chp → 2, 3, 4, 5, 6, 7, 8, 9

CASE 1: Polluting the enviorment

Moral Status
- dont throw waste papers on the ground it will pollute the enviorment

Legal Status
- cant make case legal

CASE 2: Oldies get a seat in a loaded bus

Moral Status
- youngsters should give elders a seat

Legal Status
- label some seats for elders
- fine those youngsters that dont give aways seats to the elders

CASE 3: Password Privacy in an organization

Moral Status
- no one should share their password else data can be tampered/stolen

Legal Status
- if anyone leaks someones password they should pay a fine and suspend for a day

CASE 4: An institute giving degree to those eligible vs giving degrees which are not recognised

Moral Status
- no one is supposed to give degrees unless requirements are fulfilled

Legal Status
- unrecognised degrees are not valid

Characteristics of Profession

1. Mastery of an Esoteric Body of knowledge → aquired in higher ed
   - a member of profession needs this body of knowledge in order of knowledge
   - they often embrace a division b/w researchers and practitioners
2. Autonomy
   - They have autonomy both at collective level and indivisual practice
   - sets its own standard rather than taking orders/suggestions from outsiders
3. Formal Organization
   - A professional organization that
     - controls admission to the profession
     - involved in licensing and expelling its indivisual members
4. Code of ethics
   - must be adhered to, no matter what their employment context
5. Social function
   - Medicine → promoting health
   - lawyers for justice

Profession vs Occupation

Profession
- needs extensive training
- can be called occupation if paid for his particular skill
- has to undergo higher education
- tends to be autonomus → demands responsibility lies with the indivisual

Occupation
- A person involved in a job and earning money → means having that job as an occupation
- dosen't need extensive training
- arent paid for knowledge but for what they produce → he/she is supervised by another person
- no one has autonomus power

Reservation of function
- certain activities are restricted to people with appropriate qualifications

Reservation of Title
- only those qualified are allowed the title of profession

Professional Bodies
→ Professional association, Professional organization, Professional society

- professionals are organised into 1 > professional bodies
- It is a non profit organization seeking to further a particular profession
- Starts by a group of people in a learned occupation who are entrusted with mainting control of the occupation

Is Computing a Profession?
- dosent appear to be a 'profession' in the strickest sense, as computer professional
  - have an esoteric body of knowledge
  - have varying degrees of autonomy → depending on where they work
  - There is no single organization governing it → ACM, IEEE
  - Its an activity which supports social institutions

Software Engineering
- It is an area of computing that emerges as a distinct profession within the feild of computing

Washington Accord
- an international accreditation agreement for professional engineering academic degrees

Functions of Professional bodies
- establishing a code of conduct
  - to regulate how members behave in their professional lives
  - to discipline members who breach this code
- establishing mechanisms for spreading
  - knowledge of good practices
  - new developments to its members
    - through
      - publications
      - conferences
      - worldwide web
- setting standards of education and experience
  - that must be met by people wishing to become members of this society
- advising goverment and regulatory bodies about matters within its area of expertise.

Characteristic of Engineering
- software development is now regarded as engineering
- There are 2 constraints on the characteristic of engineering
  1. Must meet the requirements concering their functionality, performance, reliability
  2. The process of designing and building the object must be completed within specified constraints of time and budget.

Agreements covering mutal recognition
There are 3
1. The Washington Accord
   - signed in 1989 the first
   - recognises professional engineering qualifications
   - typically for 4 years
2. The Sydney Accord
   - in 2001
   - recognises engineering technology qualifications
   - typically for 3 years
3. The Dublin Accord
   - in 2002
   - recognises technician engineering qualifications
   - typically for 2 years

→ are considered equivalent in accreditation → recognises

Developing software engineering as a distinct field involves several of the activities.
► For example, it means identifying a unique body of knowledge that a person must possess to be competent software engineer.
► It means developing educational requirements (curriculum) such that the person who meets the requirements is more likely to produce a quality, safe software than someone without training.
It means developing mechanisms for licensing of members.
► This will include identifying or creating the proper organization for issuing licenses and identifying requirements for obtaining a license, such as passing an exam or acquiring a certain number of years of experience.
► Another requirement for professionalization is a code of ethics.
► The state of Texas has boldly taken the first steps in this process and has established software engineering licensing in its state.
► The Texas initiative is a serious attempt at setting standards in the field.

The Status of Engineers
- Its illegal to call yourself engineers unless you are registered with the State Engineers Registration Board
- It's illegal for a company to use the word 'engineering' in its na[me] unless it employs atleast one registered engineer
- academic programes that have the term engineering in their title must be taught mostly by registered engineers
- It is illegal to carry out engineering work except under the supervision of a registered engineer.

PROFESSIONAL BODIES IN COMPUTING
BCS

Education
- BCS promotes education in a number of ways
  - approves organizations offering cources for professional exams
  - Accredits degree programs at higher education institutions
  - Sets the syllabus and accredits organizations for short cources

The Professional Examinations
- introduced in 1973
- recognises skills and lead to qualify for membership
- The stages are
  - Certificate
  - Diploma
  - Professional Graduate Diploma

Accreditation and Exemption
→ means a cource has fulfilled the educational requirement
- a cource may qualify for full or partial exemption from the HEQ → Higher Education Qualifications
- students graduating from such cources can attain professional membership

Short cources
- BCS offers a variety of short cources designed to train industry staff

Code of Conduct
- All professional bodies have a code of conduct
- The BCS's code of conduct is divided in 4 sections

1. The Pubic Interest
   - Regard public health, privacy, security, well being of pubic
   - Regard rights of third party
   - conduct professional activities w/o personal biasness
   - promote equal access to the benefits of IT
2. Duty of the Relavent Authority
   - Avoid conflicts of interest
   - Avoid misrepresentation
   - Dont pass confidential information w/o permission
3. Duty to the Profession
   - Accepting personal duty
   - Avoid actions that harm the image of the profession
   - Seek to improve professional standards through participation in their development, use and enforcement
   - encourage and support fellow members in their professional development
4. Professional Competence and Integrity
   - only take offers that are within your professional competence
   - do not claim any level of competence that you do not have
   - Get up to date knowledge within your related feild
   - Respect and value alternate viewpoints
   - seek, accept, offer honest criticisms of work
   - Avoid harming others by negligent actions
   - Reject bribery

The Advancement of Knowledge
- The first action of BCS was to establish The Computer Journal
- It was published in 1958, and regularly ever since
- currently, 6 issues a year are published

Continuing Professional Development
"The systematic maintenance, improvement and broadening of knowledge and skill and the development of personal qualities necessary for the execution of professional and technical duties throughout the individual's working life."

Activities
- CPD services to indivisual members
  - Computer Bulletin
  - keeping-up-to-date info of latest computer and development
- Career development and CPD services to the industry
  - resolving IT staff issues of placement in the industry and training

Organization
- It is a group of people working together in a formal way
- Legal existence is a must for it

e.g. schools, colleges, hospitals, banks, Private company, goverment

Commercial Organizations
- profiting
- People with particular skill set, strategy, resources work together
- The law offers several ways of setting up and operating it for eg as a
  - sole trader
  - partnership
  - copperative
  - limited company

Non Commercial Bodies
- non profiting
- Staff working as volunteers/nomial pay
- Charity or goverment runs it

Ways organizations gain legal status

1. Sole trader

- a person who runs their own bussiness
- theres no legal formalities to be become one
- if generated income is large enough (isn't necessary)
  - you can register with customs and tax
- 73% bussiness in the US use this approach

cons

- a sole trader is responsible for all bussiness debts meaning personal assets are at risk if bussiness fails (eg family home)

2. Partnership

- when a group of people run a bussiness together to make a profit and the bussiness is not a limited componay
- 73% bussiness in the US use this approach

cons

- difficult to liquidate
- non transferable
- if any partner dies, the partnership agreement dissolves
- share rate

3. Cooperatives (eg agricuture)

- stockholders include both common and preffered shareholders
- legal entity
- legal power reside to sue and to be sued
- Generate 90% of the revenue in any economy

cons

- double taxation
- No secrecy

4. Limited companies

- There are 3 key principles
  1. The company is a seperate legal entity distinct from its employees and owners
  2. Ownership is divided into shares which can be bought and sold → share holders
  3. Shareholders aren't responsible for the company debts they can only loose the amount they invested in shares

The constitution of a limited company

- For a company to be registered, it must have a constitution
- It consists of 2 documents
  1. Memorandum of association
  2. Articles of association

Memorandum

- It is a document that includes the following
  - The company's name must be unique
    - not include country name or restricted words
  - The country/countries where the company's registered office will be located
  - The company's bussiness purpose which may state it will operate as a genral comercial company
  - A liability clause stating that members liability is limited in case of a company limited by shares
  - Details of the companys authorised share capital including the no. and value of its share

Declaration of Association

- The memorandum concludes with a declaration of Association along the following lines

We, the several persons whose names, addresses and descriptions are written below, are desirous of being formed into a company in pursuance of this Memorandum of Association, and we respectively agree to take the number of shares in the capital of the company set out opposite our respective names.

