Updating the organization’s code of conduct on an annual basis ensures that the content is up-to-date and relevant as things are always changing within organizations. The code should be a living, breathing document that is highly relevant to employees and their work.

Second, the signatures are properly managed by a policy deployment solution that tracks signatures and time stamps dates. You can write the best code of conduct in the world, but if you don’t correctly deploy it to your employees and third parties, what was the point?

Strive for your employees and third parties to sign the code of conduct and understand the contents and implications.

Lastly, an effective code of conduct is digestible by the audience it is intended for. It is not inundated with legal speak that only the lawyers at the company can understand but instead written in an uncomplicated format that is easy for all to comprehend. While this may seem like a simple point to emphasize, its impact on the adoption and impact of the code of conduct within an organization can not be overstated.

1.3. Functions of codes of conduct

A code of ethics provides a framework for ethical judgment for a professional. A code cannot be said as totally comprehensive and cover all ethical situations that a professional has to face: It serves only as a starting point for ethical decision-making.

A code expresses the circumstances to ethical conduct shared by the members of a profession. It is also to be noted that ethical codes do not establish the new ethical principles.

Inspiration and Guidance

Codes give a convinced motivation for ethical conduct and provide a helpful guidance for achieving the obligations of engineers in their work.

Codes contribute mostly general guidance as they have to be brief. Specific directions may also be given to apply the code in morally good ways.

Support

Codes always support an engineer who follows the ethical principles. Codes give engineers a positive, a possible good support for standing on moral issues. Codes also serve as a legal support for engineers.

Deterrence and Discipline

Codes act as a deterrent because they never encourage to act immorally. They also provide discipline among the Engineers to act morally on the basis of laws. Codes help to investigate unethical conduct. The investigation on the basis of codes does not overrule the rights of those being investigated.

Education and Mutual Understanding

Codes have to be circulated and approved officially by the professionals, the public and government organizations which concern with the moral responsibilities of engineers and organizations.

Contributing to the profession’s Public Image

Codes help to create a good image to the public of an ethically committed profession. It helps the engineers in an effective manner to serve the public. They also give self-regulation for the profession itself.

Protecting the Status Quo

Codes determine ethical conventions which help to create an agreed upon minimum level of ethical conduct. But they can also suppress the disagreement within the profession.

Promoting Business Interests

Codes help to improve the business interests. They help to moralize the business dealings to benefit those within the profession.

1.4. Limitations Codes of Ethics

1. Codes are restricted to general and vague wordings. Due to this limitation they cannot be applicable to all situations directly. It is also impossible to analyze fully and predict the full range of moral problems that arises in a complex profession.
2. Engineering codes often have internal conflicts. So they can’t give a solution or method for resolving the conflict.
3. They cannot be treated as the final moral authority for any professional conduct. Codes represent a compromise between differing judgements and also developed among heated committee disagreements.
4. Only a few practicing engineers are the members of Professional Societies and so they can not be compelled to abide by their codes.
5. Many engineers who are the members of Professional Societies are not aware of the existence of the codes of their societies and they never go through it.
6. Codes can be reproduced in a very rapid manner.
7. Codes are said to be coercive i.e., implemented by threat or force.

1.5. Licensing

Licensing involves obtaining permission from a company (licensor) to manufacture and sell one or more of its products within a defined market area.

The company that obtains these rights (the licensee) usually agrees to pay a royalty fee to the original owner.

Licensing agreements generate revenues, called royalties, earned by a company for allowing its copyrighted or patented material to be used by another company.

Some examples of things that may be licensed include songs, sports team logos, intellectual property, software, and technology. Licensing agreements ensure that you have legal permission to use another person's or business's property.

TYPES OF LICENSING AGREEMENTS

Patent Licensing

Patents cover science and innovation. Patent licensing agreements are the documents through which a patent owner allows someone else to use their patent.

In practice, patent owners choose to license their patents so that they can have it manufactured and distributed widely.

The individuals and businesses that create patentable material (like new inventions) aren’t usually the same parties that can easily manufacture and distribute it.

It’s easier to allow someone else to handle the business side of the patent while continuing to earn royalty payments.

These are generally the most complex types of license agreements because of everything involved in obtaining and maintaining a patent

Trademark Licensing

Trademarks are signifiers of commercial source, namely, brand names and logos or slogans. Trademark licensing agreements allow trademark owners to let others use their IP.

Most often, trademark owners license their trademarks for commercial goods, like clothing, iPhone cases, or food products.

Copyright Licensing

Copyright is the artwork of the IP world. Copyrights exist in, for example, works of visual art, like paintings, or movies, or songs. Copyrights also exist in characters, like Mickey Mouse.

Copyright licensing agreements are often used for consumer goods, just like trademark licenses. They are also used for distributorships, such as with musical works or movies.

Trade Secret Licensing

Trade secrets are unique, in that they are not registered with the government. Patents, trademarks, and copyrights are most valuable when they have been registered with the federal government. Trade secrets are protected only through their secrecy.

Two of the most famous examples of trade secrets are the formulas for Coca-Cola and the recipe for KFC chicken.

Trade secret licensing agreements often come with non-disclosure agreements (or NDAs). NDAs state that the party receiving certain confidential information cannot share it with anyone.

Exclusive

Exclusive licenses are those that create a unique relationship between the licensor and the licensee. In these types of licensing agreements, the licensor agrees that the licensee is the only one who can make use of the IP. These usually cost more for the licensee.

Non-exclusive

In a non-exclusive license, the licensor may be licensing the IP out to more than one licensee. These types of license agreements usually cost less for the licensee.

Sole

In a sole license, the licensor agrees to use just one licensee, but the licensor reserves the right to continue to use their IP, as well.

There are also two different types of license agreement durations.

Perpetual

A perpetual license is one where the licensee buys the right to use the IP just once and then can use it for a lifetime. Often, these are the more expensive type of license because the licensor won't receive ongoing royalties.

Perpetual licenses can be seen most commonly in software.

Term

A term license is organized one of two ways:

(1)the licensee can pay a one-time fee for a certain term or
(2)the license can pay per use (these are traditional royalties).
Term licenses are much more common across all industries. Although many people don't think of it this way, when you pay Netflix each month, part of that fee is a license to use their proprietary digital software.

According to BrewLong attorney, Ashely Brewer: "Licensing agreements are like lease agreements. A lot depends on the property involved and the relationship of the parties."

Essential Elements of a Licensing Agreement

One of the most lucrative types of business relationships today is one between a licensee and a licensor. In this relationship, the licensor has a product of some sort that they have the legal rights to, but doesn't want to handle the marketing and selling of on its own. The licensee has the time and skills to market a product, but doesn't have a product of its own. The two parties come together and create a licensing agreement that allows the licensee to brand and market the product, and the licensor will get some type of compensation.

The licensing agreement must contain essential elements to ensure that all of the details of how things will work are covered. When done properly, this type of agreement can help prevent conflict and ensure that a healthy business relationship is able to thrive for years to come. The following are some of the most important elements of any good licensing agreement:

Scope of the Agreement

Detailing the scope of the agreement is important because it will identify all of the key components of what it covers. Some points that are often identified in this element include the following

•Exclusivity
•Territory Rights
•Guarantees of Sales
Financial Arrangement

Every licensing agreement is going to have to cover the financial arrangement of the deal. This will include things like how much the licensor gets paid for every item sold (or some other type of financial compensation arrangement), whether there is any payment for the right to use the product itself, and much more.

Time Frame of the Deal

Most licensing agreements will be valid only for a certain length of time. The agreement may have an option to renew the contract or have it modified at that time. In addition to setting a potential end date for the agreement, it is also a good idea to identify dates by which the licensee must have the product available to the market. This helps to ensure that the product is actually being sold so the licensor is not stuck in a deal that is not making any money.

Quality of Products

For many product owners, quality is a big concern for their products. When this is the case, it is essential to include specific requirements regarding the quality of how the products are made, the brands they are being sold under, and much more. One of the more popular ways of doing this is to have a clause that requires the licensor to sign off on all quality and brand decisions before they are made.

Getting Legal Help

As with any other type of contract, licensing agreements need to be written in such a way as to avoid ambiguity and confusion. Whether you are the licensee or the licensor, it is important that you have an experienced attorney there to write or review the contract before it is signed. Contact Carla D. Aikens to go over your situation and get the legal help you need today

2. Professional Ethics

objectives

1. Define term profession
2. To explain Characteristics of a profession
3. Explain the system of professions
4. Explain Professional responsibility
5. Explain Professional ethics.

2.1. Profession

The term ‘Profession’ stands for an occupation which requires some specialized study and training, and the purpose of which is generally to provide skilled services and guidance in lieu of a definite fee or remuneration.

A profession is a calling and implies acquisition of a fond of knowledge, range skills and their application in service of humanity.

They services rendered by a professional may be direct as will the case of teachers and doctors or indirect as is in the case of teacher educators i.e. teacher of a teacher.

This service might be rendered for limited segment of the population or for a limited period of time or phase of life. This service is not rendered to the entire student population which gets graduation or post-graduation, but, it is rendered to those who have aptitude for the profession.

Any professional provides professional service for a limited period of time when his/her clientele are in an institution or within the institutional framework.

A profession can be practiced independently or within an institution or both.

2.2. FUNDAMENTAL CHARACTERISTICS OF A PROFESSION

Great responsibility

Professionals deal in matters of vital importance to their clients and are therefore entrusted with grave responsibilities and obligations. Given these inherent obligations, professional work typically involves circumstances where carelessness, inadequate skill, or breach of ethics would be significantly damaging to the client and/or his fortunes.

Accountability

Professionals hold themselves ultimately accountable for the quality of their work with the client. The profession may or may not have mechanisms in place to reinforce and ensure adherence to this principle among its members. If not, the individual professional will (e.g. guarantees and/or contractual provisions).

Based on specialized, theoretical knowledge

Professionals render specialized services based on theory, knowledge, and skills that are most often peculiar to their profession and generally beyond the understanding and/or capability of those outside of the profession. Sometimes, this specialization will extend to access to the tools and technologies used in the profession.

Institutional preparation

Professions typically require a significant period of hands-on, practical experience in the protected company of senior members before aspirants are recognized as professionals.

After this provisional period, ongoing education toward professional development is compulsory. A profession may or may not require formal credentials and/or other standards for admission.

Autonomy

Professionals have control over and, correspondingly, ultimate responsibility for their own work. Professionals tend to define the terms, processes, and conditions of work to be performed for clients (either directly or as preconditions for their ongoing agency employment).

Clients rather than customers

Members of a profession exercise discrimination in choosing clients rather than simply accepting any interested party as a customer (as merchants do).

Direct working relationships

Professionals habitually work directly with their clients rather than through intermediaries or proxies.

Ethical constraints

Due to the other characteristics on this list, there is a clear requirement for ethical constraints in the professions

Professionals are bound to a code of conduct or ethics specific to the distinct profession (and sometimes the individual). Professionals also aspire toward a general body of core values, which are centered upon an uncompromising and unconflicted regard for the client's benefit and best interests.

Merit-based

In a profession, members achieve employment and success based on merit and corresponding voluntary relationships rather than on corrupted ideals such as social principle, mandated support, or extortion. Therefore, a professional is one who must attract clients and profits due to the merits of his work. In the absence of this characteristic, issues of responsibility, accountability, and ethical constraints become irrelevant, negating any otherwise-professional characteristics.

Morality

The responsibilities inherent to the practice of a profession are impossible to rationally maintain without a moral foundation that flows from a recognition of the singular right of the individual to his own life, along with all of its inherent and potential sovereign value.

2.3. Professionalism

Professionalism means behaving in an ethical manner while assuming and fulfilling your rightful responsibilities in every situation every time, without fail.

To get a bit more granular, one can say that it means, in part, conducting your affairs in such a way as to engender trust and confidence in every aspect of your work.

It means having the requisite ability to be worthy of the confidence others place in you.

It means having already made the right choices so that you attract the right sort of client and work under good circumstances rather than having to continually make the best of bad circumstances and take whatever is tossed your way, regardless of its quality.

Perhaps most importantly, professionalism means, in every situation, willfully gathering responsibility rather than avoiding it. Doing so is important because if you don't acknowledge and assume the onus of responsibility in every aspect of your work you will seldom if ever make the right choice to do what is necessary to achieve consistent success for your employer, your employees, your clients, or yourself.

Distinctions between Professionals and Non-Professionals

A professional makes deliberate choices where others have choices made for them or they simply react to what comes their way.

A professional is afforded the luxury of making deliberate choices because he has made deliberate preparations.

A professional can make deliberate preparations because his understanding of and familiarity with the relevant (professional) landscape informs him on how to prepare. Also, like the chess master, he is trained to understand the inevitable results of hundreds of different patterns; he has disciplined himself to observe the whole board and not just the most immediate features or the area with the most tension in the game,

A professional is seldom caught off-balance. The discipline for deliberate preparation and the understanding that comes with it allow that even when something unexpected or unfamiliar is introduced, a professional can quickly understand its basis and easily extrapolate the appropriate tactic, strategy, or process for ethically and successfully resolving issues.

In this capacity, and most fundamentally, a professional habitually makes the right choices because all of his choices are based on the integrity provided by his moral and ethical foundation. Any choice of expedience over integrity can quite easily be recognized by anyone as the wrong choice. Here, the professional simply acknowledges what is obvious, makes the right choice, and acts deliberately.

2.4. System of Professions

Many groups wish to be considered professional. To achieve this status the group needs to bee organised into a formal unit. They must also demonstrate a domain of activity and that if the group has control over this domain that it will be safer and more effectively run. The group must convince the public that lay people can not adequately judge the group and that only the group themselves are capable of judging themselves. Usually professional monopolies are granted on conditions that they must regulate themselves and that they must further the interests of the public.

This means that a professional group must:

- Convince the public of their special knowledge.
- Show that important social functions are at stake.
- Convince the public to trust the group (usually by means of code of Ethics)

For success the group needs:

- Formal organisation to gives the group monopoly
- Collective autonomy in order to justify individual autonomy for members
- Self regulation

Professional Practice

Modern computing science is an esoteric body of knowledge which is universally used and almost universally opaque.

The computer scientist is in the position of providing for the general public a service which is taken on trust.

In the public domain there is very little DIY (do it yourself) computing because the effort and especially the knowledge needed to create or modify computer systems is beyond the capacities or interests of most users.

In other words, the computer scientist provides a service which must be taken on trust and which, in the early 21st Century, is essential to public life.

A. What constitutes a profession?

The law society defines a profession as follows:

When a profession is fully developed it may be described as a body of men and women

(a) identifiable by reference to some register or record;

(b) recognized as having a special skill and learning in some field of activity in which the public needs protection against incompetence, the standards of skill and learning being prescribed by the profession itself;

(c) holding themselves out as being willing to serve the public;

(d) voluntarily submitting themselves to standards of ethical conduct beyond those required of the ordinary citizen by law

(e) undertaking to take personal responsibility to those whom they serve for their actions and to their profession for maintaining public confidence.

Modern professional codes of ethics cover more relationships than the two basic ones covered by the Hippocratic Code.

In general they also include relationships between employees and employers and between the professional and the public in general.

2.5. Professional Relationships

1. With employers and employees

a. Loyalty

In general employees are expected to show loyalty to their employers - they are expected to recognize and help the employer achieve her ends.

But there are limits to loyalty, for example the employee must retain the right to support the political party of their choice without threat of job loss, and they must not be expected to buy only company products, in preference to the competitor’s.

b. Trade secrets

In a free labour market it is difficult to protect trade secrets. A company can afford to hire a competitor’s employee at a higher price than the competitor if the employee carries information that gives the company a market lead over its competitor.

i) Companies attempt to guard against this practice in several ways.
ii) Employees can be asked to sign agreements promising not to reveal trade secrets.
iii) They can even be asked to agree not to work in the same industry for a set period after they leave a company.
Whether or not the employee has entered into such an agreement, there is a moral sense in which loyalty should carry over beyond the term of employment.

c. Practical issues

As an employer, the protection of workers, and the provision of a safe environment are ethical obligations and sound business practices. It is also a legal obligation.

There are three kinds of health problems that arise in the IT workplace.

>> The first of these are musculoskeletal disorders – MSDs – including the notorious RSI - repetitive strain injury. Additionally a variety of disorders called of upper limb disorders are found among those whose working day involves considerable use of a keyboard.
>>The second kind of disorder is visual.
There is little evidence that work with VDUs can cause disease or permanent damage to the eyes, but it can result in eyestrain - tired eyes or headache - and can also lead to awareness of already existing eye defects such as short sightedness.

>>The third kind of health problem is stress.
Stress can be found in any office work - resulting from the demands of deadlines, for example - but further stress can result from computer work when the system is not well understood, or is not working well. The solutions to these problems are fairly obvious, once recognized it is pretty clear what needs to be done. The Health and Safety Executive has numerous publications on H&S in the workplace, including advice on working with VDUs.

2. With clients

There are roughly three ways the relationship can be seen and it is necessary for a smooth running relationship that there be some agreement about what sort of relationship it is.

>> Essentially the difference concerns the balance in decision making between the company and the client.
>> If the company is seen as the agent of the client, it simply carries out the client’s wishes; it does not make any significant decisions of its own.
>> When it has to make a decision about aspects of design that are not obvious from the client’s wishes, then it must return to the client for clarification.
This is the agency model.

>> At the other extreme, the client may transfer all the decision-making authority into the hands of the company. In this case the company first learns as much as it can about what the client wants and then, during the process of development, makes all the decisions about how best to realize the client’s desires
This latter is the paternalistic model.

>> In between these two extremes is what we might call the partnership model where the client is engaged in making decisions but is advised by the company.

>> The decisions are not entirely the client's, nor are they entirely the company's.
>> Decisions are arrived at through a process of dialogue in which the client expresses her wishes and desires and the company advises on what is possible from a practical and what is advisable from their own point of view of superior experience.
In fact there are not three clearly defined relationships, but a whole spectrum of them.

But it is important to raise the issue of what kind of a decision process is to be adopted in order to avoid confusion and conflict arising later in the development process.

3. With the public in general

Only in the last few decades have professional bodies begun to include responsibilities to the public in their codes of conduct. But clearly professional activities can put the public at risk.

>> The professional may see ways of cutting costs (and thus increasing his profits), but which may create risks to the public (e.g., creating a flight control system).
>> He has no legal obligation to avoid those risks, and doing so does not come into the job specification.
>> But clearly he has a moral obligation to avoid cost cutting where risk is increased.
And in the last few decades the special knowledge that the professional has of possible risks to the public at large has begun to figure in what are considered professional obligations – in some cases these professional obligations are legally established.

>> The UK Disability Discrimination Act 1995, fully in force since October 2004, places a duty on organisations to provide equality of access for disabled people.
=>Web based content can fall under the provisions of the act wherever it is used to provide goods, services, staff information (such as on an intranet) or education.
=> Several kinds of disability need to be recognized:
a. Accessibility

>> Most obvious are blindness and partial-sightedness.
Here technical solutions are available in the form of screen readers, or Braille presentations, but when the standard HTML webpage is supplemented with Flash or JavaScript presentations these solutions no longer work. Also, when information is being presented aurally, and there is no corresponding print version, those with hearing impairment are excluded.

>>Language can also be a problem for those who are not fluent in or familiar with the language of the screen, or they may simply not be able to read very well, through lack of education or cognitive disability.
>> Screen navigation can be a problem for those with motor disability –
some may not be able to use a mouse easily or at all, others may find keyboards difficult or impossible. Websites depending entirely on mouse or on keyboard use will exclude these individuals. Additionally, those with dyslexia can find complex and "busy" websites confusing and unmanageable.

>> There are those whom may be excluded through lack of current technology – they may have a slow computer, a slow connection, or dated or different software.
>> At the most extreme there are those with no IT access at all.
Some cannot afford the hardware, training and support needed to use computers, and/or cannot afford the cost of Internet connection.

In the West local authorities and public libraries make an effort to fill these needs, but in other parts of the world these facilities are simply not available.

It is this problem that is referred to when people speak of social exclusion, or the digital divide.

4. With other professionals

There are two major aspects in relations with other professionals.

>> One is to treat your colleagues with dignity and respect, and the other is to encourage and support fellow members in their professional development and, where possible, provide opportunities for the professional development of new members, particularly student members.
In general it is in the interest of the profession to regulate the behaviour of their members.

>> An individual who does not act in the interest of the client will damage the reputation of the profession as a whole.
And when the trust that people place in the profession is damaged, the people will begin to look for alternative sources of expertise - they will turn to alternative medicine, or begin to practice their own conveyancing

3. Code of Ethics

Objectives

i) Explain Code of ethics and professional conduct (ACM, IEEE and BCS)
ii) Explain Legal Concepts
•Contracts
•Liability
•Breach of contract
iii) Explain Property law and Rights in IT
iv) Explain Accountability and Information Technology

3.1. Introduction to Code of Ethics

A code of ethics is a set of principles and rules used by individuals and organizations to govern their decision-making process, as well as to distinguish right from wrong. They provide a general idea of the ethical standards of a business or organization

A professional code of ethics is designed to ensure employees are behaving in a manner that is socially acceptable and respectful of one another. It establishes the rules for behavior and sends a message to every employee that universal compliance is expected.

The engineers who are represented as professionals, and who belong to a professional society need to have some moral responsibilities. A code of conduct is important for engineers to remain committed to their world.

The engineering societies such as **AAES, ABET, NSPE, IEEE** and **AICTE** have framed these codes of ethics which are helpful to engineers to strengthen the moral issues on their work. The codes of ethics play at least eight important roles such as the following −

Serving and protecting the public − Engineers are in a responsible position where trust and trustworthiness, both are essential. A code of ethics functions as a commitment by the profession as a whole that engineers will serve the public health, safety and welfare.

Guidance − Codes are written in brief yet prove effective in offering general guidance to the engineers. More specific directions may be given in supplementary statements or guidelines, which tell how to apply the code. If needed, the assistance is obtained for further specification.

Inspiration − Codes of ethics, which specify a collective commitment towards a profession, help in motivating the engineers towards ethical conduct. Actually, these codes make one feel really responsible and proud to be a professional thus motivating towards the commitment one should have towards one's profession.

Shared Standards − The standards established should be applicable to all individuals, in their particular professions. With the codes of ethics, the public is assured of engineers with minimum standard of excellence and the professionals are provided a fair way to compete.

Support for Responsible Professionals − The professionals who act ethically have more positive support through these codes. A professional engineer who has the intention to stand by the codes of ethics, can have no harm from immoral professional obligations, as he can reject smoothly yet formally. As well, these codes can provide legal support for engineers criticized for living up to work-related professional obligations.

Education and Mutual understanding − The codes which are widely circulated and officially approved by professional societies, promote a shared understanding among professionals, the public and government organizations about the moral responsibilities of engineers. These codes prompt discussion and reflection on moral issues.

Deterrence and Discipline − The professionals who fail to follow the codes exhibit unethical conduct, which is evident from the disobedience towards their profession. Such an investigation generally requires paralegal proceedings designed to get at the truth about a given charge without violating the personal rights of those being investigated. This might lead to expulsion of those whose professional conduct has been proven unethical, which also leads to loss of respect from colleagues and the local community.

Contributing to the Profession's Image − Codes project the engineers as the professionals of ethically committed profession, which inspires them to work with great commitment and more effectively to serve the public. It can also win greater powers of self-regulation for the profession itself, while lessening the demand for more government regulation.

3.2. Advantages of Codes of Ethics

Let us now see the following advantages of codes of ethics. The codes

- Set out the ideals and responsibilities of the profession.
- Exert a **de facto** regulatory effect protecting both clients and professionals.
- Improve the profile of the profession.
- Motivate and inspire practitioners, by attempting to define their raison d'etre.
- Provide guidance on acceptable conduct.
- Raise awareness and consciousness of issues.
- Improve quality and consistency.

3.3. Code of Ethics for Computing Professionals

1. A Professional member of the Computer Society (CS) shall:

- organise the resources available to him and optimise these in attaining the objectives of his organisation,
- use the codes of practice conveyed by the CS from time to time in carrying out his tasks,
- not misuse his authority or office for personal gains,
- comply with the laws relating to the management of his organisation particularly with regard to Privacy and Piracy, and operate within the spirit of these laws,
- conduct his affairs so as to uphold project and further the image and reputation of the CS
- maintain integrity in research and publications.

2. As regard his ORGANISATION a Computing professional should:

- act with integrity in carrying out the !awful policy and instructions of his organisation and uphold its image and reputation,
- plan, establish and review objectives and tasks for himself and his subordinates which are compatible with the Codes of Practice of other professionals in the enterprise, and direct all available effort towards the success of the enterprise rather than of himself,
- fully respect the confidentiality of information which comes to him in the course of his duties, and not use confidential information for personal gain or in a manner which may be detrimental to his organisation or his clients,
- not snoop around in other people's computer files,
- in his contacts and dealings with other people, demonstrate his personal integrity and humanity and when called to give an opinion in his professional capacity, shall, to the best of his ability, give an opinion that is objective and reliable.

3. As regards the EMPLOYEES, a Computing professional should:

- set an example to his subordinates through his own work and performance, through his leadership and by taking account of the needs and problems of his subordinates,
- develop people under him to become qualified for higher duties,
- pay proper regard to the safety and well-being of the personnel for whom he is responsible,
- share his experience with fellow professionals.

4. As regards the CLIENTS, a Computing professional should:

- ensure that the terms of all contracts and terms of business be stated clearly and unambiguously and honoured,
- in no circumstance supply inherently unsafe goods or services,
- not use the computer to harm other people or to bear false witness,
- be objective and impartial when giving independent advice.

5. As regards the COMMUNITY, a Computing professional should:

- make the most effective use of all natural resources employed,
- be ready to give professional assistance in community affairs,
- not appropriate other people's intellectual output,

always use a computer in ways that ensure consideration and respect for fellow humans

3.4. Computer Ethics

Computers with Internet raise a host of difficult moral issues, many of them connected with basic moral concerns such as free speech, privacy, respect for property, informed consent and harm. To evaluate and deal with these issues, a new area of applied ethics called Computer Ethics has come up. These ethics are related to all the computer professionals such as programmers, analysts, operators, designers, etc. along with the users.

The ten commandments of Computer Ethics, created in 1992 by the Computer Ethics Institute consists of the following −

One should **never** use a computer −

- To harm the people (anti-social activities)
- To interfere with other's work (illegal manipulations)
- To snoop into other's files (malware)
- To steal a computer/data (hacking)
- To bear false witness (manipulation and morphing)
- To use/ copy a software you didn't pay for (like illegal downloads and usages)
- To use or copy other's software without compensations (illegal pirated versions)
- To use other's intellectual output inappropriately (violating IPR)
- Doing without thinking of social consequences of the program being written (libeling)
- Always use a computer ensuring consideration and respect towards fellow beings.

However, these ethics are facing lax in today's world. A very small section of concerned individuals seems to be following these ethics. A large section seems to be violating these ethics. With this, there is an unprecedented increase in cybercrime.

Role of Computers in Technological Development

In this section, we will discuss the role of Computers in Technological Development. The limitations of Internet usage and free speech are to be known clearly by every netizen. In this digital era, the morals expected from a human being are the basic tools that control the unethical and sleazy manner of handling the internet.

Internet which is now a global network of networks, initially used the infrastructure of the telephone system and is now being handled by many telecommunication systems by wire, fiber or wireless systems. The Internet provides a spring of new ways to be in contact with other people and with sources of information. It has also created greater convenience in ordering consumer items, paying bills and **social experiments** trading stocks and bonds. Like other major , it also has raised a host of new issues. One set of issues centers on free speech, including control of obscene forms of pornography, hate speech, spam which is unwanted commercial speech and libel. Computers contribute to greater centralization or decentralization insofar as human decision makers direct them.

There come issues which call for trouble wherein, computers are used in embezzlement and other forms of stealing money or financial assets. The issues concerning theft of software and information is again a similar one. The computers are centrally involved when an unauthorized person uses a telephone computer system to obtain private phone numbers or when maliciously alters or scrambles the programming of a telephone computer. In today's world, malicious people have come up with not one but various ways of exploiting money, goods, services, assets, etc. through the computers and internet. The Internet besides easing our work has also paved way to gather an individual's confidential details easily.

The two main factors that make computers troublesome are their speed and geographical coverage, which allows the masses to be victimized further. The difficulty lies in tracing the underlying transactions to apprehend the thieves. This problem is compounded when the communication lines linking the computers involved cross national boundaries.

The most commonly discussed cases of computer abuse are instances such as −

- The stealing or cheating by employees at work.
- The stealing by non-employees or former employees.
- The stealing from or cheating clients and consumers.
- The violation of contracts for computers sales or services.
- The many conspiracies to use computer networks to engage in widespread fraud.

Alarmingly, the Internet has led to an explosion of identity theft, in which personal information is obtained and used to forge documents and commit fraud.

Privacy Factors

The misuse of Internet also influences privacy factors. The illegal attackers or hackers get access to restricted data which is a security threat.

- The inappropriate access which leads to security breach in an office leads to the leakage of confidential information which might severely affect the growth of the company.
- The hackers who crack the security and get unauthorized entry into the highly secured information zone, tend to copy the content or they may change the content, delete the content or get it affected with virus as soon as the authorized personnel opens the file.
- The different types of viruses such as Trojan Horse, Memory Resident, Overwrite, Browser Hijacker, Directory Virus, etc. can create instances wherein, the data on computer system get affected in various ways.
- The legitimate access to information is restricted to protect individual privacy, national security and freedom within a capitalist economy to protect proprietary information essential in pursuing corporate goals.
- The Privacy Act of 1947 prohibits the information contained in government files from being used for purposes beyond those for which it was originally gathered.

4. Legal Concepts

Objectives

Explain the application of the following

- Legal Concepts
- Contracts
- Liability
- Breach of contract

4.1. Introduction to Legal Concepts

Law is defined as part of everyone's life, a living part, a determining part, a controlling and giving part. It concerns people; it's alive.

Historic Perspective of:

1. **Common Law**

The term common law is used in two contexts.

- Originally it meant the law that was not confined to one particular area, but was administered in the whole of England. There was a danger that this description may lead the younger reader to believe that the statutory law is also included in the term common law because the statutory law applies to the country as a whole.
- The term now is used to signify the law which originated in the ancient customs and was developed by judges on the principle of stare decisi.We can conclude that common law that is today consists of the whole non-statutory law of England, excluding the law of equity.

Common Law courts

- *The Court of Exchequer*: This was the first court to be established in the 12th century to deal with disputes concerning the payment of royal revenues.
- *The Court of Common Pl*eas: This was the 2nd court to be established in the 13th century to deal with all civil cases and matters relating to land.
- *The Court of King's Bench*: This was the last to be setup in the 13th century. It's called the King's Bench because occasionally the king used to preside over this court. It mainly dealt with criminal matters and civil actions.

2. **Equity Law**

Equity was defined by Maine as 'a fresh body of rules by the side of the original law, founded on distinct principle and claiming to supersede in virtue of superior sanctity inherent in those principles'.

It is also a set of rules formulated and administered by the Court of Chancery before 1873 to supplement the rules of common law.

Origin of Equity

Citizens dissatisfied with the decisions of the judges of common Law court often made petitions to the King in Council .for a time these petitions were decided by the King himself or by his Council, and then later he delegated this function to his Lord Chancellor

Contributions of Equity Law

Equity moved slowly to supplement the rules of common law; it made its contributions in the following areas;

- It granted injunctions and would order specific performance where common law could award only damages.
- It recognized trust and a beneficiary could compel a trustee to administer the trust property in accordance with terms of the trust.
- It recognized equitable doctrine of part-performance and mortgagor's right to redemption of mortgaged property

Principles of equity

During the early development of equity the early chancellors acted as their own discretion, but eventually they did follow the decisions of earlier Chancellors.Thus,by 8th century, some firm rules of equity were established which guided later Chancellors in deciding disputes. Some of these maxims are;

- He who seeks equity must do equity.
- He who comes to equity must come with clean hands.
- Equity is equal.
- Equity looks to intent rather than form.
- Equity looks on that as done which ought to be done.

3. Criminal Law

A crime may be described as an act, default or conduct prejudicial to the community, the commission of which, by law, renders the person responsible liable to be prosecuted and punished accordingly.

Prosecution for crimes is always conducted in the name of the State.

It is the duty of the prosecution to establish the guilt of the accused beyond any reasonable doubt.

Crimes include offences like murder, rape, grievous bodily harm, robbery, theft etc

All these offences are included in the Penal Code of Kenya., the punishment of crime ranges from hanging to a fine

The term **criminal law**, sometimes called **penal law**, refers to any of various bodies of rules in different jurisdictions whose common characteristic is the potential for unique and often severe impositions as punishment for failure to comply. Criminal punishment, depending on the offense and jurisdiction, may include execution, loss of liberty, government supervision (parole or probation), or fines. There are some archetypal crimes, like murder, but the acts that are forbidden are not wholly consistent between different criminal codes, and even within a particular code lines may be blurred as civil infractions may give rise also to criminal consequences. Criminal law typically is enforced by the government, unlike the civil law, which may be enforced by private parties.