Table A

- is a standard set of articles of associations provided by the companies Act 1948 to simplify company formation
- Companies often use Table A as their base and only modify it where necessary

Directors

- The one who runs the company
- has duty towards shareholders and company employees
- must devote himself to the companies benefits and avoid personal interest
- is liable for any wrong decision

Capital

- needed to make the product/service and live while you are making it

Setting up a company

1. Form a Group
   - Gather indivisuals who agree to contribute funds to establish the company
2. Register the Company
   - register the organization as a limited company in accordance with the law
3. Consider Professional Help (optional)
   - hire an accountant and legal advisor if needed
4. Alternative Option
   - Purchase a ready made company from an agent and customise as required

Factors involving capital

- when developing a large amount is needed up front as there will be no revenue during this period.
- Cash will be required for
  - salaries for founders and staff
  - rent, utilities, office expenses → eg stationery, travel
  - cost of advertising and marketing
  - miscellaneous expenses → travelling expenses
  - Interest on borrowed funds

The Business Plan

- to start a bussiness plan
  1. Plan
     - define your bussiness idea, goals, benefits
  2. Set Targets
     - establish what you aim to achive
  3. Create a Business Plan document
     - document your plans to represent to funders demonstrating they are well thoughout and realistic

Business Plan document

- It should contain
  - Company Description
    - details on what the company will do
    - its technical feasibility
    - the expertise of the founders
  - Market Analysis
    - info about the target market
    - its estimate size
    - assessment of the competition
  - Prediction of financial performances
    - budgets
    - cash flow predictions
    - projected balance sheets
    - profit and loss statements

Sources of finances

1. Grants

- funds given to a company with the following conditions
  - The company must use the grant as specified
  - Grant does not need to be repaid
  - Grants are usually provided by goverment unions or charities
- Grants typically
  - intend to assist with capital invesment → eg premises or equipment
  - subject to a no. of conditions → needing to raise additional capital
  - covers only a portion of the capital invesment that the company proves it has made

2. Loans

- funds given to a company with the following conditions
  - The company must pay interest which may be fixed or variable
  - The loan is set for a fixed period
  - The company must repay the loan
  - If the company liquidates the lender can recover the loan from company's assets
  - security is usually required for a loan in most cases

3. Gearing

- is the relationship b/w a company's loan capital and equity capital
- It shows how much of the company's financing comes from debt vs equity

4. Equity capital

- Equity capital (invested)
  - money paid to a company in exchange for ownership shares
- Business Angles → venture capitalist
  - are wealthy indivisuals who provide equity capital to start-ups and small companies that are seeking to grow rapidly

Anual Report

- Provides details about the company's activities and performance over the past years
- It consists of 3 items
  1. Balance sheet
  2. Profit and loss account
  3. Cash flow statement

  } Financial Statements → provides a picture of the overall financial health of the business
- when a limited company is liquidated, shareholders lose the amount they invested
- to monitor company performance Anual reports are required

1. Balance sheet

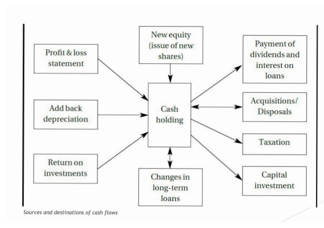
- financial statement in the anual report which shows
  - what the company owns → its assets
  - what it owes → its liabilities

2. Profit and loss Account

- shows
  - how much money has been received
  - how much has been spent in a given period (usually the accounting financial year)
- In case of non-profit-making organization it is called income and expenditure account

3. Cash flow statement

- the link that ties the balance sheet and profit and loss account to the capital expenditure



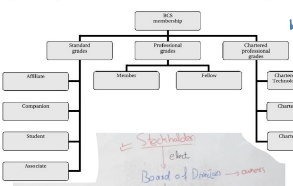
Sources and destinations of cash flows

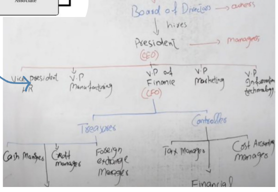
The overall picture

- To asses a companys financial state, you need to consider
  - balance sheet
  - profit and loss account
  - cash and flow statement

  together
- each statement should not be viewed in isolation as you need them all to be able to understand the financial state

Word/phrase	Meaning
code of conduct	a set of rules governing the behaviour of a group or organisation (e.g. computer professionals)
computer ethics	moral principles governing the design, building, implementation and use of computer systems
copyright	the legal right to intellectual property
freeware	copyrighted software that is available free of charge
intellectual property	something unique that has been physically created by someone (an idea that hasn't been implemented is not intellectual property)
licence	a permit to use/distribute/copy/adapt software
open source software	software that can be freely copied, distributed and adapted
shareware	copyrighted software that is available free of charge for a limited period, after which a licence must be obtained





BCS Membership Grades

1. The standard grades:
   - Affiliate: open to anyone with an interest
   - Companion: members of other professional bodies with at least five years' work experience related to information systems
   - Student: open to those following an approved course of study leading to a qualification recognized for admission to Associate or Professional membership of the Society.
   - Associate: Associate membership is open to anyone who has any of the following:
     - more than one but less than five years of IT work experience;
     - a Higher National Certificate in an IT-related field;
     - a non-accredited degree with a significant IT content.
2. The professional grades
   - Membership: In order to qualify for membership in the professional grades, you must have one of the following:
     - the BCS Professional Graduate Diploma including the project;
     - an honours degree that gives you full exemption from the BCS examinations;
     - five years of relevant professional IT work experience;
     - some combination of academic qualifications and professional IT work experience that is judged to be equivalent to one of the above.
   - Fellow: Fellow is the most senior professional grade. It is open to applicants who can demonstrate a minimum of five years IT practitioner experience, senior post and authority in that field.
3. The chartered professional grades
   - Member or Fellow holding the BCS Professional Graduate Diploma including the project or an honors degree that gives you full exemption from the BCS examinations and you must have five years of relevant professional IT work experience.
   - The Professional Advice Register
     - It maintains a register recording their members in relevant areas

- The development of Professional Bodies in Computing
  - 1946: The Institute of Electrical and Electronic Engineers (IEEE): A professional engineering society basically USA based but with members and activities spread worldwide. This was the IEEE Computer Society (IEEE-CS). It has over 100,000 members.
  - 1947: Association for Computing Machinery (ACM): USA based but have members and activites in many countries. It has over 75,000 members
  - 1957: British Computer Society (BCS): UK based society. In mid 1960's it became a qualification awarding society. Then in 2009 it named itself as BCS- The Chartered Institute of IT.
  - 1871: Institution of Electrical Engineers (IEE): It has over 130,000 members.
  - 1961: Italian Association for Informatics and Automatic Computing
  - 1965: The Computer Society of India
  - 1966: Australian Computer Society
  - 1967: the Singapore Computer Society and the Irish Computer Society
  - 1969: German Informatics Society
  - 1976: The Computer Society of Sri Lanka
  - 1998: The Computer Society of Maritius

4. Private vs. Public Limited Companies:

• Private Limited Company: A company whose shares are not available to the general public and is not listed on the stock exchange. (i.e TCS, engro)

• Public Limited Company (PLC): A company whose shares can be bought by the public and is listed on the stock exchange. Going public allows the company to raise funds but also requires them to follow strict rules and be more transparent. (i.e SSGC, NHA)

5. Advantages and Disadvantages of Going Public:

Pros of Going Public:

• Increases brand recognition and customer trust.
• Provides access to new funding by offering shares to the public.
• Easier access to bank loans, often at lower interest rates.
• Less personal financial responsibility for company debts.

Cons of Going Public:

• Stricter regulations and requirements, such as having two directors and holding AGMs.
• Running a public company is more expensive and time-consuming.
• Financial information is public and subject to media attention, positive or negative.
• Shareholders' interests and stock value fluctuations can impact company decisions.

Example Business Plan: A comprehensive business plan includes sections like an executive summary, business overview, market analysis, products and services, marketing strategies, operations plan, management team, financial plan, and appendix.

Executive Summary: The executive summary provides an overview of the entire business plan, written after completing the plan.

Business Overview: This section details the company's name, location, history, and future goals.

Market Analysis: It analyzes the industry, target market, competitors, and growth opportunities relevant to the business.

Products and Services: Describes specific services and products offered, focusing on client needs and relevant offerings.

Sales and Marketing Strategies: Outlines strategies for attracting and retaining clients, including unique selling propositions and customer retention techniques.