Criminal law history

The first civilizations generally did not distinguish between civil and criminal law. The first written codes of law were produced by the Sumerians. Around 2100-2050 BC Ur-Nammu, the Neo-Sumerian king of Ur, enacted the oldest written legal code whose text has been discovered: the Code of Ur-Nammu although an earlier code of Urukagina of Lagash is also known to have existed. Another important early code was the Code Hammurabi, which formed the core of Babylonian law. These early legal codes did not separate penal and civil laws.

The similarly significant Commentaries of Gaius on the Twelve Tables also conflated the civil and criminal aspects, treating theft or furtum as a tort. Assault and violent robbery were analogized to trespass as to property. Breach of such laws created an obligation of law or vinculum juris discharged by payment of monetary compensation or damages.

The first signs of the modern distinction between crimes and civil matters emerged during the Norman Invasion of England. The special notion of criminal penalty, at least concerning Europe, arose in Spanish Late Scolasticism , when the theological notion of God's penalty (poena aeterna) that was inflicted solely for a guilty mind, became transfused into canon law first and, finally, to secular criminal law. The development of the state dispensing justice in a court clearly emerged in the eighteenth century when European countries began maintaining police services. From this point, criminal law had formalized the mechanisms for enforcement, which allowed for its development as a discernible entity

4. International law

This term is commonly used for referring to the system of implicit and explicit agreements that bind together nation-states in adherence to recognized values and standards, differing from other legal systems in that it concerns nations rather than private citizens. However, the term "International Law" can refer to three distinct legal disciplines:

- Public international law, which involves for instance the United Nations, maritime law, international criminal law and the Geneva conventions.
- Private international law, or conflict of laws, which addresses the questions of which legal jurisdiction may a case be heard; and also the law concerning which jurisdiction(s) apply to the issues in the case law of supranational organizations, which concerns at present regional agreements where the special distinguishing quality is that laws of nation states are held inapplicable when conflicting with a supranational legal system.

The two traditional branches if of the field are:

- jus gentium — law of nations
- jus inter gentes — agreements among nations

5. Public law

Is a theory of law governing the relationship between individuals (citizens, companies) and the state. Under this theory, Constitutional law, administrative law and criminal law are sub-divisions of public law. This theory is at odds with the concept of Constitutional law, which requires all law to be specifically enabled, and thereby sub-divisions, of a Constitution.

Generally speaking, private law is the area of law in a society that affects the relationships between individuals or groups without the intervention of the state or government. In many cases the public/private law distinction is confounded by laws that regulate private relations while having been passed by legislative enactment. In some cases these public statutes are known as laws of public order, as private individuals do not have the right to break them and any attempt to circumvent such laws is void as against public policy.

Areas of public law

- Constitutional law deals with the relationship between the state and individual, and the relationships between different branches of the state, such as the executive, the legislative and the judiciary.

- Administrative law refers to the body of law which regulates bureaucratic managerial procedures and defines the powers of administrative agencies.
- Criminal law involves the state imposing sanctions for crimes committed by individuals so that society can achieve justice and a peaceable social order

6. Private law

As most U.S. states share a heritage with English law, the private law of the United States is generally called the common law (as it is in other Anglo-American common law jurisdictions). Some states, such as New York, have strong civil law influences, and have enacted laws relating to obligations such as the General Obligations Law and the General Business Law.

Public/private law distinction

The distinction between the public and the private in law is often a hazy one. Many consumer protection laws are of a public law nature, which limits the ability of companies dealing with consumers to engage in transactions that fail to respect the rights of consumers. Most laws that impose criminal penalties are considered to be public laws, as these are intended to protect all members of society and not just the areas of interaction covered by contract and tort.

JUDICIAL SYSTEM

Kenya’s Judiciary is established under chapter IV of the Constitution. The country’s superior courts of record are the Court of Appeal and the High Court. The High Court has unlimited original jurisdiction in all civil and criminal matters as well as appellate jurisdiction over matters emanating from the magistrate’s courts and statutory tribunals. The Court of Appeal, on the other hand, exercises appellate jurisdiction over the decisions of the High Court.

The Judges of the High Court and the Court of Appeal are appointed by the President acting in accordance with the advice of the Judicial Service Commission. The Constitution prescribes a minimum of eleven judges for the High Court and two for the Court of Appeal. Presently, there are 46 Judges of the High Court and eight Judges of Appeal. The Chief Justice is a member of both courts.

In the lower hierarchy of the court system are the Magistrates’ Courts and the Kadhis’ Court. The former are established under an Act of Parliament under a power donated by the Constitution and their jurisdiction has limitations defined both by geography and the nature or value of the subject matter. They deal with both civil and criminal matters and are responsible for the bulk of the litigation carried on in Kenya’s justice system. The jurisdiction of the Kadhis’ Courts is constitutionally limited to the determination of questions of Muslim law relating to personal status, marriage, divorce or inheritance in proceedings in which all the parties profess the Muslim religion.

Kenya’s court hierarchy consists of the Court of Appeal, High Court, resident and district magistrates’ courts, and *kadhis* courts, which adjudicate Muslim personal law concerning personal status, marriage, divorce, and inheritance among Muslims. Kenya’s president appoints judges, including the chief justice, who presides in the Court of Appeal. The High Court is responsible for judicial review. Kenya accepts compulsory International Court of Justice jurisdiction, with reservations. The judiciary is constitutionally independent, and judges have security of tenure. This constitutional status and the theoretical life tenure of judges have not, however, ensured immunity from executive-branch pressure.

Court of Appeal.

The Kenya Court of Appeal serves as the Supreme Court of the country. It has final appellate jurisdiction in both criminal and civil cases. Appeals are brought to the Court of Appeal from the Kenya High Court.

The Court of Appeal is made up of the Chief Justice and three other members. The Court of Appeal has the power, authority, and jurisdiction over the court from which the appeal originated.

Appeals from any Kenyan Court to the Privy Council in England are no longer allowed. Kenya Court of Appeal sits mostly in Nairobi, the capital of Kenya but travels on circuit to other principal towns in Kenya to hear appeals.

High Court.

The High Court has original jurisdiction for certain serious crimes and hears appeals from the lower courts. It can adjudicate the constitutionality of acts of the National Assembly and enforcement of the Bill of Rights. The High Court is the second highest court and is presided over by judges of the High Court (puisne judges). The high court can attend to any civil case. In criminal matters however, Kenya High Court only hears cases of murder and treason. On all other criminal cases, the High Court only attends to appeals from subordinate courts.

The Chief Justice is also a member of the High Court. The High Court can also act as assize courts, moving from one region to another.

Resident Magistrate's Courts.

The Resident Magistrate's Courts are presided over by either a senior resident magistrate or a resident magistrate. There is a Resident Magistrate's Court in each province, each of which can hear both serious and non-serious criminal cases.

Appeals from this court are brought to the High Court. The Resident Magistrate's Court is divided into First, Second, and Third Class, which differ according to the severity of punishment they are empowered to impose.

District Magistrate's Courts.

The District Magistrate's Courts are based at every district headquarters. There is a District Magistrate's

Court in every province. The District Magistrate's Courts are also qualified to hear cases involving African customary law. Like the Resident Magistrate's Court, this court is also divided into three classes.

2. Special Courts.

Traditional Courts.

A chief or a council of elders at the village level can try minor criminal cases. The case decisions are accepted as final for certain customary issues (Constitution of Kenya, 1963).

Kadhi's Courts.

The Kadhi's courts exist at the same hierarchical level as the Resident Magistrate's Court. However, they mainly try criminal cases involving personal Muslim law. Both parties to the case must be of Muslim faith (Nyachae and Kinuthia, 1993). Kadhi's Courts are subordinate courts that determine cases relating to personal status, marriage, divorce and inheritance in proceedings in which all the parties profess the Muslim religion.

JUDGES

* Number of judges.

The High Court has a total of twelve justices including the Chief Justice.

* Appointment and qualifications.

The Chief Justice, who is appointed by the President of the Republic, is also the President of the Court of Appeal and a member of the High Court. The President of the Republic appoints other judges of the Court of Appeal and appoints the judges of the High Court upon the advice of the Judicial Service Commission.

The Resident Magistrates are appointed by the Judicial Service Commission. The magistrates must be academically and professionally certified lawyers with at least five years on the bench.

The magistrates at the District Magistrate's Courts are not expected to be qualified lawyers.

Rather, they are civil servants who have been trained to hold adjudicatory positions at the District court levels. However, they are appointed by the Judicial Service Commission and are gradually being replaced with certified lawyers.

4.2. Legal Contract

Contract is an agreement set out between two or more parties. They set out aim of the parties; they create a legal binding obligation, ways of terminating the contract and consequences of terminating the contract.

Anson defines contract as, an agreement enforceable at law, made between two or more persons, by which rights are acquired by one or more, to acts or forbearance on the part of the other.

The law of contract as administered in Kenya, is an adaptation of the rule of English law of contract as modified by section two and three of the law of Kenya Act (cap 23) 1962.section 3(3) of the Act, expressly exclude s the application of the English statute of frauds Act, while section 4 abolishes the application of the Indian law of contract in Kenya . Contract law help in handling disputes.

Valid contract is an agreement that is binding and enforceable it has all the essential elements.

Voidable contract, is an agreement that is binding and enforceable, but because of lack of one or more of the essential of valid contract, it may be set aside at the option if the aggrieved party.

Void contract is not a contract at all. it means an agreement which is completely destitute of any legal effect. e.g where one of the basic ingredients to create legal relations is missing.

Contracts should be setout in a clear and logical manner and should be complete and consistence. There should not be ambiguity and the parties to the agreement should not be left in no doubting into their rights and duties.

Essentials of valid contract:

According to Ashiq Hussein [2003], there are six features that any valid contract should have:

1. There must be offer and acceptance

The most important feature of a contract is that one party makes an offer for an arrangement that another accepts. This can be called a 'concurrence of wills' or 'ad idem' (meeting of the minds) of two or more parties. There must be evidence that the parties had each from an objective perspective engaged in conduct manifesting their assent, and a contract will be formed when the parties have met such a requirement. Offer and acceptance can be oral or written (Lord Steyn, 1997).

2. There must be an intention to create legal relations.

There is a presumption for commercial agreements that parties intend to be legally bound .On the other hand, many kinds of domestic and social agreements are unenforceable on the basis of public policy, for instance between children and parents. Example is found in the case of *Balfour v. Balfour*. (*Balfour v. Balfour*, 1919)Using contract-like terms, Mr. Balfour had agreed to give his wife £30 a month as maintenance while he was living in Sri Lanka. Once he left, they separated and Mr. Balfour stopped payments. Mrs. Balfour brought an action to enforce the payments. At the Court of Appeal, the Court held that there was no enforceable agreement as there was not enough evidence to suggest that they were intending to be legally bound by the promise

3. There must be consideration or the contract must be under deed

Consideration is known as 'the price of a promise' and is a controversial requirement for contracts under common law. Consideration can be defined as some right, interest, profit or benefit accruing to one party, or some forbearance, detriment, loss or responsibility given, suffered or undertaken by the other.

The idea is that both parties to a contract must bring something to the bargain, where both parties must confer some benefit or detriment e.g. money. This can be either conferring an advantage on the other party, or incurring some kind of detriment or inconvenience towards oneself. Three rules govern consideration.

- Consideration must be real, but need not be adequate. For instance, agreeing to buy a car for a penny may constitute a binding contract. While consideration need not be adequate, contracts in which the consideration of one party greatly exceeds that of another may nevertheless be held invalid for lack of real consideration.
- Consideration must not be from the past. For instance, in (*Eastwood v. Kenyon*, 1840) the guardian of a young girl obtained a loan to educate the girl and to improve her marriage prospects. After her marriage, her husband promised to pay off the loan. It was held that the guardian could not enforce the promise because taking out the loan to raise and educate the girl was past consideration--it was completed before the husband promised to repay it.

- Consideration must move from the promisee. For instance, it is good consideration for person A to pay person C in return for services rendered by person B. If there are joint promisees, then consideration need only to move from one of the promisees.

4. There must be contractual capacity

The law presumes every person is competent to enter into contracts, but certain categories of persons due to age, status or mental instability, have disabilities in this connection. Lack of contractual capacity of one or both the parties may render the contract void, voidable or unenforceable. The special rules affecting each class of person's included: infants or minors, insane or drunken persons, corporations and married women.

5. There must be genuine consent i.e. the consent must not be obtained through mistake, misrepresentation or undue influence

6. The object of the contract must be lawful.

Terms of a contract

In an ordinary contractual transaction, the terms are of two kinds

1. *Conditions*: These are terms of major importance and it's said that they go to the root of the contract. Their breach entitles the innocent party to avoid the contract and claim damages. Under the sale of Goods Act, the innocent party is permitted if he wishes so, to continue with the contract and claim damages for breach of the conditions.
2. *Warranty:* Is a term of lesser importance and as such does not go to the root of the contract. its breach entitles the innocent party to claim damage, but gives no right to the termination of the contract .

Only breach of condition terminates the contract but not of warranty. The court is the one that determines whether a term is a condition or warranty, taking into consideration the circumstance in which such a term was agreed.

A contract is a legally enforceable agreement between two or more parties. It may be oral or written. A contract is essentially a set of promises. Typically, each party promises to do something for the other in exchange for a benefit.

Required Characteristics

To constitute a legal contract, an agreement must have all of the following 5 characteristics:

>> Legal purpose. A contract must have a legal purpose to be enforceable.

>> Mutual Agreement. All parties to the contract must have reached a "meeting of the minds." That is, one party must have extended an offer to which the other parties have agreed.

>> Consideration. Each party to the contract must agree to give up something of value in exchange for a benefit.

>> Competent Parties. The parties to a contract must be competent. That is, they must be of sound mind, of legal age, and unencumbered by drugs or alcohol. If you enter into a contract with a minor or an insane person, the contract will not be enforced.

>> Genuine Assent. All parties must engage in the agreement freely. A contract may not be enforced if mistakes have been made by one or more parties. Likewise, a contract may be voided if one party has committed fraud or exerted undue influence over another. If an agreement was made under duress, the contract is not valid.

So long as the contract meets the requirements above, it is enforceable in a court of law which means that a court can compel noncompliant party to abide by the terms of the contract.

Generally, a contract does not need to be in writing and in many cases an oral agreement with all of the elements listed above will constitute a valid and enforceable contract.

Some situations however require that a contract be in writing to be enforceable.

Oral v. Written Contract

Contracts made only by spoken agreement may be legally enforceable. However, it is best to memorialize them in writing, especially if a legal remedy becomes necessary, so that there will be proof in court. Also, there are certain types of contracts that must be in writing in order to be enforceable:

- Contracts involving the sale or transfer of land
- Promises to pay someone's debt obligations
- Contracts that cannot be completed within one year of its making

- Contracts involving the sale of goods for more than $500
- Contracts that will go beyond the lifetime of the one performing the contract

Bilateral or Unilateral Contracts

Most contracts are bilateral. This means that each party has made a promise to the other.

A bilateral contract is an agreement in which each of the parties to the contract makes a promise or set of promises to each other.

For example, in a contract for the sale of a home, the buyer promises to pay the seller $200,000 in exchange for the seller's promise to deliver title to the property. These common contracts take place in the daily flow of commerce transactions, and in cases with sophisticated or expensive precedent requirements, which are requirements that must be met for the contract to be fulfilled.

In a unilateral contract, one party makes a promise in exchange for an act by the other party. Insurance policies are unilateral contracts. When you buy liability insurance or any other type of policy, you pay a premium (an act) in exchange for the insurer's promise to pay future claims.

In unilateral contracts one party makes a promise, but the other side does not promise anything. In these cases, those accepting the offer are not required to communicate their acceptance to the offeror.

In certain circumstances, an implied contract may be created. A contract is implied in fact if the circumstances imply that parties have reached an agreement even though they have not done so expressly.

Invitation to treat

Where something is advertised in a newspaper or on a poster, this will not normally constitute an offer but will instead be an invitation to treat, an indication that one or both parties are prepared to negotiate a deal.

Electronic contracts

Entry into contracts online has become common. Many jurisdictions have passed e-signature laws that have made the electronic contract and signature as legally valid as a paper contract.

The Contract as a Document

The term "contract" often refers to a written agreement, typically including some or all of the following elements:

- introductory material (sometimes known as "recitals" or "whereas provisions")
- definitions of key terms
- a statement of the purpose or purposes of the agreement
- the obligations of each party (and conditions that may trigger obligations)
- assurances as to various aspects of agreement (sometimes phrased as warranties, representations, or covenants)
- boilerplate provisions
- a signature block
- Exhibits or attachments.

The Contract as a Process

"Contract" is a noun, but it can be used as a verb, too. When you contract with somebody, you participate in a process that typically involves three phases.

Phase 1: Contemplating the deal. The parties each assess the prospective arrangement and its risks ("Can I trust her?") and attempt to predict the future ("Will I regret paying this price for the computer next month? Will it be outdated?").

Phase 2: Reaching an agreement. During this phase the parties negotiate and agree on the terms, usually formalized in a written contract or some other documented evidence of the arrangement (such as a receipt or purchase order, for example).

Phase 3: Performance and enforcement. Once the contract is in place, the parties are legally required to perform their mutual obligations. If one party fails to perform, the other can sue to enforce the deal.

Types of contracts

1. Contract of deed

This includes court judgment and personal recognisances. They are not true contracts since the obligations under them are imposed on the parties by the courts, and do not result through mutual agreement.

2. Contract under deed or specialty contracts

Also known as under seal contract and is the only formal contract. It must be (I)in writing (ii)signed, sealed and delivered. Sealing and delivering are usually mere formalities. Delivery can be actual (i.e. hading over the sealed document)or constructive(i.e. party delivering the deed touches the seal with his fingers saying “I deliver to you as my act and deed”).

3. Simple contracts (parol)

This is a contract, which does not satisfy the requirement of the contract under deed. It may be oral, written or partly oral and partly written, or merely implied by conduct

The following contracts must be in writing, otherwise they are void

1. All contracts which require to be stamped e.g. bills of exchange, promissory notes and transfer of shares in limited companies
2. Acknowledgement of statute barred debts. In case of a simple contract, if an action is not maintained to recover the debt within six years, the claim becomes time-barred. but if the debtor acknowledges this statute barred debt in writing the right of action in favor of the creditor is revived for another six years.
3. Transfer of immovable property, the law requires the transfer of immovable property by registered instrument.
4. Representation of character or credit worthiness. Section 3(2) of the law of contract Act provides that any representation made relating to character, credit, and ability of any other person must be in writing and signed by the party to be responsible in case the default is made by a person for whom the representation was made.

The following contracts must be supported by written evidence otherwise they are unenforceable

1. *Contracts for sale of goods of two hundred shillings or more:* by section 6 of the Kenya sale of Goods Act the contracts for the sale of goods for the value of two hundred shillings or over are required to evidence in writing, otherwise he contract is unenforceable.
2. *Every Hire purchase Agreement* must be evidenced in writing and registered within 30 days of its execution
3. *Contracts of Guarantee:*” A special promise to answer for a debt, default of miscarriage of another person” is required to be evidenced in writing by section 3(1) of the law court Act. In the absence of any memorandum or note thereof in writing and signed by the person to be charged, no action can be maintained.
4. *Contracts for the sale of land:* By section 3(3) as amended by the law of Contract Act 1968,all agreements for the sale of land or other disposition of land must be supported by written evidence, signed by the party to be charged or by his agent.
5. *Contracts of employment* for over one month. Section 5 of Kenya Employment act (Cap 226) provides that a contract of service which is not in writing or supported by sufficient memorandum is not enforceable for a longer period than one month from the date of entering it
6. *Money lending contracts*: Section 11(1) of the Kenya moneylenders Act provides that no action may be brought for payment of the loan unless a note or memorandum in written signed by the borrower can be produced in court

4.3. Agreement vs. Contract

An agreement is any understanding or arrangement reached between two or more parties.

A contract is a specific type of agreement that, by its terms and elements, is legally binding and enforceable in a court of law.

Comparison Chart

	Agreement	Contract
Definition	An arrangement (usually informal) between two or more parties that is not enforceable by law.	A formal arrangement between two or more party that, by its terms and elements, is enforceable by law.
Validity based on	Mutual acceptance by both (or all) parties involved.	Mutual acceptance by both (or all) parties involved.
Does it need to be in writing?	No.	No, except for some specific kinds of contracts, such as those involving land or which cannot be completed within one year.
Consideration required	No	Yes
Legal effect	An agreement that lacks any of the required elements of a contract has no legal effect.	A contract is legally binding and its terms may be enforceable in a court of law.

Benefits

The primary benefit of an agreement that does not meet the criteria of a contract is that it is inherently informal. Where the agreeing parties have a longstanding relationship and share a considerable degree of trust, the use of a non-contract agreement can save time and allow for more flexibility in the fulfillment of the agreed-upon obligations. Agreements lacking all the required elements of a contract may also be more viable in situations where the drafting of a contract would prove prohibitively burdensome on the parties involved.

The main advantage of contracts is that they spell out the specific terms that the contracting parties have agreed upon, and in the event of a breach – where one or more parties fail to fulfill their obligations – serve as a guide for a court of law to determine the proper remedy for the injured party or parties. Even where parties have a good relationship and trust one another, the use of a contract provides an extra layer of assurance that the obligations entered into under the contract will be fulfilled as the parties themselves intended. Contracts are generally advisable over less stringent agreements in any official business or commercial matter due to the added protection they provide.

4.4. Breach of Contract

Breach of contract

A contract may be discharged (terminated) by breach; that is, the failure of one of the parties to perform his obligation under the contract.

Breach of contract may occur in any one of the three ways:

1. *Failure to Perform:* where a person fails to perform a contract, when then performance is due, the other party can hold him liable for the breach, provided the time of performance was made as the essence of the contract.
2. *Renunciation:* It may sometimes happen that even before the time of performance arrives, one party to a contract repudiates (rejects) his liabilities. This is known as an anticipatory breach. Here it requires that the aggrieved party sues immediately before the actual time stipulated for performance of the contract if remedy is to be given.
3. *Self-disablement:* this occurs when the defendant disables himself from performing his contractual obligation, or does some act which makes the performance of contract impossible.

Remedies for breach of contract

Refusal of further performance

A party who suffers by a breach of contract is entitled to treat the contract as ended and may refuse any further performance on his own part.

Damages

This is the normal remedy for breach of contract. The aim of law is to place the injured party as far as possible in the position he would have been if the contract had been performed.

It is not for every kind of damage that the plaintiff is entitled to recover compensation. In some cases, the law considers that the loss sustained from breach of contract is too remote to merit any compensation.

The condition is that the accused has to have been aware of the loss incurred, in order to claim damages.

Specific Performance

This is an order requiring a person to carry out a contractual obligation. It is usually granted where a contract is for:

a) The sale of land

b) Taking debentures in a company.

c) Sale of rare goods which are not easily available in the market or the value of such could not be measured in money.

It is not granted where:

a) Damages would provide an adequate remedy

b) Contract is to render personal services.

c) One party to the contract is an infant

d) The contract is to lend money

Injunction

This is an order of the court restraining the doing, continuance or repetition of a wrongful act. The court will not however, enforce contract by injunction if damages are a more suitable remedy since it can always award damages in lieu of an injunction.

If one party fails to fulfill his or her duties under the agreement, that party has breached the contract.

Breach of contract is a legal cause of action and a type of civil wrong, in which a binding agreement or bargained-for exchange is not honored by one or more of the parties to the contract by non-performance or interference with the other party's performance.

Breach occurs when a party to a contract fails to fulfill its obligation as described in the contract, or communicates an intent to fail the obligation or otherwise appears not to be able to perform its obligation under the contract.

If one party breaches a contract, the other party may suffer a financial loss. The resulting damages will have to be paid by the party breaching the contract to the aggrieved party.

What Should You Do in the Event of a Breach

If there has been a breach of contract, your first step is to look at the contract to see if there are instructions as to what you should do in the event of a breach.

Many contracts will talk about mandatory arbitration or about a liquidated damages clause that goes into effect. It's important to thoroughly read the contract before you make any quick decisions.

Your second step should be to let the other party know that a breach has occurred. If you are committed the breach but do not want to tell them, then you can face more serious consequences if you attempt to hide the breach.

If the other party breached, then it's important to tell them that you are aware of a breach and ask them if they can verify it. While a breach of contract can be stressful, giving the other party an opportunity to remedy the breach can strengthen your case if you go to court.

The third step is to discuss the situation either with the other party or a lawyer. If you feel that the breach will require you to go to court, then contact your lawyer right away and let them know of the situation.

Be sure to hold onto any documents related to the contract and keep careful record of every incident that occurred from the contract. This will make it easier for you to argue the merits of your argument and be compensated for the breach.

Four Types of Contract Breaches

There are four types of contract breaches: anticipatory, actual, minor and material.

Anticipatory breach vs. actual breach

- An actual breach occurs when one person refuses to fulfill his or her side of the bargain on the due date or performs incompletely.
- Anticipatory breach occurs when one party announces, in advance of the due date for performance, that he intends not to fulfill his side of the bargain.

Both actual and anticipatory contract breaches are bad news for the individuals and organizations at hand. They can waste both money and time, and certainly lead to frustration for everyone involved. A breach of contract, no matter what form it may take, entitles the innocent party to maintain an action for damages.

Minor breach vs. material breach

A breach is likely material if one party ends up with something significantly different than what was specified in the contract.

For example, if you contact with a web designer to build a new site for home cafe, but end up with a blog about bagels that doesn't even mention your place, the breach is probably material. In most cases, a material breach means the non-breaching party is no longer required to perform his or her end of the deal and has a right to remedies.

A minor breach, sometimes called a partial breach. In many cases, a minor breach means that one party failed to perform some part of the contract even through the specified item or service was ultimately delivered.

Consider the cafe website contract. If the finished product met all the client's demands but was completed a day after it was requested, the breach might be considered minor. Unless the initial contract terms specifically mentioned that 'time is of the essence' or that the website was under a tight deadline, a reasonable delay from the web designer would only be considered a minor breach.

Fundamental Breach: This occurs when one party violates the contract terms so egregiously that the other party may terminate the contract (as well as seek damages).

Requirements of a breach of contract

1. The contract must be valid. It must contain all essential contract elements by law. A contract isn't valid unless all these essential elements are present, so without them, there can be no lawsuit.
2. The plaintiff or the party who's suing for breach of contract must show that the defendant did indeed breach the agreement's terms.

The plaintiff must have done everything required of him in the contract.

The plaintiff must have notified the defendant of the breach before proceeding with filing a lawsuit. A notification made in writing is better than a verbal notification because it offers more substantial proof.

Types of remedies for broken contracts

You have several options for obtaining compensation.

A. Sue for Damages. You may sue the contractor for damages.

There are many kinds of damages, including the following:

1) Compensatory damages aim to put the non-breaching party in the position that they had been if the breach had not occurred.

2) Punitive damages are payments that the breaching party must make, above and beyond the point that would fully compensate the non-breaching party. Punitive damages are meant to punish a wrongful party for particularly wrongful acts, and are rarely awarded in the business contracts setting.

3) Nominal damages are token damages awarded when a breach occurred, but no actual money loss to the non-breaching party was proven.

4) Liquidated damages are specific damages that were previously identified by the parties in the contract itself, in the event that the contract is breached. Liquidated damages should be a reasonable estimate of actual damages that might result from a breach.

B. Specific Performance. You can compel the contractor to complete the work required by the contract.

If damages are inadequate as a legal remedy, the non-breaching party may seek an alternative remedy called specific performance.

Specific performance is best described as the breaching party's court-ordered performance of duty under the contract.

Specific performance may be used as a remedy for breach of contract if the subject matter of the agreement is rare or unique, and damages would not suffice to place the non-breaching party in as good a position as they would have been had the breach not occurred.

C. Other Remedies. If the contractor tricked or forced you into signing the contract, you might convince a court to terminate the agreement or amend its terms.

Cancellation and Restitution

A non-breaching party may cancel the contract and sue for restitution if the non-breaching party has given a benefit to the breaching party.

"Restitution" as a contract remedy means that the non-breaching party is put back in the position it was in prior to the breach, while "cancellation" of the contract voids the contract and relieves all parties of any obligation under the agreement.

Defenses to a Breach of Contract Lawsuit

As in all lawsuits, the defendant—the party being sued—has a legal right to offer a reason why the alleged breach is not really a breach of contract or why the breach should be excused. In legal terms, this is called a defense. Common defenses against a breach of contract include:

- Fraud

This means ”knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment." When a defendant presents this defense, he's saying that the contract isn't valid because the plaintiff failed to disclose something important or because he made a false statement about a material or important fact. The defendant must establish that the fraud was deliberate.

- Duress

This occurs when one person compels another to sign a contract through physical force or other threats. This, too, can invalidate a contract because both parties did not sign of their own free will, which is a standard contractual prerequisite.

- Undue influence

This is similar to duress. It means that one party had a power advantage over the other and that he used that advantage to force the other to sign the contract.

- Mistake

An error committed by the defendant can't invalidate a contract and take away a breach of contract case, but if the defendant can prove that both parties made a mistake about the subject matter, it might be enough to invalidate the contract and this would serve as a defense.

- Statute of Limitations

Many types of cases have time limits imposed by law, deadlines by which a case must be brought and filed. A breach of contract case can be thrown out of court if the defendant can show that the statute of limitations has expired. Statutes of limitations cases are based on time frames that are set by individual state law so they can vary. They average from three to six years for a written contract.

If You Think Your Contract Has Been Breached

See an attorney if you think that the party you've entered into a contract with has breached it in some way. Law is intricate and small details of your case—things that you don't think are related or are a particularly big deal—can make a significant difference. Only a lawyer will be able to tell you if you have a strong case before you spend time and money launching into a lawsuit on your own—one that you could lose because of misunderstanding or an error.

And, of course, if you're accused of breaching a contract, you'll want legal help to sort out the details of your case and to help you establish a defense.

4.5. Liability

Liability is any legal responsibility, duty or obligation. The state of one who is bound in law and justice to do something which may be enforced by action. This liability may arise from contracts either express or implied or in consequence of torts committed.

in legal terms, the word liability refers to fault. The person who is at fault is liable to another because of his or her actions or failure to act.

Categories of liability

Traditionally there are three categories of liability that the courts use to deal with claims that products or services have caused physical or economical injury to consumers e.g.

In so far as computers software is part of a machine and the machine injures someone physically or economically the producer of software and operator can be held liable.

1. Warranty

A warranty can be expressly stated by seller of good implied by simply being sold in market place where it's assumed by court that the merchant is making an impression that products are of good quality and are in good condition.

If software is part of machine it will be treated as a machine and warrant promises are enforceable. If software is a service warrant, the law does not apply unless the software author makes some specific warranties in performance of the software. If software is a book then warranty does not apply.

2. Negligence

This occurs when the product cause physical or economic harm to individuals, when the injury could have been prevented and when the producer has a duty to care about the consumer of the product. Negligence require fault.

Producers of software have been found liable in cases where software is part if machine but not as services

3. Strict liability in tort

This is a separate class of liability that arises when a defective product causes injury. In this case individuals can bring fret against the manufacturers, independent of question of fault, warranty or care. Meaning a manufacturer of a product that injures people, can be held strictly liable regardless of whether or not he could have prevented the defect.

The software act as part of product rather than a service the strict liability applies.

What is Contractual Liability?

The term contractual liability means liability that one party assumes on behalf of another by way of a contract. Contractual liability is automatically covered by the standard ISO general liability policy.

Indemnity Agreements

Many businesses engage in contracts like building leases, equipment leases, maintenance agreements, and construction agreements. These contracts are likely to contain an indemnity agreement.

An indemnity agreement is a promise by one party to assume liability for third-party claims filed against someone else. In a typical indemnity agreement, Party X agrees that if Party Y is sued by Party Z because of Party X's negligence, Party X will indemnify (reimburse) Party Y for costs that result from Party Z's lawsuit. The party providing indemnification is called the indemnitor while the party being indemnified is the indemnitee.

In a building or equipment lease, the property owner is usually the indemnitee while the lessee is the indemnitor. In a construction or service contract, the person doing the work or providing the service is the indemnitor while the property owner or general contractor is the indemnitee. An indemnity agreement is also called a hold harmless agreement. The following example demonstrates how such an agreement works.

Example

Busy Builders is a general contractor that has been hired by a property owner to construct a new office building. Busy hires Lucky Landscaping to design and build the outdoor space. Lucky will be responsible for planning and installing walkways, gardens, fountains, seating areas, and other features.

Busy knows that Lucky could make a mistake while performing its landscaping work. The error could trigger an accident that injures someone or damages someone's property. The injured party might seek compensation from Busy Builders as well as Lucky Landscaping. To protect itself against potential claims, Busy requires Lucky Landscaping to sign a contract containing an indemnity agreement.

The agreement states that if someone sustains bodily injury or property damage because of Lucky's negligent landscaping work and the injured party sues Busy Builders, Lucky will pay for the loss. Lucky will pay any damages assessed against Busy and defend Busy (or pay its defense costs).

Risk Transfer

Busy Builders has used an indemnity agreement to transfer the risk of landscaping-related lawsuits to Lucky Landscaping. Lucky will be doing the landscaping work so it is in a better position than Busy Builders to prevent landscaping-related losses. For this reason, Lucky assumes the risks associated with those losses.