Operations Plan: Details staffing requirements, operational processes, and necessary equipment for running the business.

Management Team: Provides an overview of the management team, including their qualifications, roles, and organizational structure.

Financial Plan: Summarizes financial projections, including profit and loss statements, cash flow, balance sheets, and financing needs.

Appendix: Includes additional supporting information such as market research and legal documentation.

Business Plans Are Not Predictions: A business plan should not be viewed as a prediction of success, but as a scenario illustrating the potential for success.

Code of Conduct:

• Be honest and ethical in all your dealings with others.
• Treat everyone with respect, regardless of their race, ethnicity, gender, sexual orientation, religion, or disability.
• Be inclusive and welcoming to people from all backgrounds.
• Be fair and just in your treatment of others.
• Be accountable for your actions and decisions.
• Be committed to continuous learning and improvement.
• Be a team player and support your colleagues.
• Be innovative and creative in your work.
• Be passionate about your work and the organization's mission.
• Be committed to excellence in all that you do.

Be a good corporate citizen and contribute to the community.

• Be mindful of your environmental impact and strive to reduce your carbon footprint.
• Be supportive of diversity and inclusion in the workplace.
• Be respectful of all cultures and religions.
• Be honest and transparent in your dealings with customers and partners.
• Be committed to providing excellent customer service.
• Be fair and honest in your pricing practices.
• Be committed to protecting the privacy of your customers and employees.
• Be committed to complying with all applicable laws and regulations.
• Be committed to continuous improvement of the organization's products and services.
• Be committed to the long-term success of the organization.
• Promote a culture of ethical decision-making and ethical behavior.
• Provide training on ethics and diversity to all employees.
• Create a system for reporting and investigating ethical violations.
• Hold employees accountable for their ethical behavior.

values

Employer: Training and workshops for their professional and social development, Establishing culture of listening, accepting diversity, delegating ownership, making inclusive and open
communication, appreciation and reward, recognition, health and safety, security Rehabilitation program for disable people.

Employee: in case that employer would have their values then the right employees will become part of the team. Otherwise there will be a problem of incompatibility and will arise in conflicts in future.
Example : Google set their value for instance democratic web, don't be evil

Sole Trader

Definition[?] A sole trader is an individual who operates their own business independently. No legal formalities are required to become a sole trader; simply starting a business qualifies you.
Tax Registration: If your business income is substantial, you may need to register with customs and tax authorities, but this is not required to establish your status as a sole trader.
Key Points to Remember
Individual Ownership[?] Sole traders have full control and ownership of the business.
Liability[?] They are personally liable for all business debts.
Simplicity[?] The setup is straightforward with minimal regulatory requirements.
Risk: Personal assets are on risks.

Partnership

Definition[?] A partnership is formed when a group of people conducts a business with the aim of making profits, and the business is not structured as a limited company.
Key Features
Articles of Partnership[?] A formal agreement outlining the terms and conditions of the partnership.
Liquidity[?] Partnerships can be difficult to liquidate, meaning selling or dissolving the business can be complicated.
Nontransferable[?] Ownership interests in a partnership typically cannot be transferred without the consent of other partners.
Dissolution[?] The partnership agreement is automatically dissolved if one of the partners passes away.
Challenges:
Share Rate[?] Disagreements may arise regarding the distribution of profits or responsibilities among partners.

Limited Companies

A limited liability company operates under three fundamental principles:
[?][?] Corporate Identity[?] The company is a legal entity separate from its owners and employees.
[?][?] Share Ownership[?] Ownership is divided into shares, which can be individually bought and sold. Owners of these shares are called shareholders or members.
[?][?] Limited Liability[?] Shareholders are not personally responsible for the company's debts. Their maximum loss is limited to the amount they paid for their shares.
Limited companies provide a separate legal identity and protect shareholders from personal liability for company debts. Ownership is through shares, promoting individual investment and transferability.

Cooperatives

A cooperative is a member-owned business organization (that requires at least five shareholders) each having equal voting rights regardless of their level of investment or involvement. Every shareholder is expected to actively participate in the cooperative's operations.
Key Features
Revenue Contribution[?] Cooperatives generate approximately 90% of revenue in many economies. Legal Entity[?] Recognized as a separate legal entity.
Legal Powers[?] Can sue and be sued in their own name.
Taxation[?] Often subject to double taxation on income.
Transparency[?] Generally, there is no secrecy regarding financial operations.
Advantages
Cost-Effective[?] Typically inexpensive to register.
Democratic Control[?] All members have equal votes at meetings, promoting fairness.
Youth Inclusion[?] Members under 18 can join but cannot vote or hold office.
Limited Liability[?] Members are not personally liable for debts unless caused by reckless actions.
Member Ownership[?] Controlled by its members, not external investors.
Disadvantages
Attraction Issues[?] Hard to draw in members primarily seeking financial returns, as cooperatives focus on services.
Minimum Requirement[?] At least five members are needed to form a cooperative.
Limited Profit Distribution[?] Surplus profits may be distributed minimally, and some cooperatives maynot distribute profits at all.
Equal Voting Rights[?] All members have one vote, regardless of their investment level.
Active Participation[?] Members must be involved in operations.
Education Needs[?] Ongoing education for members is necessary for effective participation.

LLC vs Corporations

LLCs provide flexibility in management and taxation, allowing profits to pass through to owners' personal tax returns, avoiding double taxation. They also offer limited liability protection, meaning personal assets are generally protected from business debts.
Corporations, on the other hand, are more formal entities, requiring adherence to specific regulations and structure (like a board of directors). They also face double taxation: the corporation pays taxes on profits, and shareholders pay taxes on dividends.
Key Differences: [?][?]
Structure:
Corporation: A formal entity with a defined structure, including a board of directors and shareholders. It requires adherence to corporate formalities like annual meetings and record-keeping.
LLC[?] More flexible and less formal, allowing for various management structures (member- managed or manager-managed). Fewer regulatory requirements.
[?][?] **Taxation**:
Corporation: Subject to double taxation; the corporation pays taxes on its profits, and shareholders pay taxes on dividends.
LLC[?] Generally enjoys pass-through taxation, meaning profits are taxed only at the owner's personal income tax rate, avoiding double taxation.
[?][?] **Management**:
Corporation: Managed by a board of directors; decisions are made through formal voting processes.
LLC[?] Managed by its members or appointed managers, allowing for more straightforward decision- making.
[?][?] **Ownership**:
Corporation: Ownership can be transferred easily through the sale of stock; it can have anunlimited number of shareholders.
LLC[?] Ownership is less flexible; transferring ownership may require approval from other members.

2. Types of Rights:
Rights are often categorized into negative rights and positive rights. Understanding this distinction is important in both personal and professional settings.
• **Negative Rights**: These rights require others to refrain from doing something harmful or restrictive. For example, people have the right not to be killed, robbed, or harmed. Negative rights do not require others to take any specific action to protect you; they only need to avoid causing harm.
o Examples of Negative Rights:
- Right to Life: People should not kill you.
- Right to Privacy: Your personal information should not be exposed.
- Freedom of Speech: You should be able to express your opinions without interference.
- Freedom of Religion: You are free to follow any religion without being forced to change it.

• **Positive Rights**: These rights require others to actively help you or take action to support your needs. For example, if you have the right to live, then others might need to provide you with food, shelter, or security to protect that right.
o Examples of Positive Rights:
- Right to Education: The government or society must provide educational resources.
- Right to Healthcare: Society or healthcare systems should provide medical care when needed.

3. **Combining Negative and Positive Rights**:
Most rights require both restraint from harmful actions (negative rights) and active protection (positive rights). For example, the right to life not only requires others to avoid killing you (negative right) but may also require someone to protect you or save your life in an emergency (positive right).
4. Further Classification of Rights:
Rights are also categorized into Legal Rights and Moral Rights:
Legal Rights: These are rights that are protected by law. The government enforces these rights, and there are punishments for violating them.
o Example: The right to free speech is protected by law in many countries, meaning if someone tries to stop you from speaking, they could face legal consequences.
Moral Rights: These are not necessarily written into law but are based on customs, traditions, or ethical beliefs about what is right and wrong. Violating moral rights may not result in legal punishment but can lead to social disapproval or feelings of guilt.
o Example: Helping elderly people or respecting others' opinions might not be enforced by law, but violating these norms may be considered immoral.
5. Moral vs. Legal Distinction:
• Moral rights are based on personal or societal values of good and bad. They guide behavior but do not have legal consequences.
• Legal rights are enforced by law, with penalties for violations. If someone breaks a legal right, they might face fines, jail time, or other forms of punishment.
Example:
• Moral: You shouldn't throw litter on the ground because it's wrong and harms the environment.
• Legal: If there's a law against littering, you could be fined for throwing trash on the street.

2. **Fixed vs. Current Assets:**
• Assets are resources owned by the company that are expected to bring future benefits.
o Fixed Assets: These are long-term assets like buildings, machinery, or land, which the company plans to use for more than a year.
o Current Assets: These are short-term assets like cash or inventory that can be quickly turned into money, usually within a year.
3. Tangible vs. Intangible Assets:
• Tangible Assets: Physical assets like buildings, vehicles, or equipment that you can touch.
• Intangible Assets: Non-physical assets like trademarks, patents, or company reputation (goodwill). Sometimes, intangible assets are more valuable than tangible ones, especially for companies that deal in technology or software.

4. Current Liabilities vs. Fixed Liabilities:
• Current Liabilities: Debts that need to be paid within one year, such as bills or short-term loans.
• Fixed Liabilities (Long-term Liabilities): Debts that are not due for at least one year, like long-term loans or bonds. These are often used to finance long-term investments like buying property.

Profit and Loss Account (P&L):
1. What is a Profit and Loss Account?
• Also called an Income Statement, the P&L summarizes a company's revenues, costs, and expenses over a specific time period (usually a month, quarter, or year). It shows whether the company made a profit or a loss.
2. Why is the Profit and Loss Account Important?
• It helps businesses see how well they are performing, which areas are making money, and which areas are losing money. Investors also look at this statement to decide whether to invest in the company. Companies are often required by law to produce and submit regular financial statements, including the P&L account, for regulatory and tax purposes. Helps in creating budgets.
3. Example:
• Imagine a bookstore with revenue from book sales, expenses for rent and staff, and other costs. The P&L account would list all these revenues and expenses and show whether the bookstore made a profit or not for the year.
An income and expenditure account summarizes the surplus or deficit of a non-profit organization by matching incomes and expenses over a specific period, serving as its final account, in contrast to a trading and profit and loss account for profit-oriented businesses.
Cash Flow Statement:
1. What is a Cash Flow Statement?
• A Cash Flow Statement shows how cash moves in and out of the business over a period of time. It explains where the company got its money from and how it was spent. This statement ties together the balance sheet and profit and loss account by showing the actual cash situation.
2. Why is the Cash Flow Statement Important?
• It helps businesses and investors understand whether the company has enough cash to run its operations and pay its bills. Even profitable businesses can run into trouble if they don't have enough cash on hand.
3. Types of Cash Flows:
• Operating Activities: Cash earned from the company's core business activities, like selling products or services.
• Investing Activities: Cash used for buying or selling long-term assets like property or equipment.
• Financing Activities: Cash received or paid out for loans or investments, like bank loans or payments to investors.

Assets = liabilities + Owners Equity

Vertical Format of Balance Sheet
Imaginary Company Name
Balance Sheet as at..

Particulars	Note	Amt
Assets (180 000, 20000, 160 000)		
Non-Current Assets:		
Property, Plant & Equipment		X
Intangible Assets		X
Investments		X
Other Non-Current Assets		X
Current Assets:		
Inventories (Closing)		X
Investments		X
Trade Receivables		X
Cash And Cash Equivalents		X
Other Current Assets (Cash in Bank/hand)		X
Total Assets		X
Equity And Liabilities		
Equity		
Share Capital		X
Retained Earnings		X
Other Equity		X
Non-Current Liabilities: → More than 1 years		
Long-Term Borrowings		X
Long-Term Provisions		X
Deferred Tax Liabilities (Net)		X
Other Non-Current Liabilities		X
Current Liabilities: → less than 1 yeas		
Short-Term Borrowings		X
Trade Payables		X
Other Current Liabilities		X
Short-Term Provisions		X
Total Equity And Liabilities		X

Asset = Capital + liability.
A = C + L
Non-Current Asset
Value for the year - Depreciation

→ BALANCE SHEET

Cash Flow from Operating Activities

I. Net profit before taxation and extraordinary items*		XXXX
II. Adjustments related to Non-cash and Non-operating Items		
Add: Items to be added:		
Depreciation on Fixed Assets	XXXX	
Interest on Borrowings	XXXX	
Preliminary Expenses/Underwriting Commission/Discount on Issue of Debentures/Shares Written Off	XXXX	
Goodwill/Patents/Trade Marks/Copyright amortised	XXXX	
Loss on Sale of Machinery/Land and Building/Investments, etc.	XXXX	
Premium payable on redemption of Preference Shares/Debentures	XXXX	XXXX
Less: Items to be deducted:		
Interest Income/Other Income	XXXX	
Dividend Income	XXXX	
Discount on Redemption of Preference Shares/Debentures	XXXX	
Profit on Sale of Machinery/Land and Building/Investments, etc.	XXXX	(XXXX)
Operating Profit before Working Capital Changes		**XXXX**
III. Adjustments related to change in Current Assets and Current Liabilities		
Add: Decrease in Current Assets	XXXX	
Increase in Current Liabilities	XXXX	XXXX
Less: Increase in Current Assets	XXXX	
Decrease in Current Liabilities	XXXX	(XXXX)
Cash generated from Operations		**XXXX**
Less: Income taxes paid (Net of Refund)		(XXXX)
Cash before Extraordinary Items		**XXXX**
Less: Extraordinary Items		(XXXX)
Net Cash Inflow/Outflow from Operating Activities		**XXXX**

CASH FLOW STATEMENT

Statement of Cash Flows
For the Year Ended June 30, 19x1
Increase (Decrease) in Cash and Cash Equivalent
(amounts in thousands)

Cash flows from operating activities:		
Net income		$ 41
Add (subtract) items that affect net income and cash flow differently		
+ Depreciation	$ 18	
− Gain on sale of plant assets	(8)	
− Increase in account receivable	(13)	
− Increase in interest receivable	(2)	
+ Decrease in inventory / − Increase in Inventory	3	
− Increase in prepaid expenses	(1)	
+ Increase in account payable / − Dec in Acc pay	34	
− Decrease in salary and wage payable	(2)	
− Decrease in accrued liabilities / + In in Acc liab	(2)	
Net cash inflow from operating activities		68
Cash flows from investing activities:		
Acquisition of plant assets (+Initial funding + loan)	$ (306)	
Loan to another company	(11)	
Proceeds from sale of plant assets	62	
Net cash flows from investing activities		(255)
Cash flows from financing activities:		
Proceeds from issuance of common stock	$ 1 01	
Proceed from issuance of long-term debt	94	
Payment of long-term debt	(11)	
Payment of dividends	(17)	
Net cash flows from financing activities		167
Net decrease in cash		(20)
Cash balance, December 31, 19x1		42
Cash balance, December 31, 19x2		$ 22

INCOME STATEMENT OR P & L

SSS Company
Vertical Income Statement
For the year ending Dec 31, 2023

Income		
Sales	XXX	
Less:		
Sales Returns	(XXX)	
Net Sales		XXX
Cost of Goods Sold (COGS)		
Operating Stock (opening stock/inventory)	XXX	
Add:		
Purchases	XXX	
Wages	XXX	
Carriage Inward	XXX	
Direct Expenses	XXX	
Less:		
Closing Stock (inventory)	(XXX)	
Net Cost of Goods Sold (COGS)		XXX
Gross Profit Net Sales - Cost of Goods Sold		XXX
Operating Expense		
Add:		
Administrative Expenses (Electricity, Depreciation, salary)	XXX	
Finance Expenses (loan ka interest exp)	XXX	
Selling Expenses	XXX	
Total Operating Expense		XXX
Operating Profit (Gross Profit - Operating Expenses)	XXX	
Add: Non-operating Income	XXX	
Less: Non-operating Expenses	(XXX)	
Net Profit Before Tax	**XXX**	
Less: Tax (Charged on Net profit Before Tax)	(XXX)	
Net Profit After Tax		XXX

→ Income Statement
Net Sales - COGS = Gross Profit
Gross Profit - Operating = Profit after operating (Profit before taxes)

Balance sheet

- ASSETS
- LIABILITIES
- Stockholders Equity
- Networth

CASH FLOW

- Net income (do not repeat these)
- CASH Flow from Operating Activities
- CASH Flow from Investing Activities
- CASH Flow from Financing Activities
- Networth

Income Statement OR P&L

- Revenue
- Expense
- Networth

Q1)

A new e-commerce company is preparing for its first-year financial review. The company has $750,000 in total revenue and $550,000 in expenses, including salaries ($250,000) and operational costs ($200,000). Initial funding was $300,000, with $75,000 in cash reserves, $120,000 in current liabilities, $180,000 in inventory, and a $60,000 long-term loan. The company has $70,000 in accounts receivable and $25,000 in other liabilities. Draft a sample balance sheet, profit and loss account, and cash flow statement for the first year.