An indemnity agreement transfers from Party A to Party B the financial consequences of a loss. It does not eliminate Party A's liability for the injured person. In the previous example, Lucky Landscaping has agreed to pay damages and defense costs that result from lawsuits against Busy that arise out of Lucky's work. The agreement will not prevent lawsuits by third parties against Busy Builders, nor will it affect Busy's liability to an injured third party. It merely transfers liability for the financial consequences of the lawsuit (damages and defense costs) from Busy Builders to Lucky Landscaping.

Contractual Liability Coverage

Most general liability policies contain a contractual liability exclusion like the one found in the standard ISO policy. The exclusion is located under Coverage A, Bodily Injury and Property Damage Liability. It eliminates coverage for the following:

Bodily injury or property damage for which the insured is obligated to pay damages by reason of the assumption of liability in a contract or agreement.

The exclusion contains two important exceptions. It does not apply to:

1) Liability the insured would have in the absence of the contract; or

2) Liability assumed under a contract that qualifies as an insured contract

Liability That Exists in the Absence of the Contract

First, the exclusion doesn't apply to bodily injury or property damage for which you would liable if the contract did not exist. For example, suppose that you rent a forklift from an equipment rental company. You are using the forklift to move some crates outside your warehouse when you accidentally drop a crate on a truck that belongs to a customer.

When you signed the rental agreement, you probably assumed liability for damage you might cause to other people's property while using the forklift. If the rental agreement did not exist, you will still be legally liable under common law for the damage you have caused to the customer's truck.

Liability Assumed Under an Insured Contract

The second exception applies to liability assumed by an insured under an insured contract if the injury or damage occurs after the contract has been executed. Insured contract is a defined term that includes virtually any contract in which you assume the tort liability of someone else. If you engage in a contract that meets this definition, your assumption of liability should be covered.

In the Busy Builders scenario outlined previously, suppose that the building owner's cousin (Jim), is visiting the construction site when he is injured by a backhoe operated by a Lucky Landscaping employee. Jim sues Lucky Landscaping and Busy Builders for bodily injury. Lucky is liable for the claim against Busy under the construction contract. If Lucky is insured under a general liability policy, its insurance should cover Jim's claims.

No Contractual Coverage for Personal and Advertising Injury

Note that contractual liability applies only to bodily injury or property damage. If you assume liability under a contract on behalf of someone else for claims that allege personal and advertising injury, the claims will not be covered under your liability policy. Contractual liability is specifically excluded under personal and advertising injury liability coverage (Coverage B).

5. Property law and Rights

Objectives

Explain the terms

- Property law
- Intellectual Property
- Copyright
- Patents

Explain Accountability and Information Technology

5.1. Property law

The term property is normally used in two different senses, and it is important to distinguish between them:

1. When the sale of goods act talks of property in goods, it means the ownership of them. In contract for the sale of specific goods, the seller transfers the property (ownership) in goods to the buyer when the contract is made, and it is immaterial whether the line of delivery or of payment or both is postponed.
2. Usually the word property means the things, which are capable of being owned although they need not exist in tangible form. Hence in this sense the term property includes:

a) *Things in possession* – such as pens, books, desks, chairs, etc.

b) *Things in action* – these have no physical existence and include things such as debts, patents, copyrights, etc. they are called *choses in action*, which can be enforced only by action and not by taking possession.

Ownership and possession

All legal systems distinguish between ownership and possession. It is, therefore, necessary to deal with them briefly. Ownership's a matter of law and it denotes the relation between a person and any right that is vested in him over property.

A person is an owner of property if he has the ultimate legal right over its use and disposal.

Ownership may be acquired in three ways:

a) Originality: where a person creates something new, or acquires something, which no one claims or has been abandoned by its previous owner.

b) Derivatively: when a person sells his goods to the buyer or he makes a gift to another person, the right of ownership is transferred to the latter.

c) By succession: where a previous owner dies, the property may pass to his heir or to someone else under a will.

While ownership is a matter of law, possession is a matter of fact. Possession is physical detention coupled with the intention to hold the things in detention as one's own.

Possession can be converted into ownership under the following two circumstances:

a) If wrongful possession of land continues for twelve years, and of goods for six years.

b) The holder of a negotiable instrument, a factor, and a seller in market overt can give a better title than they themselves have, provided the buyer takes what they offer for value and in good faith.

European law; the influence of European law on English law

The European Union consists mainly of countries which use civil law and so the civil law system is also in England in this form, and the European Court of Justice, a predominantly civil law court, can direct English and Welsh courts on the meaning of EU law.

The Law of the European Union is the unique legal system which operates alongside the laws of Member States of the European Union (EU). EU law has direct effect within the legal systems of its Member States, and overrides national law in many areas, especially in terms of economic and social policy. The EU is not a federal government, nor is it an intergovernmental organization. It constitutes a new legal order in international law for the mutual social and economic benefit of the Member States. It is sometimes classified as supranational law.

English law, the legal system of England and Wales, is the basis of common law legal systems throughout the world (as opposed to civil law or pluralist systems in other countries, such as Scots law). It was exported to Commonwealth countries while the British Empire was established and maintained, and it forms the basis of the jurisprudence of most of those countries. English law prior to the American revolution is still part of the law of the United States, except in Louisiana, and provides the basis for many American legal traditions and policies, though it has no superseding jurisdiction.

The essence of English common law is that it is made by judges sitting in courts, applying their common sense and knowledge of legal precedent (stare decisis) to the facts before them. A decision of the highest appeal court in England and Wales, the House of Lords, is binding on every other court in the hierarchy, and they will follow its directions. For example, there is no statute making murder illegal. It is a common law crime - so although there is no written Act of Parliament making murder illegal, it is illegal by virtue of the constitutional authority of the courts and their previous decisions. Common law can be amended or repealed by Parliament; murder, by way of example, carries a mandatory life sentence today, but had previously allowed the death penalty.

England and Wales are constituent countries of the United Kingdom, which is a member of the European Union and EU law is effective in the UK. The European Union consists mainly of countries which use civil law and so the civil law system is also in England in this form, and the European Court of Justice, a predominantly civil law court, can direct English and Welsh courts on the meaning of EU law.

EU law covers a broad range which is comparable to that of the legal systems of the Member States themselves. Both the provisions of the Treaties, and EU regulations are said to have "direct effect" horizontally. This means private citizens can rely on the rights granted to them (and the duties created for them) against one another. For instance, an air hostess could sue her airline employer for sexual discrimination. The other main legal instrument of the EU, "directives", have direct effect, but only "vertically". Private citizens may not sue one another on the basis of an EU directive, since these are addressed to the Member States. Directives allow some choice for Member States in the way they translate (or 'transpose') a directive into national law - usually this is done by passing one or more legislative acts, such as an Act of Parliament or statutory instrument in the UK. Once this has happened citizens may rely on the law that has been implemented. They may only sue the government "vertically" for failing to implement a directive correctly. An example of a directive is the Product liability Directive, which makes companies liable for dangerous and defective products that harm consumers.

England and Wales are constituent countries of the United Kingdom, which is a member of the European Union and EU law is effective in the UK. The European Union consists mainly of countries which use civil law and so the civil law system is also in England in this form, and the European Court of Justice, a predominantly civil law court, can direct English and Welsh courts on the meaning of EU law.

Overseas influences

The influences are two-way.

The United Kingdom exported its legal system to the Commonwealth countries during the British Empire, and many aspects of that system have persisted after the British withdrew or granted independence to former dominions. English law prior to the Wars of Independence is still an influence on United States law, and provides the basis for many American legal traditions and policies. Many states that were formerly subject to English law (such as Australia) continue to recognise a link to English law - subject, of course, to statutory modification and judicial revision to match the law to local conditions - and decisions from the English law reports continue to be cited from time to time as persuasive authority in present day judicial opinions. For a few states, the Judicial Committee of the Privy Council remains the ultimate court of appeal. Many jurisdictions which were formerly subject to English law (such as Hong Kong) continue to recognise the common law of England as their own - subject, of course, to statutory modification and judicial revision - and decisions from the English Reports continue to be cited from time to time as persuasive authority in present day judicial opinions.

The UK is a dualist in its relationship with international law, i.e. international obligations have to be formally incorporated into English law before the courts are obliged to apply supranational laws. For example, the European Convention on Human Rights and Fundamental Freedoms was signed in 1950 and the UK allowed individuals to directly petition the European Commission on Human Rights from 1966. Now s6(1) Human Rights Act 1998 (HRA) makes it unlawful "... for a public authority to act in a way which is incompatible with a convention right", where a "public authority" is any person or body which exercises a public function, expressly including the courts but expressly excluding Parliament. Although the European Convention has begun to be applied to the acts of non-state agents, the HRA does not make the Convention specifically applicable between private parties. Courts have taken the Convention into account in interpreting the common law. They also must take the Convention into account in interpreting Acts of Parliament, but must ultimately follow the terms of the Act even if inconsistent with the Convention (s3 HRA).

Similarly, because the UK remains a strong international trading nation, international consistency of decision making is of vital importance, so the Admiralty is strongly influenced by Public International Law and the modern commercial treaties and conventions regulating shipping.

5.2. Intellectual Property (IP)

Introduction

The emergence of the Internet has caused policymakers, legislators, rights holders, content creators, businesses, content users and others to rethink the way intellectual property should operate in a modern inter-connected society. The range of new technologies and the speed of innovation raises intellectual property issues: domain names are often inextricably linked with trademark issues; and the ease with which digital technologies allow for copying and distribution challenges copyright law enforcement.

Intellectual property is currently at the center of an international debate in many different forums regarding how to reconcile the potential of the Internet with traditional intellectual property approaches, including how to stop unlawful transactions on the Internet. Two principal approaches have emerged: involving Internet intermediaries in enforcement and using Internet technical measures to prevent access to un-authorised content.

The need for Protecting Private property

Incentive to create:

The economic philosophy behind the legislations empowering States to grant IP rights is the conviction that encouragement of individual efforts by direct personal gains is the best way to advance public welfare through the talents of authors and inventors in Science and useful Art”1 . 1US Supreme Court in Mazer v Stein (1954)

Works against the ‘lazy’ in you! It prevents free riding on works or reputation of others and Frees your creative mind Prevents possible holdout of life enriching ideas from learned and ingenious minds.

in summary

Why Protect your Intellectual Property?

- Incentive to create
- Prevent unjust enrichment
- Prevent “hold out” of life enriching ideas

5.3. Legal basis of Protecting IP

Domestic Obligations: The Constitution of Kenya:

- The fundamental rights in the Constitution provide every person with the right to property; which must be understood to also include intellectual property.
- It provides:- Sec.75. (1) No property of any description shall be compulsorily taken possession of, and no interest in or right over property of any description shall be compulsorily acquired, except where the following conditions are satisfied

Different aspects of IP

Type of IP	**IP Rights**
Inventions	Patents
works of Art and Authorship	Copyright
Source identification/Brand names	Trademarks
Aesthetics/Ornamental features	Designs
Proprietary information	Trade secrets

5.4. Accountability and Information Technology

The bottom line is that technology accountability requires more than just standing up and taking ownership. It's **a process of proactive investigation, preparation, and study into what's best for an organization**. One thing's for sure - technology will continue to evolve and new trends will continue to emerge.

Accountability is **an assurance that an individual or an organization will be evaluated on their performance or behavior related to something for which they are responsible**. The term is related to responsibility but seen more from the perspective of oversight.

While **responsibility refers to someone's duty to carry out a task to completion, accountability generally refers to what happens after something has happened**. Accountability is therefore concerned with the consequences of someone's actions, rather than their initial duty to carry these actions out.

Accountability in the workplace is important because **individuals who feel responsible for their actions may be more likely to perform their tasks well and efficiently**. A workplace that values accountability may also foster greater commitment and increased employee happiness.

Corporate accountability involves being answerable to all an organization's stakeholders for all actions and results. Through performance and accountability reporting (PAR), for example, an organization compiles and documents factors that quantify its profitability, efficiency and adherence to budget, comparing actual results against original targets. The PAR process is usually carried out once per fiscal year, although in some cases it is done more often.

Corporate accountability also implies that an organization must be answerable for any deviations from its stated goals and values, which might be documented and made publicly available through a mission statement or vision statement. Beyond that, the concept of corporate accountability is often broadened to imply a requirement for business to follow ethical, responsible and sustainable practices.

Characteristics of Accountability

Some lazy types among us can confuse accountability with being held to account, and will avoid it like the plague. They fail to realise the following qualities are the hallmarks of excellent, must-have employees.

1. Answer emails and requests

In an era of increasing rudeness and indifference, it is a rare pleasure to receive clearly written and polite emails, and answers to requests. 'Dan from Optus' demonstrated this wittily and politely in his social media strategy not long ago when dealing with customer complaints – and got results well beyond those achieved by other telcos (and possibly a lot of job offers too!).

2. Do what you promise

Those who do otherwise generate angry customers, clients and stakeholders. It can be difficult to hit the bullseye of people's expectations every time, but attempting to BS one's way out of it leads to major fails all around. If you can't deliver, then definitely do not promise in the first place.

3. Take responsibility for actions

This is a sign of a mature, fair-minded individual. But don't automatically shoulder the blame when it isn't due. Show preparedness to discuss what went wrong and to flag possible remedies.

4. Proactively solve problems

This signals one's realisation that something is causing grief; there's a spanner in the works compounding what's already going on. Roll up your sleeves and work to get answers or directions towards a solution.

5. Don't blame or make excuses

Occasionally when one's unfairly in the firing line, making excuses or blaming can be tempting. Try not to do this. Deal with the matter at hand and when the pressure has eased off, canvass with others what actually happened and how it can be prevented in the future.

6. Always remain ethical in your actions

This is easily said and not always put into practice. Some people just can't resist instant gratification, even when it's undeserved or illegitimate. Do the right thing and it's true – you are eventually rewarded (in a meaningful, 'soul' way).

7. Be honest and transparent in all work

Sometimes this doesn't pay but it's important when you're dealing with others who are somewhat less than transparent. Keep your standards high and clear for all to see.

8. Demonstrate outcomes

Some conflate this with a pretence of competence. You may recognise these types, because they talk much more than they deliver. There's a time for bold or impressive talk, granted, but at the end of the day people want outcomes. Be the doer, not the showpony.

9. Review and evaluate to improve

Perfection is seldom attained in anyone's lifetime but accountability-conscious people are not necessarily perfectionists for the sake of it. They recognise instead that there's always room for improvement and they do it with good grace and perspective.

10. Show humility and the will to apologise

An accountable person has a good sense already of when they've transgressed and they usually swiftly apologise. Those who refuse to acknowledge others in discussions, debates or disputes seldom do this. A genuine apology will clear the air.

How many of these ten qualities do you have? Are you someone that people respect? You will be respected and admired more if you deliver on each of these ten characteristics.

MANAGEMENT OPPORTUNITIES, CHALLENGES, AND SOLUTIONS

The ethical and social implications of information systems are now more far-reaching than ever, affecting individuals who use information systems as well as managers and employees in business firms.

Opportunities

Managers have the opportunity to create an ethical business environment that is within the law, and it is their responsibility to do so. Doing the right thing with information systems in the long term will always lead to a stronger, more reliable organization. This may not mean that management actions will always make employees, shareholders, or customers happy, but these actions should be the result of a careful ethical analysis using the principles we have outlined in this chapter.

Management Challenges

Technology can be a double-edged sword. It has been the source of many benefits, but it also has created new opportunities for breaking the law or taking benefits away from others, raising the following management challenges.

UNDERSTANDING THE MORAL RISKS OF NEW TECHNOLOGY

Rapid technological change means that the choices facing individuals also rapidly change, and the balance of risk and reward and the probabilities of apprehension for wrongful acts change as well. In this environment it is important for management to conduct an ethical and social impact analysis of new technologies as they emerge. Managers might take each of the moral dimensions described in this chapter and briefly speculate on how a new technology impacts each dimension. There may not always be right answers for how to behave, but there should be management awareness of the moral risks of new technology.

ESTABLISHING CORPORATE ETHICS POLICIES THAT INCLUDE INFORMATION SYSTEMS ISSUES

As a manager, you will be responsible for developing, enforcing, and explaining corporate ethics policies. Historically, corporate management has paid much more attention to financial integrity and personnel policies than to the information systems area. But based on what you will have learned after reading this chapter, it will be clear your corporation should have an ethics policy in the information systems (IS) area covering such issues as privacy, property, accountability, system quality, and quality of life. The challenge will be in educating non-IS managers about the need for these policies, as well as educating your workforce.

Solution Guidelines

Some corporations have developed far-reaching corporate IS codes of ethics, including FedEx, IBM, American Express, and Merck & Co. Most firms, however, have not developed these codes of ethics, leaving their employees unsure about expected correct behavior. There is some dispute concerning a general code of ethics versus a specific information systems code of ethics. As managers, you should strive to develop an IS-specific set of ethical standards for each of the five moral dimensions:

- *Information rights and obligations.* A code should cover topics such as employee e-mail and Internet privacy, workplace monitoring, treatment of corporate information, and policies on customer information.
- *Property rights and obligations*. A code should cover topics such as software licenses, ownership of firm data and facilities, ownership of software created by employees on company hardware, and software copyrights. Specific guidelines for contractual relationships with third parties should be covered as well.
- *System quality*. The code should describe the general levels of data quality and system error that can be tolerated, with detailed specifications left to specific projects. The code should require that all systems attempt to estimate data quality and system error probabilities.
- *Quality of life*. The code should state that the purpose of systems is to improve the quality of life for customers and for employees by achieving high levels of product quality, customer service, and employee satisfaction and human dignity through proper ergonomics, job

and workflow design, and human resources development.

- *Accountability and control*. The code should specify a single individual responsible for all information systems, and reporting to this individual should be others who are responsible for individual rights, the protection of property rights, system quality, and quality of life (e.g., job design, ergonomics, and employee satisfaction). Responsibilities for control of systems, audits, and management should be clearly defined. The potential liabilities of systems officers and the corporation should be detailed in a separate document.

6. Computer Crime

the following sub-topics will be covered here

- Computer Misuse and Computer Crime

- Computer Misuse and Criminal Law

- Privacy and Freedom of information

6.1. Computer abuse and Computer crime

Computer abuse and computer crime mean two separate things. In computer abuse an individual is dishonest or unethical and using a computer in an unauthorized manner. In contrast, a criminal commits illegal acts with a computer.

Computer abuse refers to a broad category of activities wherein a computer is used to improperly or illegally cause harm to somebody else or their property. Cyber-bullying, hacking, identity theft, and even using a work PC for personal business are all examples of computer abuse.

cybercrime, also called computer crime, **the use of a computer as an instrument to further illegal ends**, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.

Computer Misuse was added to the list of serious crimes with a maximum penalty for being found guilty increasing to **a prison sentence of 14 years and the possibility of a fine**. If a charge included threats to national security or human welfare, a life sentence can be imposed.

What Is Computer Abuse?

Computer abuse is the legal term for the use of a computer to carry out improper or illegal activities, but which do not constitute financial crimes that would be classified as wire fraud.

Examples of computer abuse include using a computer to expose personally identifiable information (PII) such as Social Security numbers, using a computer to change the content of a website owned by someone else, intentionally infecting one computer with a virus or worm that will spread to other computers, using a computer to illegally share copyrighted items, or using one computer to gain unauthorized access to another. Other examples of computer abuse include cyberbullying and using a work computer for personal tasks on company time.

The Computer Fraud and Abuse Act of 1984

The CFAA criminalizes certain types of computer abuse by banning “unauthorized access” of computers and networks. The law has been used to successfully prosecute both high- and low-level hackers for both civil and criminal matters. Early on, for example, the law was used to convict the man who released the first computer worm in 1988. Over the years, however, the law’s vagueness has resulted in punishments as severe as decades in prison for minor abuses that did not cause economic or physical harm.

While the law was intended for the prosecution of hackers committing computer abuse by stealing valuable personal or corporate information, or causing damage when they break into a computer system, Congress has expanded the scope of the CFAA five times so that activities that were once considered misdemeanors are now federal felonies. As a result, everyday users can be punished for seemingly minor infractions of an application’s terms of service.

The CFAA, for instance, makes white lies such as understating your age or weight on a dating site a crime (even though this is rarely if ever prosecuted). It also makes violating a company’s policy on using a work computer for personal use a felony. If the law were widely enforced, almost every white collar worker in America would be in prison for computer abuse. Because it is arbitrarily and sometimes overly enforced, federal judges and scholars have advocated for changing the law to decriminalize terms of service violations. One impediment to loosening the law has been resistance by corporations who benefit from it. One of the changes to the CFAA in 1994, for example, amended the law to allow for civil actions, giving corporations a way to sue employees who steal company secrets.

Examples of Computer Abuse

An incident that many people might not think of as computer abuse is creating a fake social media account. If the social media service’s terms and conditions require users to provide accurate information about their identities when creating an account, they could be prosecuted under the CFAA. This outcome is unlikely unless an individual uses a fake account for malicious purposes, such as cyberbullying, but it is a possibility—and that possibility of being prosecuted for something as minor as the mere creation of a fake account is a major problem with the CFAA. Attorneys have been able to exploit the law’s weaknesses to defend clients who should perhaps have been punished, and prosecutors have been able to exploit the law to obtain convictions for minor incidents.

The most well-known example of the unintended consequences of expanding the Computer Fraud and Abuse Act was the threat of a 35-year prison sentence for internet activist Aaron Swartz for allegedly downloading millions of pay-walled academic articles to which access was restricted through a subscription service, probably with the intent to freely distribute them. Arguably, Swartz’s alleged actions would be constituted as theft, but did the proposed punishment fit the alleged crime? Swartz did not seem to think so — he took his own life before the case could go to trial.

Aaron’s Law was a bill introduced in the United States Congress in 2013 in honor of Swartz to loosen the CFAA. Though the bill did not pass Congress, it remains an influential bill

The Computer Misuse and Cybercrimes Act No. 5 of 2018 (the **Act**) was assented to on 16 May 2018 and commenced on 30 May 2018. The Act aims to protect the confidentiality, integrity and availability of computer systems, programs and data as well as facilitate the prevention, detection, investigation, prosecution and punishment of cybercrimes.

Prior to the commencement of the Act, Bloggers Association of Kenya filed Petition 206 of 2018 at the High Court challenging the constitutionality of twenty-six (26) sections of the Act. Some of the salient provisions that were suspended covered the composition of the National Computer and Cybercrimes Co-ordination Committee and the establishment of certain offences.

The High Court suspended the contested sections on 30 May 2018 and the suspension was lifted on 20 February 2020 when the High Court dismissed the petition.

Subject to any appeal to the Court of Appeal, all the provisions of the Act are in full force and effect. We highlight some of the key provisions of the Act below:

1. The Act establishes various offences including unauthorised interference or interception of computer systems programs or data, false publication of data, cyber harassment, cybersquatting, cyber terrorism, identity theft and impersonation, phishing, computer fraud, computer forgery, unauthorised disclosure of passcodes, fraudulent use of electronic data, issuance of false e-instructions among others.
2. The Act requires service providers to assist in investigation of offences e.g. by collecting and providing data to the investigation officers.
3. The Act prescribes hefty penalties for contravention of its provisions. These include fines, imprisonment, confiscation of assets purchased from proceeds of an offence and compensation.

Pursuant to the commencement of the Act, companies can prevent the commission of the offences established under the Act by formulating and implementing cybersecurity strategies, frameworks, policies and procedures.

6.2. Privacy and Freedom of information

Alternatively referred to as **cyber crime**, **e-crime**, **electronic crime**, or **hi-tech crime**. **Computer crime** is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

Why do people commit computer crimes?

In most cases, someone commits a computer crime to obtain goods or money. Greed and desperation are powerful motivators for some people to try stealing by way of computer crimes. Some people may also commit a computer crime because they are pressured, or forced, to do so by another person.

Some people also commit a computer crime to prove they can do it. A person who can successfully execute a computer crime may find great personal satisfaction in doing so. These types of people, sometimes called black hat hackers, like to create chaos, wreak havoc on other people and companies.

Another reason computer crimes are sometimes committed is because people are bored. They want something to do and don't care if they commit a crime.

Examples of computer crimes

Below is a list of the different types of computer crimes today. Clicking any of the links gives further information about each crime.

- **Child pornography** - Making, distributing, storing, or viewing child pornography.
- **Copyright violation** - Stealing or using another person's Copyrighted material without permission.
- **Cracking** - Breaking or deciphering codes designed to protect data.
- **Cyber terrorism** - Hacking, threats, and blackmailing towards a business or person.
- **Cyberbully or Cyberstalking** - Harassing or stalking others online.
- **Cybersquatting** - Setting up a domain of another person or company with the sole intention of selling it to them later at a premium price.
- **Creating Malware** - Writing, creating, or distributing malware (e.g., viruses and spyware.)
- **Data diddling** - Computer fraud involving the intentional falsification of numbers in data entry.
- **Denial of Service attack** - Overloading a system with so many requests it cannot serve normal requests.
- **Doxing** - Releasing another person's personal information without their permission.
- **Espionage** - Spying on a person or business.
- **Fraud** - Manipulating data, e.g., changing banking records to transfer money to an account or participating in credit card fraud.
- **Green Graffiti** - A type of graffiti that uses projectors or lasers to project an image or message onto a building.
- **Harvesting** - Collect account or account-related information on other people.
- **Human trafficking** - Participating in the illegal act of buying or selling other humans.
- **Identity theft** - Pretending to be someone you are not.
- **Illegal sales** - Buying or selling illicit goods online, including drugs, guns, and psychotropic substances.
- **Intellectual property theft** - Stealing practical or conceptual information developed by another person or company.
- **IPR violation** - An intellectual property rights violation is any infringement of another's Copyright, patent, or trademark.
- **Phishing** or **vishing** - Deceiving individuals to gain private or personal information about that person.
- **Ransomware** - Infecting a computer or network with ransomware that holds data hostage until a ransom is paid.
- **Salami slicing** - Stealing tiny amounts of money from each transaction.
- **Scam** - Tricking people into believing something that is not true.
- **Slander** - Posting libel or slander against another person or company.
- **Software piracy** - Copying, distributing, or using software that was not purchased by the user of the software.
- **Spamming** - Distributed unsolicited e-mail to dozens or hundreds of different addresses.
- **Spoofing** - Deceiving a system into thinking you are someone you're not.
- **Swatting** - The act of calling in a false police report to someone else's home.
- **Theft** - Stealing or taking anything (e.g., hardware, software, or information) that doesn't belong to you.
- **Typosquatting** - Setting up a domain that is a misspelling of another domain.
- **Unauthorized access** - Gaining access to systems you have no permission to access.
- **Vandalism** - Damaging any hardware, software, website, or other object.
- **Wiretapping** - Connecting a device to a phone line to listen to conversations.

Data privacy defines who has access to data, while data protection provides tools and policies to actually restrict access to the data. Compliance regulations help ensure that user's privacy requests are carried out by companies, and companies are responsible to take measures to protect private user data

Data Security and Protection

Data security is one of the most daunting tasks for IT and infosec professionals. Each year, companies of all sizes spend a sizable portion of their IT security budgets protecting their organizations from hackers intent on gaining access to data through brute force, exploiting vulnerabilities or social engineering. Throughout this guide are links that will help you learn more about the challenges related to securing sensitive data, ensuring compliance with government and industry mandates, and maintaining customer privacy. Along with the challenges, you'll find advice on how to solve them.

Why data security is important

The average cost of a data breach in 2019 was calculated at $3.92 million, according to a report by the Ponemon Institute and IBM Security. High-profile companies such as Capital One, Evite and Zynga experienced data breaches that exposed more than 100 million customer accounts each. The average security incident in 2019 involved 25,575 accounts, according to the report. To make matters worse, this information must be disclosed to customers, and organizations could potentially wind up as cautionary tales.

The lessons from these breaches are numerous, including the need to do the following:

- review credential requirements and policies;
- keep track of what data is retained and where it is stored;
- check for cloud misconfigurations regularly; and
- force password resets if a breach is suspected.

The move to the cloud presents an additional threat vector that must be well understood in respect to data security. The 2019 SANS State of Cloud Security survey found that 19% of survey respondents reported an increase in unauthorized access by outsiders into cloud environments or cloud assets, up 7% since 2017.

Ransomware and phishing also are on the rise and considered major threats. Companies must secure data so that it cannot leak out via malware or social engineering.

Breaches can be costly events that result in multimillion-dollar class action lawsuits and victim settlement funds. If companies need a reason to invest in data security, they need only consider the value placed on personal data by the courts.

Sherri Davidoff, author of *Data Breaches: Crisis and Opportunity*, listed five factors that increase the risk of a data breach: access; amount of time data is retained; the number of existing copies of the data; how easy it is to transfer the data from one location to another -- and to process it; and the perceived value of the data by criminals.

Many organizations realize that the value of data and the cost to protect data are increasing simultaneously, making it near impossible to protect data by just layering on more security. Instead, IT and infosec teams must think proactively and creatively about their data protection strategies.

They should also assess their risk versus the protections their current security investments provide and make decisions accordingly. To do so requires an unprecedented level of visibility that most organizations do not possess right now.

Security expert Ashwin Krishnan advised IT and security professionals to focus on three key aspects when trying to improve data security in the modern enterprise: the more data generated and collected presents a bigger "surface" for data breaches; customer rights expand with new regulatory compliance and privacy compliance mandates, such as GDPR and the California Consumer Privacy Act; and companies have to be aware if they are involved in data brokering.

Data privacy and compliance standards

Developing, implementing and enforcing data security best practices is made easier if organizations fully understand the privacy and compliance mandates to which they must adhere.

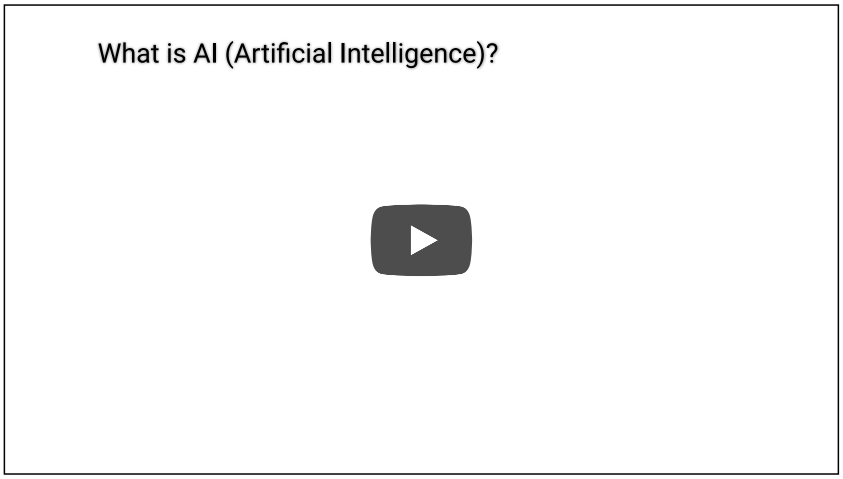
The California Consumer Privacy Act (CCPA) went into effect January of this year. It enforces consumers' rights to control their personal information. Many experts believe a version of the CCPA will likely become federal law. CCPA itself is a take on the European Union's General Data Protection Regulation, which also protects consumers' personal data.

While companies worry that the cost to comply with government mandates could be prohibitive, many are still going forward in their efforts to ensure data is able to be discovered, reported on and erased. That way, when consumers request to see their data and then delete it, businesses will be ready.

To follow the multiple compliance mandates, organizations can create a data inventory, establish processes to get consumers their information under deadline and make updates to the organization's privacy statement.

The future of data security

AI and machine learning are going to be key in compliance efforts going forward. Companies are looking to automate some regulatory compliance processes, including data location and extraction. Inventories, as security expert Michael Cobb noted, become outdated unless automated scanning tools are deployed to sustain data discovery capture by recording regular snapshots of all applications and repositories where personal information resides. Automation, in his opinion, is the only way large organizations can remain compliant with a large volume of data that is structured and unstructured and stored in data centers and in the cloud.



Next-generation technology could also help companies fall in line with other compliance mandates, such as PCI DSS. For companies that have lagged behind on compliance, some security experts suggest considering a zero-trust model as a security strategy. With zero trust, companies would look at the full lifecycle of data management and broaden their focus beyond just payment card data to other forms of personal data, including financial data, intellectual property and customer data. They would make no assumptions on where data is expected to be found or how it is being used -- only that the risk must be mitigated.

Data security will remain a significant challenge well into the future, but creative applications of AI and machine learning and zero-trust models will help IT and infosec teams protect data and ensure consumer privacy.

The Privacy Act:

Regulates Federal Government agency recordkeeping and disclosure practices. Allows most individuals to seek access to Federal agency records about themselves. Requires that personal information in agency files be accurate, complete, relevant, and timely

Data privacy is the protection of personal data from those who should not have access to it and the ability of individuals to determine who can access their personal information.

Freedom of Information and Protection of Privacy Act

The *Freedom of Information and Protection of Privacy Act* (FIPPA) provides a right of access to records held by public bodies and regulates how public bodies manage personal information. FIPPA also provides an independent review process for people who disagree with access and privacy decisions made by public bodies under the Act.

Difference between Freedom of Information and Data Protection.

FOI covers information held by public authorities, but not requests for personal information about the person making the request. FOI is about providing access to public information. Data protection legislation protects personal data.

Freedom of information should be guaranteed as a legal and enforceable right permitting every individual to obtain records and information held by the executive, the legislative and the judicial arms of the state, as well as any government owned corporation and any other body carrying out public functions.