Total revenue	750,000
Expenses	550,000
↳ Salaries	250,000
↳ Operational cost	200,000
Initial funding	300,000
↳ cash reserves	75,000
Current liabilities	120,000
Inventory	180,000
long term loan	60,000
Accounts Receivable	70,000
Other liabilities	25,000

BALANCE SHEET

ASSETS		
Inventory	180,000	
Account receivable	70,000	
Cash reserves	75,000	
		325,000
LIABILITIES		
Curr liabilities	120,000	
Other	25,000	
long term loan	60,000	
		205,000

Networth: 120,000

CASH FLOW

Net income		300,000
CASH Flow from Operating Activities		
Curr liabilities	120,000	
Inventory	(180,000)	(means -ve)
Accounts Receivable	(70,000)	
Other liabilities	25,000	
		(105,000)
CASH Flow from Investing Activities		
long term loan	60,000	
Initial funding	300,000	
		360,000
CASH Flow from Financing Activities		

Networth: (105,000) + 360,000
= 155,000

Income Statement

Revenue		
Total Revenue	750,000	
		750,000
Expenses		
Salaries	(250,000)	
Operational costs	(200,000)	
		(450,000)

Networth: 750,000 + (450,000) (-ve)
= 300,000

MANAGEMENT ACCOUNTING

ishma hafeez notes

COST OF LABOUR

► The cost of employing someone is more than just the cost of their salary.
► In most countries, employers are required to pay a tax for every employee. This tax usually goes by a name such as employers' national insurance contribution (in the UK) or social security contribution; it is proportional to the employee's salary.
► In some countries, this contribution may be as large as 60 per cent of salary, while in others it is very much smaller.

Payroll

The total cost of employing a person, that is, the salary plus employers' social security contributions plus any other costs associated directly with the employee, is sometimes known as the employee's payroll cost or direct cost.
Example :
►Consider a technician who is employed to assemble the computers and suppose that he is paid an annual salary of £20,000. His payroll costs are £22,000.
► The direct cost of the technician is £22,000 per year so the direct cost of an hour of their time is £22000/1505 = £14.62.

OVERHEADS

► Costs that cannot be directly associated with a particular product are known as overheads.
► There are many costs that we have ignored. Even if our technician works as a sole trader, with no assistance, there will be other costs he has to pay for a computer costs £200 and it takes 10 hours of a technician's time to assemble the computer, install the software and configure it, then the cost of constructing the finished product is £200 + 10 × £14.62 = £346.20.

BUDGETING

► A budget is a financial plan showing the expected income and expenditure for an organization over a specific period, typically one year,

► For many reasons, particularly with taxation and social security, owners should treat themselves as employees and pay themselves a salary, rather than attempt to live on the company's profits. This accounts for the item labeled 'Owner's payroll costs'.
► The services of an accountant will be necessary to help prepare the annual accounts and possibly to advise from time to time. The advice lawyer may also be necessary from time to time. These items are covered under the heading 'Professional fees'.
► Finally, employers are legally required to carry insurance to cover any claim against them for injuries suffered by employees during their employment; other insurance, against theft from the company's premises for example, may also be necessary. This explains the heading 'Insurance'.

CASH FLOW FORECAST

A company may be very profitable but unable to pay its bills. For that reason, it may be forced into receivership. This apparent paradox typically arises because bills have to be met, in particular staff have to be paid, before the income they generate is received. To avoid this difficulty businesses, need to prepare cash flow forecasts, that is, estimates of the amount of money that will flow into and out of the company each month.
companies normally try to forecast twelve months.

following methods calculate the cost of labor/ hour:

1. Direct Cost Method:
Calculate the hourly labor cost by considering the salary and employer's social security contribution only.
2. Fixed Overhead Allocation Method:
Calculate the hourly labor cost by distributing the total overhead equally across all units produced.
3. Overhead Proportional to Hours of Labor Method:
Allocate the overhead proportionally to the number of hours worked by the technician. Then, calculate the total cost of labor per hour.

1. Direct cost method

hourly labour cost = $\frac{\text{total T cost}}{\text{T hours}}$

2. Fixed allocation overhead method

overhead per technician = $\frac{\text{overhead}}{\text{no. of T}}$

total labour cost = total T cost + overhead per T

hourly labour cost = $\frac{\text{total labour cost}}{\text{T hours}}$

3. Overhead ∝ hours of labour

overhead /h / technician = $\frac{\text{overhead}}{\text{T hours} \times \text{no. of T}}$

hourly labour cost = direct cost + overhead /h/T

4. Overhead ∝ total cost

Total cost for all T = total T cost × no. of T
Total cost = total cost for all T + overhead
∝ overhead in total cost = $\frac{\text{overhead}}{\text{total cost}}$
Total cost /T = total T cost (1 + $\frac{\text{total cost /T}}{\text{T hours}}$)

Example

Technicians annual salary = 25,000
Employers social security contribution = 12% → 3,000
Total technician cost = 28,000
Technician work hours = 1,500 h/y
Overhead = 70,500
Total technicians = 3

1. Direct cost method

hourly labour cost = $\frac{28{,}000}{1{,}500}$ = 18.67/h

2. Fixed allocation overhead method

overhead per technician = $\frac{70{,}500}{3}$ = 23,500

total labour cost = 28,000 + 23,500 = 51,500

hourly labour cost = $\frac{51{,}500}{1{,}500}$ = 34.33/h

3. Overhead ∝ hours of labour

overhead /h / technician = $\frac{70{,}500}{1{,}500 \times 3}$ = 15.67/h

hourly labour cost = 18.67 + 15.67 = 34.34 /h

4. Overhead ∝ total cost

Total cost for all T = 28,000 × 3 = 84,000
Total cost = 84,000 + 70,500 = 154,500
∝ overhead in total cost = $\frac{70{,}500}{154{,}500}$ = 0.4564
Total cost /T = 28,000 (1 + 0.4564) = 40,779
hourly labour cost = $\frac{40{,}779}{1{,}500}$ = 27.19 /h

Cost of labor

TABLE 7.1 *Calculation of the number of revenue-earning hours in a year*

Total number of weekdays (1)	260
Public holidays (2)	10
Annual leave (3)	20
Sick leave (4)	5
Unproductive time (5)	10
Total non-revenue-earning time (2) + (3) + (4) + (5) = (6)	45
Total number of revenue earning days (1) – (5) = (7)	215
Total number of hours available (7) × 7	1505

You have been hired to calculate the total labor cost for technicians assembling computers under two plans. The technicians are paid an annual salary of **£30,000**, and the employer's social security contribution is **10%** of the salary. Each technician works **1,600 hours** per year. The company has a total overhead of **£90,000**, and 4 technicians are working across both plans.

Using the following methods, calculate the cost of labor per hour for **both plans**:

1. **Direct Cost Method**
   Calculate the hourly labor cost by considering only the salary and employer's social security contribution.
2. **Fixed Overhead Allocation Method**
   Calculate the hourly labor cost by distributing the total overhead equally across both plans and all workers.
3. **Overhead Proportional to Hours of Labor Method**
   Allocate the overhead proportionally to the number of hours worked by each technician. Then, calculate the total cost of labor per hour.

Technicians annual salary: 30,000

Employees social security contribution: 10% of salary = 3000

Total cost of Technician: 30,000 + 3000 = 33,000

Technician works hours: 1,600 hr/year

1) Hourly Labour cost = $\frac{33,000}{1,600}$ = 20.63/hr

2) Overhead: 90,000 → Shared among 3 Technicians

Overhead Per Technician: $\frac{90,000}{4}$ = 22,500

Total labour cost: direct cost + overhead

33,000 + 22,500 = 55,500

Hourly Labour cost = $\frac{51,500}{1,600}$ = 34.69/hr

3) Overhead Per hour: $\frac{90,000}{1,600 \times 4}$ = 14.06/hr

Total cost Per hour = Direct cost/hr + Overhead/hr

= 20.63 + 14.06 = 34.69/hr

1. Direct cost method

hourly labour cost = $\frac{\text{total T cost}}{\text{T hours}}$

2. Fixed allocation overhead method

overhead per technician = $\frac{\text{overhead}}{\text{no. of T}}$

total labour cost = total T cost + overhead per T

hourly labour cost = $\frac{\text{total labour cost}}{\text{T hours}}$

3. Overhead ∝ hours of labour

overhead /h / technician = $\frac{\text{overhead}}{\text{T hours} \times \text{no. of T}}$

hourly labour cost = direct cost + overhead /h/T

4. Overhead ∝ total cost

Total cost for all T = total T cost x no. of T

Total cost = total cost for all T + overhead

∝ overhead in total cost = $\frac{\text{overhead}}{\text{total cost}}$

Total cost/T = total T cost (1 +)

hourly labour cost = $\frac{\text{total cost /T}}{\text{T hours}}$

You have been hired to calculate the total labor cost for a technician who assembles computers. The technician's annual salary is £25,000, and the employer's social security contribution is 12% of the salary. The technician works 1,500 hours per year. Additionally, the company has overheads of £70,500, and three technicians are working in the company.

Using the following methods, calculate the cost of labor per hour:

Technihans annual salary = 25,000

Employees social security contribution = 12% → 3,000

Total technihian cost = 28,000

Technihan work hours = 1,500 h/y

overhead = 70,500

Total technihians = 3

1. Direct cost method

hourly labour cost = $\frac{28,000}{1500} = 18.67/h$

2. Fixed allocation overhead method

overhead per technihan = $\frac{70,500}{3} = 23,500$

total labour cost = 28,000 + 23,500 = 51,500

hourly labour cost = $\frac{51,500}{1500} = 34.33/h$

3. Overhead ∝ hours of labour

overhead /h / technihan = $\frac{70,500}{1,500 \times 3} = 15.67/h$

hourly labour cost = 18.67 + 15.67 = 34.34 /h

4. Overhead ∝ total cost

Total cost for all T = 28,000 x 3 = 84,000

Total cost = 84,000 + 70,500 = 154,500

∝ overhead in total cost = $\frac{70,500}{154,500} = 0.4564$

Total cost/T = 28,000 x 1.4564 = 40,779

hourly rate = $\frac{40,779}{1,500} = 27.19/h$

BCS-7B

Consider a software house team based on three developers: a UI/UX developer, a Web developer, and a deployment engineer (used to deploy the product) working on their product and providing maintenance and customization services for their product. They are withdrawing the same fixed **$50,000** annual salary with **1600** working hrs.

Given below is a chart of Services against which its development hrs and costs are mentioned.

Software Services	Cost of Service	Development hours	Expected Sales
UI/UX	$200	5 hrs	25
Web	$300	5 hrs	75
Deployment	$400	8 hrs	50

The expected forecast for the upcoming year is **150 product services** they want to grab with an overhead of **$60,000**. This overhead will be distributed to all service charges equally.

You are tasked to calculate the cost of labor in all possible ways.

per hour salary = $\frac{50000}{1600}$

per hour Salary = 31.25$

annual Salary = 50,000
working hours = 1600

upcoming services = 150
overhead = 60,000

① Fixed Cost

overhead = $\frac{60000}{150} = 400$

overhead, service cost, working hours, Per hour salary

UI/ux → 400 + 200 + 5 × 31.25 = 756.25

Web → 400 + 300 + 5 × 31.25 = 856.25

Deployment → 400 + 400 + 8 × 31.25 = 1050

② Overhead proportion w.r.t # of hours

$\frac{60000}{3 \times 1600} = 12.5$

Cost of an hour's labor = 31.25 + 12.5 = 43.75

d, service cost, working hours, cost of an hour labour

UI/ux → 200 + 5 × 43.75 = $418.75

Web → 300 + 5 × 43.75 = $518.75

Deployment → 400 + 8 × 43.75 = $750

③ Overhead proportion w.r.t total Cost

service cost, working hours, Per hour salary

UI/ux → 300 + 5 × 31.25 = 356.25

Web → 300 + 5 × 31.25 = 456.25

Deployment → 400 + 8 × 31.25 = 650

factor = $\frac{\text{overhead } 60000}{(25 \times 356.25) + (75 \times 456.25) + (50 \times 650)} = 0.79$

(25 × 356.25): expected sales; (75 × 456.25): total cost

factor = 0.79 + 1

factor = 1.79

Total cost, factor

UI/ux → 356.25 × 1.79 = 637.69

Web → 456.25 × 1.79 = 816.69

Deployment = 650 × 1.79 = 1163

	fixed	w.r.t labor	w.r.t hours
UI/ux	756	419	638
web	856	519	817
deploy	1050	750	1163

Problem 1: VSNKO Company

4 - techs → annual salary: $35000
social contri: 10%

1 - Manager → annual salary: $50000
social contri: 12%

Time: 1800 hours per year
Fixed overhead: $80000 (rent, utilities, admin)
Variable overhead: $50000
Overhead prop to Direct cost: $40000

Q) The company is planning its annual budget and wants to determine

a) Payroll cost for each employee

Tech

Social contri = 0.1 × 35000 = 3500
Cost per tech = 35000 + 3500 = 38500
Total techs payroll = 38500 × 4 = $154000

Manager

Social contri = 0.12 × 50000 = 6000
Cost per manager = 50000 + 6000 = $56000

b) Overhead ~~calculation~~ Allocation using Fixed, variable, Overhead prop to DC

Fixed Overhead

Total fixed overhead = $80000
Total hours worked by 4 techs = 4 × 1800 = 7200 hours
Fixed overhead per hour = $\frac{80000}{7200}$ = $11.11

Variable Overhead (Proportional to labour content)

Total variable overhead = $50000
= $\frac{50000}{7200}$ = $6.94

Overhead proportional to Direct Cost

Total Direct Overhead = $40000

Basic Model Material Cost = $400

↳ Direct labor Cost
= 10 × Techs hourly rate
= 10 × $\frac{38,500}{1800}$ = $213.9

Fixed Overhead = 10 × 11.11 = $111.1
Variable Overhead 10 × 6.94 = 69.4

Total Cost before Direct Cost Overhead
⇒ 213.9 + 400 + 111.1 + 69.4 = $794.4

Direct Cost Overhead (10% of Total Direct Cost)
⇒ 794.4 × 10% = $79.44

Total Cost for Basic Model
$794.4 + 79.44 = $873.84

Do the same for all models provided

c) Budget Decision

Compare the total cost for Basic Model to tell profitability.

Total product cost = DLC + MC + FOC + VOC + DO

INVESMENT APPRAISAL

Investment Appraisal

Investment appraisal is the analysis done to consider the profitability of an investment over the life of an asset alongside considerations of affordability and strategic fit. Less resources and a greater number of proposals lead company owners and investors to decide which proposal to drop which to pick.

Investing in.....

There is no single way of assessing and comparing the different proposals;
factors that must be taken into consideration include, for example:
► the extent to which the proposals are consistent with the company's long-term plans;
► the risk attached to the proposals;
► the availability of the necessary resources even if the money is available.

THE TIME VALUE OF MONEY

► The time value of money is a basic financial concept that holds that money in the present is worth more than the same sum of money to be received in the future.
► This is true because money that you have right now can be invested and earn a return, thus creating a larger amount of money in the future.
► The time value of money is sometimes referred to as the net present value (NPV) of money.

Discount Factors—Present Value of a Single Amount*

n/i	1%	2%	3%	4%	5%	6%	7%	8%	9%	10%
1	0.99010	0.98039	0.97087	0.96154	0.95238	0.94340	0.93458	0.92593	0.91743	0.90909
2	0.98030	0.96117	0.94260	0.92456	0.90703	0.89000	0.87344	0.85734	0.84168	0.82645
3	0.97059	0.94232	0.91514	0.88900	0.86384	0.83962	0.81630	0.79383	0.77218	0.75131
4	0.96098	0.92385	0.88849	0.85480	0.82270	0.79209	0.76290	0.73503	0.70843	0.68301
5	0.95147	0.90573	0.86261	0.82193	0.78353	0.74726	0.71299	0.68058	0.64993	0.62092
6	0.94205	0.88797	0.83748	0.79031	0.74622	0.70496	0.66634	0.63017	0.59627	0.56447
7	0.93272	0.87056	0.81309	0.75992	0.71068	0.66506	0.62275	0.58349	0.54703	0.51316
8	0.92348	0.85349	0.78941	0.73069	0.67684	0.62741	0.58201	0.54027	0.50187	0.46651
9	0.91434	0.83676	0.76642	0.70259	0.64461	0.59190	0.54393	0.50025	0.46043	0.42410
10	0.90529	0.82035	0.74409	0.67556	0.61391	0.55839	0.50835	0.46319	0.42241	0.38554

Calculating values from DCF table

► Discount factor for a discount rate of 8 per cent over a period of four years is 0.7350. This means that, if the discount rate is 8 per cent, the present value of a sum of £1,000 payable in four years time is
£1000 × 0.7350 = £735.

Example
A new van will cost £10,000. There will be annual costs of £500 for insurance and £150 for road tax. The cost of maintenance is estimated to be £200 in each of the first two years, £300 in year 3, £400 in year 4 and £500 in year 5.
At the end of the fifth year, it is expected that the van will be sold for around £2,000. The interest rate that the company pays on its borrowings is 10 percent.

If the van is hired(rented)
Van hire costs £35 per day and it hires a van for about 100 days a year. All the costs are subject to inflation, which is judged to be around 5 per cent over the period, but the resale value of the van is the cash figure expected at the time.