7. Software safety

- Health and Safety at Work

- Software Safety

7.1. Health and Safety at Work

Safety and health at work refer to **guidelines, programs, and practices that safeguard any worker's safety, well-being, and health**. The ultimate purpose of any safety and health program is to provide the most secure working environment and minimize the likelihood of injuries, accidents, and deaths on the job.

The purpose of health and safety is **to protect your workers, sub-contractors, customers and members of the public when they are involved with your business**. You have a duty of care under the Health and Safety at Work Act 1974 but more than that, it's good business practice to adhere to health and safety laws.

The main provisions of these Regulations require employers to provide: adequate lighting, heating, ventilation and workspace (and keep them in a clean condition); staff facilities, including toilets, washing facilities and refreshment; and. safe passageways, i.e. to prevent slipping and tripping hazards.

It ensures that all employers provide a safe working environment and look out for the health of their employees—wherever their place of work. It relates to the wellbeing of not only permanent staff but also casual, self-employed and temporary workers, as well as visiting members of the public.

There are five main regulations that businesses with safety equipment must consider:

1. The Health and Safety at Work Act 1974
2. The Personal Protective Equipment At Work Regulations 1992
3. PUWER
4. LOLER (if you’re using lifting equipment)
5. WAHR (if you’re working at height)

1. The Health and Safety at Work Act 1974

The Health and Safety at Work Act 1974 (HSWA, the HSW Act, the 1974 Act or HASAWA) is the main piece of legislation covering occupational health and safety in the UK. The act clarifies the general responsibilities of everyone from employers and employees to owners and managers of the workplace for maintaining health and safety.

2. The Personal Protective Equipment at Work Regulations 1992

The Personal Protective Equipment At Work Regulations 1992 is a set of regulations created under The Health and Safety Act placing liability on the employer to ensure suitable personal protective equipment has been granted for those who may be exposed to a risk to their health or safety at work.

3. Provision and Use of Work Equipment Regulations 1998 (PUWER)

These regulations aim to make work safer for anyone using and coming in contact with equipment, this includes employers, employees, contractors, suppliers and people who may need to access any equipment. The regulation ensures that equipment is kept in good order and that maintenance, training and inspections are carried out to suitable and sufficient levels to identify if the equipment can be used.

4. Lifting Operations and Lifting Equipment Regulations 1998 (LOLER)

LOLER places responsibilities on people and companies who own, operate or have control over lifting equipment. If any lifting equipment is provided you must manage and control the risks to avoid any injuries or damages.

5. The Work at Height Regulations (WAHR)

Falls from height is one of the biggest causes of deaths and major injuries for the work at height sector. The Work at Height Regulations was introduced to prevent death and injury caused by a fall from height.

The computer is a vital tool in many different jobs and activities, for adults and children. But long periods of using a computer can increase your chance of developing an injury. Inappropriate computer use can cause muscle and joint pain, overuse injuries of the shoulder, arm, wrist or hand, and eyestrain.

Children can experience particular physical and psychological problems if they play computer games too much. You can reduce or avoid these risks with the correct furniture, better posture and good habits, such as taking rest breaks and restricting time spent playing computer games.

Posture-related injuries from computer use

Back and neck pain, headaches, and shoulder and arm pain are common computer-related injuries. Such muscle and joint problems can be caused or made worse by poor workstation (desk) design, bad posture and sitting for long periods of time.

Although sitting requires less muscular effort than standing, it still causes physical fatigue (tiredness) and you need to hold parts of your body steady for long periods of time. This reduces circulation of blood to your muscles, bones, tendons and ligaments, sometimes leading to stiffness and pain. If a workstation is not set up properly, these steady positions can put even greater stress on your muscles and joints.

Preventing computer-related muscle and joint injuries

Tips to avoid muscle and joint problems include:

- Sit at an adjustable desk specially designed for use with computers.
- Have the computer monitor (screen) either at eye level or slightly lower.
- Have your keyboard at a height that lets your elbows rest comfortably at your sides. Your forearms should be roughly parallel with the floor and level with the keyboard.
- Adjust your chair so that your feet rest flat on the floor, or use a footstool.
- Use an ergonomic chair, specially designed to help your spine hold its natural curve while sitting.
- Use an ergonomic keyboard so that your hands and wrists are in a more natural position.
- Take frequent short breaks and go for a walk, or do stretching exercises at your desk. Stand often.

Computer-related overuse injuries of the hand or arm

Muscles and tendons can become painful with repetitive movements and awkward postures. This is known as ‘overuse injury’ and typically occurs in the elbow, wrist or hand of computer users. Symptoms of these overuse injuries include pain, swelling, stiffness of the joints, weakness and numbness.

Preventing computer-related overuse injuries

Tips to avoid overuse injuries of the hand or arm include:

- Have your mouse at the same height as your correctly positioned keyboard.
- Position the mouse as close as possible to the side of the keyboard.
- Use your whole arm, not just your wrist, when using the mouse.
- Type lightly and gently.
- Mix your tasks to avoid long, uninterrupted stretches of using the computer.
- Remove your hands from the keyboard when not actively typing, to let your arms relax.

Eyestrain from computer use

Focusing your eyes at the same distance point for long periods of time causes fatigue. The human eye structurally prefers to look at objects more than six metres away, so any work performed close up puts extra demands on your eye muscles.

The illuminated computer screen can also cause eye fatigue. Although there is no evidence that eye fatigue damages your eyesight, computer users may get symptoms such as blurred vision, temporary inability to focus on faraway objects and headaches.

Preventing eyestrain from computer use

Tips to avoid eyestrain include:

- Make sure your main source of light (such as a window) is not shining into your face or directly onto the computer screen.
- Tilt the screen slightly to avoid reflections or glare.
- Make sure the screen is not too close to your face.
- Put the screen either at eye level or slightly lower.
- Reduce the contrast and brightness of your screen by adjusting the controls.
- Frequently look away from the screen and focus on faraway objects.
- Have regular eye examinations to check that any blurring, headaches and other associated problems are not caused by any underlying disorders.

Injuries from laptop computers

The growing use of laptop computers has caused more pains, strains and injuries among computer users.

Laptop computers were designed to be used for short periods of time when a person couldn’t access a desktop computer. But these days many people use a laptop all the time.

The problem is that the monitor and keyboard of a laptop are very close together. To position the monitor at the right height for your back and neck causes you to lift your arms and shoulders too high. But to position the keyboard at the best height for your arms and shoulders, you must hunch your shoulders and neck to see the monitor.

Carrying your laptop around can also strain your muscles and joints.

Preventing injury from laptop computers

Tips to reduce laptop dangers include:

- Use a correctly set-up desktop computer instead of a laptop as often as you can.
- Use peripheral equipment, such as a docking station, separate keyboard, mouse and laptop stand.
- Take frequent breaks.
- Carry your laptop in a backpack or in wheel-along luggage.

Children and computer-related injuries

Researchers believe that electronic games may be among the causes of childhood obesity (being very overweight). And like adults, children might also get overuse injuries of the hand, and muscle and joint problems such as back and neck pain or headaches.

Some research has shown that playing violent computer games and a large amount of game time may cause aggressive behaviour in some children and may negatively affect a child's school work. Although computer and video games are fun and offer benefits such as improved spatial awareness, parents should keep in mind that moderation is important in avoiding health problems.

Health risks from computer games

Playing computer games for too long or without correct furniture and posture can lead to health problems such as:

- Overuse injuries of the hand
- Obesity
- Muscle and joint problems
- Eyestrain
- Behavioural problems including aggressive behaviour
- Photosensitive epileptic seizures (caused by flashing or rapidly changing lights – this is rare).

Parents can reduce the risk of children developing computer-related health problems. You can encourage your child to:

- Sit at least one metre away from the screen
- Take frequent breaks
- Pursue other activities. Encourage your child to enjoy different hobbies and interests, particularly sports and physical activities.

You can also:

- Set sensible time limits on your child's game playing. Some guidelines recommend no more than two hours of screen time each day
- Set up the computer, desk, chair and keyboard to suit your child's height. For example, adjust the chair so that your child's feet rest flat on the floor
- Buy an ergonomic chair
- Buy a smaller mouse, which suits the size of your child's hand
- Teach your child to use the keyboard and mouse properly and safely, such as pushing the buttons and other controls gently. Using unnecessary force increases the risk of overuse injury.

Benefits of computer games

Playing video and computer games is a lot of fun, and can offer children other important benefits too. Depending on the game, playing can improve:

- Spatial awareness
- Iconic skills (reading images or diagrams)
- Visual attention skills (such as keeping track of various objects at the same time)
- Attention span in children who have attention problems.

Where to get help

- Your doctor
- Physiotherapist
- Health and safety officer
- Australian Physiotherapy Association Tel. (03) 9092 0888 or 1300 306 622
- WorkSafe Victoria Tel. (03) 9641 1444 or 1800 136 089

Things to remember

- Working at a computer can cause back, neck and shoulder pains, headache, eyestrain and overuse injuries of the arms and hands.
- You can help avoid computer-related injuries with proper furniture, better posture and good working habits.
- Parents should put sensible time limits on their children's computer use and video-game playing.
- Your child should take regular breaks from using a computer and should do some physical activities each day.

7.2. Software Safety

In software engineering, software system safety **optimizes system safety in the design, development, use, and maintenance of software systems and their integration with safety-critical hardware systems in an operational environment**.

Software safety issues become important **when computers are used to control real-time, safety-critical processes**. This survey attempts to explain why there is a problem, what the problem is, and what is known about how to solve it

A safety requirement may be met by **a combination of safety functions, and these may be implemented in systems of different technologies** – for example, a software-based system along with management procedures, checklists, and validation procedures for using it.

Software safety issues become important when computers are used to control real-time, safety-critical processes. This survey attempts to explain why there is a problem, what the problem is, and what is known about how to solve it. Since this is a relatively new software research area, emphasis is placed on delineating the outstanding issues and research topics.

Fundamental Principles of Software Safety Assurance - Tim Kelly

Context Lack of agreement in the details of requirements of software safety assurance standards has long been recognised However, some common fundamental principles can be observed Tension sometimes exists between those advocating demonstrating compliance to standards as the principal assurance approach and those that promote the production of software assurance cases Often incorrectly presented as totally opposing alternative approaches

3 4+1 Principles P1 - Software safety requirements shall be defined to address the software contribution to system hazards. P2 - The intent of the software safety requirements shall be maintained throughout requirements decomposition. P3 - Software safety requirements shall be satisfied. P4 - Hazardous behaviour of the software shall be identified and mitigated. P4+1 - The confidence established in addressing the software safety principles shall be commensurate to the contribution of the software to system risk.

4 DO-178C Principle 1 Assumed starting point in DO-178B/C is that behavioural safety requirements allocated to software have already been derived by system level safety analysis performed in accordance with ARP 4754A ARP4754A addresses the problem of validation of these requirements ARP 4754A also defines the process for judging the criticality of the contribution of software to system level hazards and expresses this as an allocated software DAL

5 DO-178C Principle 2 strong emphasis on maintaining traceability through the stages of software development recognises problem of validation of decomposition, e.g. through requirements for review simply recording traceability information is necessary for but insufficient need justification (cf. Rich Traceability)

6 DO-178C Principle 3 well addressed - verification evidence that addresses the demonstration of requirements both under normal conditions and fault conditions DO-178C admits a wider range of verification techniques

7 DO-178C Principle 4 recognises that Software design process activities could introduce possible modes of failure into the software or, conversely, preclude others and In such cases, additional data should be defined as derived requirements and provided to the system safety assessment process. Removal of errors leading to unacceptable failure conditions as an objective of testing Acknowledges that The effects of derived requirements on safety related requirements are determined by the system safety assessment process. However,

8 DO-178C Principle 4+1 captured through the mechanism of DALs that tailor requirement for the demonstration of the objectives of the standard according to criticality

9 IEC Principle 1 clearly defines safety lifecycle that describes generation of safety requirements from hazard analysis Two Aspects: Functional Requirements + Integrity Requirements

10 IEC Principle 2 process of requirements decomposition and allocation addressed across Parts 1, 2 (concerning requirements allocated to hardware) and 3 (concerning requirements allocated to software) validation and justification of this decomposition and allocation receives less attention

11 IEC Principle 3 strongly emphasised, e.g. in Part 3 requirements must be demonstrably satisfied described as software safety validation choice of techniques guided by techniques recommended for SIL

12 IEC Principle 4 weakly supported software development lifecycle defined in Part 3 assumes a conventional flow down of software requirements into implementation (and test) little mention of the potential for emergent hazardous behaviours as a result of design commitments made during software development no specific mention of the activity of software hazard analysis

13 IEC Principle 4+1 addressed the mechanism of SILs that tailor guidance on design measures (e.g. architectural features) and development and assurance techniques (e.g. types of testing) according to the criticality of the software

14 ISO Principle 1 clearly defines safety lifecycle that describes generation of safety requirements from hazard analysis Two Aspects: Functional (Behavioural) Requirements + Integrity (ASIL) Requirements

15 ISO Principle 2 process of requirements decomposition and allocation addressed across Parts 3, 4, 5 (concerning requirements allocated to hardware) and 6 (concerning requirements allocated to software) (Brief) mention of validation (e.g. checking whether Functional Safety Requirements address safety goal

16 ISO Principle 3 strongly emphasised, e.g. in Part 6 requirements must be demonstrably satisfied for software 6-11 Verification of Software Safety Requirements alongside unit, integration test etc. robustness testing (e.g. fault injection also mentioned) choice of techniques guided by techniques recommended for ASIL

17 ISO Principle 4 software development lifecycle defined in Part 6 assumes a conventional flow down of software requirements into implementation Some mention of the potential for emergent hazardous behaviours as a result of design commitments made during software development (esp. in architecture) There is mention of the safety analysis for software

18 ISO Principle 4+1 addressed the mechanism of SILs that tailor guidance on development and assurance techniques (e.g. types of testing) according to the criticality of the software Example (from Part 6):

19 Observations P1-3 can be observed to be at the heart of the standards P4 is less well addressed However, they discuss the potential for systematic error introduction within the software development lifecycle Standards attempt to address P4+1 through DALs and SILs differences in allocation and what is varied lack of a significant evidence-base that demonstrates that either approach to varying confidence can be easily correlated with achieved risk reduction

20 Generic vs. Specific Application of Principles intent of principles is not that they are addressed generically (e.g. by appeal to generic processes or adherence to standards) should be evidenced specifically requirements and processes of a standard may be capable of demonstrating principles, but may still fall short in practice consider Requirements Review application of standards cannot be considered in a tokenistic sense, as a talisman of confidence

21 Generic vs. Specific Application Significant issue re: P4+1 of Principles Standards established a general set of requirements for varying requirements, processes and techniques according to an abstract level of required confidence Generality is potentially a problem Is it what s required in a specific case - e.g. applicability of MCDC metrics? Opportunity cost of doing something that doesn t add to confidence Some mechanisms to address: PSAC, SAS in DO-178C, Justification of selection from amongst loose SIL recommendations in IEC 61508

22 How Principles relate to Example definition: Assurance Cases a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that the software is safe when forming part a system for a given application in a given environment. does not describe how a compelling, comprehensible and valid case is to be made, Genericism is both weakness and strength Weakness: many possible candidates - e.g. pure appeal to process or adherence to standard (compliance / conformance argument) Strength: the very requirement for an assurance case is a requirement for a developer to state their case for their specific software development

23 Worst Case - Best Case Worst - fail to cover the 4+1 principles to the same extent as the two standards described (we are to ignore standards at our peril!) Best - addressing all of the relevant requirements and recommendations of standards, and in addition presenting compelling arguments for the specific enactment of those standards

24 Assurance Case Guidance Def Stan Issue 4 Part 1 re: P2 The means of recording [requirements] traceability is not prescribed; however, traceability should be demonstrated within the Safety Case. Def Stan Issue 4 Part 2 re: P3 and P4 Demonstration of safety includes finding the credible evidence that shows that the derived safety requirements are correctly implemented and hence that safety requirements are satisfied. Evidence should demonstrate that implementation has not adversely affected the safety of the system. Pattern based Guidance that explicitly addresses principles (Hawkins et al. 2013)

25 P4+1 & Assurance Cases Remains a challenge Alternative approaches proposed: Quantitative reasoning about Possibility of Perfection - Littlewood and Rushby Baconian philosophy (incl. defeaters) - Goodenough and Weinstock Risk + Confidence Argument approach (incl. concept of assurance deficits) York + Virginia explicit and specific treatment of Principle 4+1 Consider P3 Risk argument

26 Complementarity Existing software safety and assurance standards represent a substantial BOK e.g. coverage requirements of DO-178B/C can be seen as important for flushing out implementation errors in the software development process If nothing else, should be used as an informative checklist e.g. a (product oriented) risk mitigation requirement within in a standard that is not addressed in an assurance case could require justification Challenge is sometimes to understand the (risk reduction) rationale behind some of their requirements, see (Holloway 2013)

27 Targeting Assurance Case Effort Many standards provide the template for the technical risk argument needed at the core of any software assurance case (forming central pillar of response to P1,2 & 3) Standards also provide general requirements and recommendations for the avoidance of potentially hazardous errors and anomalous behaviour (P4) Standards also provide general guidance on how effort should be tailored according to risk (P4+1) Confidence can be lost in the (lack of) justification of the specific instantiation of these template structures and general guidance Assurance Cases can help here!

28 Targeting Assurance Case Effort P1 - assurance cases are well suited to the (inevitably subjective) justification of the adequacy of the identified software safety requirements P2 - well suited to the hard problem of the justification of maintenance of intent in traceability structures P3 - well suited to the justification of the adequacy of evidence (e.g. the appropriateness and trustworthiness of specific forms of evidence for requirements satisfaction) P4 - usefully targeted at the justification of the management of unintentionally hazardous side effects of otherwise intentional design commitments P4+1 - directly relates to the notion of a confidence / meta argument

29 Summary Principles based evaluation of software safety standards P1-3 served well, P4 & 4+1 not so well Assurance Cases shouldn t duplicate aspects covered well by standards, and shouldn t ignore the BOK Standards suffer from problems relating to specific enactment and judgement Standards can t remove (subjective) judgement Assurance cases are good at explicitly representing and recording judgements Crass to say it s either-or

8. Professional development

Professional development refers to continuing education and career training after a person has entered the workforce in order to help them develop new skills, stay up-to-date on current trends, and advance their career.

Professional development refers to continuing education and career training after a person has entered the workforce in order to help them develop new skills, stay up-to-date on current trends, and advance their career.

Beyond continuing education, professional development can refer to many different types of relevant educational or training opportunities relevant to the professional's work. Even when not required, many professionals who want to excel in their career will voluntarily seek out professional development and learning opportunities.

Many fields require professionals to participate in continuing education and ongoing learning, sometimes as a prerequisite for keeping their job or to maintain their license, designation, or certification. In these cases, the field likely has specific continuing education (CE) or continuing professional education (CPE) requirements which must be completed through an approved continuing education provider.

The purpose of professional development is to give professionals the opportunity to learn and apply new knowledge and skills that can help them in their job and further their career. Professional development is all about building your skill set and knowledge base for your field.

And professional development isn't just helpful for you — it's helpful for your employer, too. By having opportunities to learn, increase your skill sets, and stay up-to-date on industry trends, professionals like yourself increase your own worth while also adding to your company's overall value.

Professional development and professional training opportunities provide many other specific benefits for both young and experienced professionals. Some of these benefits are listed below, but this list is by no means comprehensive.

Benefits of professional development include:

1. **Professional development expands your knowledge base.** Professional development and continuing education opportunities can expose both young and experienced professionals to new ideas, solidify their knowledge, and increase their expertise in their field. Those who actively seek out these learning opportunities are those who will benefit most from them.

2. **Professional development boosts confidence and credibility.** By increasing professionals' expertise through professional development, their confidence in their work will increase as well. No one likes to think they're missing important skills in their industry. Professional development courses, continuing education, and training opportunities allow professionals to build confidence and credibility as they acquire new skill sets and professional designations.

3. **Professional development increases earning potential and hireability.** Professional development and continuing education offers both young and experienced professionals with opportunities to boost their earning potential and future hireability by increasing their knowledge and updating their skill sets. Professional credentials, certifications, and designations — most of which can be accessed and obtained online — also provide easy ways to increase a professional's value. Professionals with the right skill sets who seek out and take advantage of upskilling opportunities are certainly more bankable than those who don't.

4. **Professional development can provide networking opportunities.** Many professional development opportunities such as workshops, conferences, and other networking events allow professionals to branch out and meet other people within their industry who may be able to help them with career opportunities in the future. When you decide you want a change or are ready to move up in your career, your professional network and the professional relationships you forged will come in handy.

5. **Professional development keeps professionals current on industry trends.** Professional development and continuing education and learning opportunities are great ways to stay up-to-date on industry knowledge and trends. Every professional industry is constantly evolving, so employees should use professional development and training opportunities to expand their knowledge base, learn new practices and techniques, and embrace new technology.

6. **Professional development can open the door to future career changes.** For professionals who are looking to make a complete career change or to pivot within their industry, new skills acquired through professional development training could be critical to opening new doors within their field or to transition to a new industry.

Ways to improve your professional development include:

- **Develop a timeline with career milestones**. If appropriate, take your timeline to your boss or manager during your one-on-one meetings or annual reviews and ask them to help you manage your career to reach your milestones.

- **Take advantage of any and every training program** and professional development opportunity your company offers and you think would be helpful to your career.
- **Find a mentor you look up to** and whose career growth you would like to imitate. A mentor is a great way to learn about new opportunities, and learning from someone else's experience can give you an edge over other professionals.
- **Consider a lateral move within your industry** to broaden your experience. Having an understanding of and being able to perform multiple related jobs can be very helpful as you progress in your career.

Most importantly, **have a career plan**. A career plan should include your timeline and milestones mentioned above along with your career goals and how you plan to achieve them. The most successful people in any industry who are satisfied in their careers proactively planned what they wanted from their career. As your career progresses and you gain a better understanding of your industry and what you want from a career, be sure to update your career plan.

Examples of professional development opportunities include:

- **Attend a professional conference.** Conferences are great opportunities to learn from experts in your field, network with like-minded professionals, and have a good time. If an out-of-town conference is not possible, there are still many online conferences and webinars professionals can register for.
- **Participate in workshops.** The purpose of workshops is to bring together professionals with specific expertise to discuss problems and offer solutions. Unlike most conferences, workshops require active participation from those attending. This hands-on experience can be especially useful in learning new skills.
- **Complete your CE/CPE.** Continuing education is required to maintain most professional licenses and designations. Some people view continuing education as a chore they have to get out of the way every year, but proactive professionals take advantage of their continuing education courses to hone their knowledge and update themselves on their industry.
- **Take advantage of microlearning.** Microlearning is an effective learning method especially useful for busy professionals. Also known as "bite-sized learning", microlearning consists of brief learning units that give brief, focused bursts of content (usually between 1 and 10 minutes long) allowing professionals to fit short learning sessions into their busy schedules.
- **Shadow a colleague.** If opportunity presents itself, it may be useful to shadow a colleague or superior whose type of job or skills you're interested in. Shadowing another professional can be a positive learning experience that can offer a lot of clarity about your interest in that career.
- **Read a book that can help you in your field.** There are going to be a lot of books out there, no matter what industry you're in. If you're unsure of what to read, ask your manager or mentor what they recommend.

Obtaining a professional certification, license, or designation can help your career — and your salary. Have you ever been passed up for a job because other applicants had more training or certifications? The truth is relevant certifications, licenses, and designations for your field will only help your career.

For one, obtaining a designation or completing a certificate program not only demonstrates your training and knowledge but also a commitment to your career. Companies will rightfully think you truly want to contribute to their success and thereby your own success.

If there are specific certifications or designations often required or desired in your industry, do what you can to obtain and maintain them. Whenever you have the skills sought after by employers, you'll find it much easier to achieve your career goals — and make more money doing it.

Completing an online certificate program demonstrate a real commitment to your career. It means you're serious about contributing to your company's success by helping it operate more efficiently and profitably. It means you set goals-and achieve them. When you obtain the skills employers seek, you'll find yourself in demand, with real advantages for career success. And you can do this through convenient online training.

9. Personal skills of the IS Professional

Having a strong set of computer information systems skills can set you up for a rewarding career. As big data, the Internet of Things, cloud computing and emerging technologies shape the business world, career opportunities abound for those with the right skills and knowledge.

If you're ready to succeed in computer information systems, skills needed include a variety of both hard and soft skills. From knowledge of hardware and operating systems to team leadership, having the right skills in your toolkit will help you find success in this growing field.

Computer information systems (CIS) are where computers and technology intersect with the business world. CIS professionals maintain, implement and use systems that drive the business world. This means that CIS professionals need different skills than computer science (CS) professionals.

CIS is a unique career choice because it requires several skills ranging from business to computer programming. There are many divergent paths that CIS professionals can take in their careers, but the fundamentals remain the same.

Computer information systems skills include both hard and soft skills. The difference between hard and soft skills is important:

- **Hard skills** are teachable, technical and measurable skills. They might include mathematics, writing, reading, knowledge of a programming language and other computer skills.
- **Soft skills** are more like traits. These are the skills that might make you a better employee. Communication skills, manners and leadership skills are soft skills.

Soft skills and hard skills are equally important. It's been said that your hard skills are what stand out to employers on your resume and help you get the job, while the soft skills are what come into play when it comes to being successful on the job. Computer information systems professionals need both soft and hard skills for career success.

The hard skills you need for a computer information systems career can vary based on the tasks of a job. As an example, web developers need different hard skills than database administrators. Computer systems information skills need to match your career interests.

While the hard skills you need for a CIS job can vary, the soft skills remain the same. Soft computer information systems skills can include:

- Problem solving and analytical skills
- Communication and interpersonal skills
- Cool demeanor and ability to work under pressure
- Attentiveness to detail
- Ability to work on a team
- Time management and organization
- Management and leadership skills
- Imagination, creative thinking
- Recollection (verbal and logical)
- Focus on results
- Strong personal motivation for developing new knowledge

Computer Information Systems Skills

Computer information systems is a unique career choice because it requires several skills ranging from business to computer programming. There are many divergent paths that CIS managers can take in their careers, but the fundamentals remain the same.

Three important computer information systems skills include communication of complex ideas, management of personnel, and analytical skills. Let's break down these three skills and how they might apply to a CIS career.

Communication of Complex Ideas

As in most tech roles, CIS professionals require a keen ability to communicate IT-related issues to other people throughout their organizations. Often positioned as managers within their respective organizations, CIS professionals must communicate these ideas to upper management, stakeholders, and lower-level employees all the same.

Management of Personnel

In most cases, the career trajectory in computer information systems puts one on a path towards managing an organization's IT department. As a result, it is important to have a basic understanding of management. This includes a subset of the following skills: departmental time management, listening to employees and providing resources, issuing performance reviews and training new employees.

Analytical Skills

Corporate technology changes daily and CIS professionals are responsible for steering their organizations toward new trends and away from the old. This often requires several tiers of analytical ability, ranging from math in dealing with a budget, to predictive accuracy in dealing with the efficacy of a new piece of technology.

Corporate Information Technology

Perhaps the most important of all computer information systems skills, especially when starting in the industry, is a general understanding of all IT tasks performed in the corporate setting. In most cases, corporate networking and organizational structure are different than what CIS students learn in college. This is a skill that can be attained quickly with an internship.

Computer Information Skills by Job

As mentioned above, the skills required for a computer information systems career can vary based on your individual interests and job path. Learn more about how information technology and computer information systems skills can lead you to your dream job.

Software Developer Skills

You need a few specific skills to be a software developer. To be a successful software developer, you need to have a few technical CIS skills. A few skills you'll need include:

Programming, scripting and markup languages: Developers need to be strong in at least one language, good developers are skills in many. According to a survey from Stack Overflow, the most popular programming languages in 2019 were:

- JavaScript
- HTML CSS
- SQL
- Python
- Java
- Bash/Shell/Powershell
- C#
- PHP
- C++
- TypeScript
- C
- Ruby

1. **Networking Basics:** Most developers work on a client-server model. This means understanding basic networking is essential to developing an application.
2. **Text editors:** All programs start with text editors, regardless of the developer's skill. Knowing the basics of these simple programs can help immensely. Knowing an editor and its keyboard shortcuts can make life easier.
3. **SDLC:** All developers need to know the software development life cycle (SDLC). This boils down to 7 phases:
    - Requirement gathering and analysis
    - Feasibility study
    - Design
    - Implementation and Coding
    - Testing
    - Deployment
    - Maintenance

Knowing the ins and outs of the SDLC is essential.

Knowing the technical skills above, among many others, will help you become a good developer.

Computer and Information Systems Manager Skills

You'll need a number of CIS skills to land a job as a computer and information systems manager. Three key skills for a computer and information systems manager include:

1. **Business management skills:** CIS jobs exist where business and technology interset. This means you'll need to know basic business principles like strategic planning, resource allocation, leadership technique, production methods, and coordination of people and resources.
2. **Technical knowledge:** Computer and information systems managers need a strong understanding of technology like circuit boards, processors, chips and computer hardware and software, including basic applications and programming.

3. **Mathematics:** Math is a foundational skills for many CIS careers. Systems managers need an understanding of algebra, statistics, calculus and geometry.

Information Security Analysts Skills

Information security analysts protect computer networks and have many in-demand skills. A few of the skills required to be a successful information security analyst include:

1. **Networking:** To protect networks, you'll need to know their ins and outs and intricacies. This is because malware and other cybersecurity threats depends on computer networks to maximize damage.
2. **Security fundamentals:** When you have top security skills, you'll be able to comb log records to recognize dangerous or atypical activity that could pose a threat These security skills could stop attacks before they happen.
3. **Communication and documentation:** When a security breach or a threat occurs, information security analysts need to communicate and document the danger in a concise and thorough manner. This takes excellent communication and documentation skills.
4. **Incident handling skills:** A proficient information security analyst should be able to prevent most threats before they become an incident. However, sometimes threats become real and this is where incident handling skills come into play. An information breach could be a crime scene, so it is important to know how to respond.

Database Administrator Skills

Database administrators store and organize data using specialized software, some of which they might build themselves. It takes a number of special skills to perform this work. Top skills for database administrators include:

1. **Knowledge of database design, theory and queries:** It takes a lot of specific knowledge to make a database work. Knowledge of these basic database principles is essential.
2. **Structured query language:** Database administrators need to know how databases talk. This includes knowledge of a structured query language (SQL) like SQL/PSM or Transact-SQL.
3. **Storage and networking skills:** The database needs to live somewhere and its information needs to be accessible to users. This is where data storage and networking skills come into play.

How to Develop CIS Skills

If you're seeking to develop computer information systems skills, completing a certification or degree program can help you. There are many options fo CIS certs and degrees. Computer information systems education options include:

1. Certification
2. Associate's degree
3. Bachelor's degree
4. Master's degree
5. PhD

No matter which computer information systems degree you choose to get the skills you'll need, it's important that you complete a CIS internship to get the hands-on skills you need for career success. Between an education program and an internship, you should be ready for a CIS career.

Requirements for Computer Information Systems Career Success

Before pursuing a career in computer information systems, there are several requirements one must meet. Each path in the CIS career trajectory may pose different requirements, but these are ones that generally appear on all career paths.

Several Years of Work Experience

If you look at a job board for openings in computer information systems, you will find many jobs – but very few of them will be for entry-level positions. Entering the field of CIS usually requires a candidate to have several years of experience working in a computer-related position such as programming or information technology. Previous management experience also comes into play, but management experience coming from outside of the tech industry will have less weight.

Certifications and Continued Education

One of the traditional requirements for advancing in a CIS career is through certifications. These are often applied to highly-specific corporate paths such as CIS risk management, internal audit, or systems security. After gaining experience at an organization, many employers are willing to pay for your certification in a recognized certification program for specialized technical training. In addition to graduate degrees in business administration or management information systems, these certifications are a great way to traverse through the higher-paying opportunities in CIS.

Characteristics for CIS Career Success

If you have the skills and meet the requirements of a CIS professional, you may also be interested in knowing whether you display some of the main characteristics of professionals in the field. Having a career in this industry will be more rewarding if you display the following characteristics.

An Interest in Technology

If you are the person among your friends and family who enjoys helping with tech-related issues, or if you have many tech side projects of your own, then you display an obvious interest in the field. This helps to make your job more rewarding, and your coworkers, employees and managers will notice your passion for the industry.

Leadership Qualities

This is something that can be developed through courses, lectures and other professional activities, but having a natural sense of leadership and responsibility will help in advancing through the ranks of your CIS career. Especially as you work your way into management positions, it’s important to have an interest in helping people improve.

An Entrepreneurial Spirit

Often, CIS professionals are intimately involved in their organization’s budget and other business-related information. As a result, your day-to-day life in the industry will be much more rewarding if you enjoy the process of running a business. Within the bounds of corporate requirements and limitations, the most successful CIS professionals take ownership of their duties like they would a personal business.

In all, the computer information systems skills, requirements and characteristics are at the crossroads of the technology and business industries. If you are interested in starting a career in this industry, take note of the requirements, gain the skills, and ask yourself if you have the characteristics that will lead you to a rewarding career in computer information systems.