PITFALLS OF DCF

DCF analysis to assess a proposal for developing a software product, as the sources of uncertainty are very much greater. Although an NPV of £52,993 and an IRR of 23 per cent look attractive, but
we must consider that:
► most software projects take more effort than expected;
► most software doesn't work very well when it's first released;
► we may not manage to sell as many copies as we expected;
► there is a considerable risk that a competitor will launch a similar product before ours is ready.
The way is to carry out a series of DCF analyses with different estimates of the cash flows and the discount rate and see how the results change.

DCF(Discounted cash flow)

► One important criterion to choose which of the proposals will give the best return on the investment?
► The financial way of determining this, is to use the method known as discounted cash flow (DCF)

► Discounted cash flow (DCF) is a valuation method that estimates the value of an investment using its expected future cash flows. Analysts use DCF to determine the value of an investment today, based on projections of how much money that investment will generate in the future.
► Discounted cash flow can help investors who are considering whether to acquire a company or buy securities. Discounted cash flow analysis can also assist business owners and managers in making capital budgeting or operating expenditures decisions.

It is important to realize that DCF is a tool that is used for many different purposes, for example:
► by investors on the stock market to assess whether the share price of a company reflects accurately its financial prospects;
► to assess whether it is better to purchase capital equipment or to lease it;
► to decide which of several possible projects is the most financially appealing;
► to decide whether a proposed capital project will be worthwhile.

Purchasing vs Leasing

Suppose you want to get a car worth Rs.10,00,000/- and you have that amount. The car finance department offers you to lease the car providing you pay a down payment of 20% that is Rs.2,00,000/- and a monthly payment of Rs.20,000 for 5 years(60 months).
Thus,
(20,000 * 60) + 2,00,000 = 14,00,000
While if you purchase it, you must pay Rs. 10,00,000/-
Would you purchase the car or lease it on these terms?

TABLE 8.2 *DCF analysis of van purchase versus leasing*

	Year 0	Year 1	Year 2	Year 3	Year 4
Buying a van					
Van purchase/sale	(10000)				2000
Tax and insurance	(650)	(683)	(717)	(752)	(790)
Maintenance	(200)	(210)	(331)	(463)	(608)
Annual cash flow	(10850)	(893)	(1048)	(1215)	602
NPV of annual flow	(10850)	(812)	(866)	(914)	412
Total NPV	(13030)				
Continuing to rent					
Annual costs	(3500)	(3675)	(3859)	(4052)	(4254)
NPV of annual costs	(3500)	(3341)	(3189)	(3044)	(2906)
	(15980)				

Example
A new van will cost £10,000. There will be annual costs of £500 for insurance and £150 for road tax. The cost of maintenance is estimated to be £200 in each of the first two years, £300 in year 3, £400 in year 4 and £500 in year 5.
At the end of the fifth year, it is expected that the van will be sold for around £2,000. The interest rate that the company pays on its borrowings is 10 percent.

If the van is hired(rented)

Van hire costs £35 per day and it hires a van for about 100 days a year. All the costs are subject to inflation, which is judged to be around 5 per cent over the period, but the resale value of the van is the cash figure expected at the time.

Cost of capital

► Even if the company has the cash available to buy the van outright, there is still a cost because the company will lose the income it could have received by investing the money somewhere else, in a suitable interest-bearing account. Such a cost is known as an opportunity cost.
► Opportunity cost is the cost of the investment/opportunity you miss out on over the cost of the investment/opportunity you choose.
► If the company can pay cash for the van, this is the interest rate it would be appropriate to use in the DCF analysis.

Interest Rate

Suppose you put your Rs.10,00,000/- in the bank provided the bank gives you an interest of 10% per annum
Thus
(10/100) * 10,00,000 = 100,000 per annum

Discount factor

In general, if the interest rate is r (expressed as a fraction such as 0.03, not a percentage), then the present value of a sum of money X due in t years time is:

$$\frac{X}{(1+r)^t}$$

TABLE 8.3 *DCF analysis of a proposed software package development*

	Year 0	Year 1	Year 2	Year 3	Year 4
Development cost	105000	55125			
Maintenance			38588	40517	42543
Sales and marketing	10000	21000	22050	23153	24310
Number of sales		10	20	40	30
Revenue		50000	100000	200000	150000
Net cash flow	(115000)	(26125)	39363	136331	83147
Discount factor	1	0.9091	0.8264	0.7513	0.6830
Present value	(115000)	(23750)	32529	102425	56789
Cumulative present value	(115000)	(138750)	(106221)	(3796)	52993

Software House- Example

Consider a company that is assessing a proposal for the development of a software product. It is estimated that three people will be required for development in the first year and a further person and a half in the second year; suitable staff cost £35,000 per year, including the employer's pension and national insurance costs. The product will be released in the second year. After the second year, maintenance is expected to require one person, full-time. Sales and marketing costs are estimated to be £10,000 in the first year, rising to £20,000 for each of the next four years.
The product itself is a fairly high-value but specialized product. It is expected that about 100 copies will be sold over this period, at around £5,000 a copy.

Inflation

► Inflation in a financial context means the fall in the value of money over time.
► It is usually expressed as an annual percentage. Thus, for example, an inflation rate of 5 per cent means that in a year's time goods that today cost £100 will cost £105. In two years, they will cost £100 × 1.05 × 1.05 = £110.25.

Handling Inflation

► Initially estimate all costs in today's money.
► Then estimate an inflation rate of 5 per cent and adjusted
the cash flows for future years to take this into account.
► Used the 'monetary' rate of interest rather than the 'real' rate.
► In normal economic conditions this is the simplest way to carry out a DCF analysis.

Problem 2:

Imagine a company is evaluating whether to invest in new equipment or lease it. The equipment costs $50000 with 5 years of useful life. The company estimates it can generate cash flows of $15000 per year. The lease option requires a down payment of $10000 and annual payments of $9000. The interest rate on borrowed funds is 8%. and inflation rate is 3%.

- equipment cost: 50,000
  - with 5 years of useful life
- estimated cash flow generates: 15,000/y
- lease option
  - down payment: 10,000
  - annual payment 9,000
  - interest rate: 8%
  - inflation rate: 3%

Cashflow Analysis

Purchase: Total initial cost = $50000

Annual cashflow: $ 15000 per year for 5 year

Leasing

→ Down payment = $10000

→ Annual = 9000 × 5 = $45000

→ Total = 55,000

Present Value of Cashflows

DCF for purchase (8% for 5 years)

$$\frac{X}{(1+r)^t}$$

Year 1: $\frac{15000}{(1+0.08)^1} = 13888$

⋮

Year 5: $\frac{15000}{(1+0.08)^5} = 10,212$

Total PV = 13888 + 12857 + 11907 + 11026 + 10212 = $59893

Net PV = Total PV − Initial Cost

NPV = $59893 − 50000 = $9893

(net PV, cost)

Cashflow for Lease

Year 1: $\frac{9000}{(1+0.08)^1} = 8333$

⋮

Year 5: $\frac{9000}{(1+0.08)^5} = 6122$

TPV = 8333 + 7714 + 7146 + 6611 + 6122

= $35926

Total cost of Leasing = 35926 + 10000 = 45926

(TPV, down payment)

Impact of inflation (3% in 5 years)

inflated cashflow for year t = $15000 \times (1.03)^{t-1}$

Year 1: $5000 (no adjustment needed)

Year 2: 15000 × (1.03) = 15450

Year 5: 15000 × $(1.03)^4$ = 16882

Recalculate Inflate PV

Year 1: $\frac{15000}{1.08} = 13888$

Year 2: $\frac{15450}{(1.08)^2}$

⋮

⋮

= 13239

Year 5

Total PV (with inflation)

TPV = 13888 + 13239 + ... = 63307

NPV with inflation = 63307 − 50000 = 13307

(TPV, Cost)

→ NPV with inflation +ve indicate

Case 1: Positive NPV for Purchase (with Inflation) Greater Than Leasing Cost:
Conclusion: Purchasing the equipment is the better option as it provides a higher net present value compared to leasing. The company gains more financial benefit by investing in the equipment upfront.

Case 2: Positive NPV for Purchase (with Inflation) Less Than Leasing Cost:
Conclusion: Although purchasing results in a positive NPV, leasing might be more cost-effective if the leasing total cost is lower than the benefit gained from owning.

Case 3: NPV for Purchase is Negative:
Conclusion: If purchasing results in a negative NPV, it implies that the investment does not meet the desired return threshold. Leasing would likely be a better option in this scenario to avoid losses.

Case 4: Total Cost of Leasing is Lower Than Purchase but Provides Less Flexibility:
Conclusion: Leasing may be cheaper in terms of total cash outlay, but if the NPV of ownership is positive, purchasing may still be more advantageous for long-term asset control and potential residual value.

Case 5: Impact of Inflation Reduces NPV Significantly:
Conclusion: If inflation adjustments show that future cash flows lose significant value, leasing might be better as it can mitigate some risks associated with inflation eroding returns.

STRUCTURE AND MANAGEMENT OF ORGANIZATIONS

Organisation
Definition: An organization is a group of people working together in a formal way.
Explanation: The work that must be done is shared between these people and there are rules about who does what.
How the work is shared and how tasks and people are grouped together – the structure of the organization – will vary very much from organization to organization. It is surprising, however, that organizational structures have much more in common than might be expected.

1 Matrix management
► In a bureaucratic model every individual and every unit in the organization is responsible to only one manager. This is not realistic in the context of project-based, high-technology companies.
► MM believes that individuals may be responsible to more than one manager and requires rules that will enable possible conflicts to be resolved.
► For instance, a specialist in high-speed communications working for a systems integrator may well find themselves working on two or three projects simultaneously, as well as having a more general responsibility for maintaining the company's expertise in the area.
In the past 30 years or so the idea of matrix management has become fashionable as a way of addressing such situations. However, The results are not encouraging.

STRUCTURING PRINCIPLES
1 ► Structure by function
2 ► Structure by geography
3 ► Product line structure
4 ► Structure by market sector
5 ► Structure by technology
6 ► Operational structure

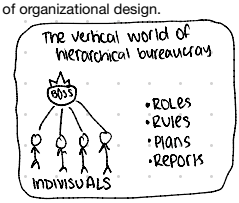
ORGANIZATIONAL MODELS
1 ► The bureaucratic model
2 ► The organic model
3 ► Matrix management

1 The bureaucratic model
Organizational theory is the study of how organizations are structured and how they work.(in 19th century)
The founders of the theory were sociologists like Max Weber and Mary Parker Follett, and practical businesspeople like Henri Fayol and Lyndall Urwick. They developed what is known as the bureaucratic model.
In a modified form, this model still describes the organizational structures found in most large and many smaller organizations.

The bureaucratic model characteristics
The ideal bureaucratic organization was thought to have the following characteristics:
1. All tasks are split up into specialized jobs, in which jobholders become experts; management can thereby hold the jobholders responsible for the effective performance of their duties.
2. Precise rules govern the performance of each task. This means that there should be no variation in the way tasks are carried out and therefore no problems with the coordination of different tasks.
3. Everyone (and hence each unit) in the organization is accountable to one and only one manager.
4. To ensure that personalities and personal relationships do not interfere with the organization's performance, employees must relate both to other employees and clients in an impersonal and formal manner.
5. Recruitment is based on qualifications and employees are protected against arbitrary dismissal. Promotion is based on seniority and achievement. Lifetime employment is envisaged.

2 The organic model
The best-known alternative model is the organic model Rensis Lickert expresses the basic assumption of the model in the following
(rather verbose) terms:
"An organization will be effective to the extent that its structure is such as to ensure a maximum probability that in all interactions and in relationships within the organization, each member, in the light of his background, values, desires, and expectations, will view the experience as supportive and one which builds a sense of personal worth and importance."

Key features of organic model
► This view underlies the organizational structure of most small professional companies – software houses, advertising agencies, and even solicitors' and GPs' practices
► it is also common in academic institutions, both schools and universities. The view is not necessarily consciously articulated – nor is this view and the adoption of the structures it suggests sufficient to achieve effectiveness!
► Proponents of the bureaucratic model claim that it is universally applicable.
► Proponents of the organic model make similar claims.
► Common sense is that those who believe each has its appropriate place should be of the contingency school of organizational design.

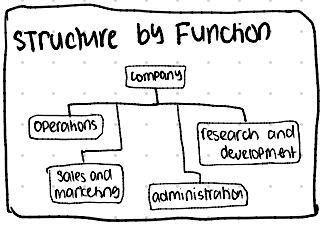


1 Structure by function
There are the activities that are the primary purpose of the organization. These activities are known as operations.

All organizations services or pay their bills and pay their employees. They need to ensure that the buildings they use are cleaned regularly. If they charge for their services, they may need to send out bills and ensure that these are paid. They will probably need to hire new employees from time to time. These activities are generally known as administration.

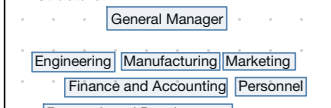
Many organizations will need to publicize their services or products and try to persuade people to use or buy them. In the business world, these activities are usually known as sales and marketing.

Finally, many organizations need to be continually developing new products or services or developing new ways to deliver them. These activities are known as research and development.

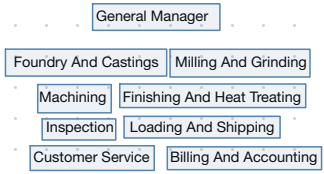


Functional Organizational Structures: Strategic Advantages/Disadvantages
Strategic Advantages
► Permits centralized control of strategic results
► Promotes in-depth functional expertise
► Enhances operating efficiency where tasks are routine and repetitive
Strategic Disadvantages
► Poses problems of functional coordination
► Can lead to interfunctional rivalry, conflict, and empire-building
► May promote overspecialization/ narrow viewpoints

Functional Organizational Structures: "Typical" Functional Organizational Structure



Process-Oriented Functional Structure



3 Product line structure
A product line structure is a structure that is based around the different types of product that an organization produces. For example, where a motor vehicle manufacturer organizes around types of vehicle.
► Companies that produce and market a substantial piece of software for corporate customers – a multi-user accounting package
► For example – often organize themselves into three main operational divisions: development and maintenance of the software, consultancy, and training. This should be regarded as a product line structure since the three types of activity, providing software, giving advice to companies in how to use it, and providing training for customer staff, can be considered to be different services that the company provides and they are typically provided by different teams of people.

5 Structure by technology
► A technology-based structure was once a favorite model for software companies.
► A company might have divisions specializing in artificial intelligence, communications, web-based systems, databases, and real-time systems.
► There are several problems with type of structure: it usually requires several different technologies to meet a customer's needs;
► there are many applications that cannot be said to require specific technologies;
► there are many competent software engineers whose expertise runs across a number of technologies;
► it is difficult, if not impossible, for sales and marketing staff to predict which potential clients will need which technology. It is particularly serious and companies that are primarily structured by technology have serious problems finding their clients.
► They are not sufficiently 'customer-focused' – they concentrate on selling the technologies that they have rather than finding out what the customer needs.

2. **Structure by geography**

► In many cases it makes sense to group activities on a geographical basis. Multinational companies, that is, companies that operate in several different countries, are usually forced to have some geographical elements in their structure.

► The subsidiaries are subject to the laws of the countries in which they are registered, in particular, the laws regarding employment, accounting, and taxation.

► Within a single country, geographical factors have become less important as a result of the development of modern communications, and, as a result, geographical structures have been replaced by structures based on other factors.

Geographic Organizational Structures: Strategic Advantages/Disadvantages

Strategic Advantages

► Allows tailoring of strategy to needs of each geographic market

► Improves coordination within the market

► Takes advantage of economies of local operations

Strategic Disadvantages

► Greater difficulty in maintaining consistent company image across areas

► Can result in duplication of staff services at headquarters and district levels, making a relative-cost disadvantage

4. **Structure by market sector**

► Structure by market sector means structure based on the different market sectors to which its customers or prospective customers belong.

► From the sales and marketing point of view it has the great advantage that each division can readily identify its potential customers, and its staff, both sales and technical, are likely to be familiar with customers' problems and to speak a language that the customer understands.

► Example :

Different branches of BATA Automobiles

Structure by market sector Disadvantages

There are two dangers with this approach.

► There is the risk one division may be unaware of technological expertise that exists in another division. This may lead to inefficient use of resources through unnecessarily hiring additional specialists or employing consultants, or, worse, to failing to learn from mistakes that have been made by other parts of the company.

► The second danger with a structure based on market sector is that, by continuing to concentrate on its traditional areas even when these markets are becoming saturated, the company will miss new opportunities and will stagnate.

6. **Operational structure**

► The actual operations of a company may be organized on a project basis or on a production basis, although the line separating the two may be vague.

► Project-based activity is not restricted to operations. Most research and development is organized on a project basis and such administrative activities as introducing a new accounting system or transferring a company's head office are also to be regarded as projects, in that they last for a fixed length of time, after which they should be complete.

► Projects last a comparatively long time but the team carrying out the work only stays together for the length of the project. Production activities are comparatively short, but the team carrying them out stays in existence indefinitely.

DEPTH OF STRUCTURE

The depth of an organizational structure is the number of layers in the structure – or, more precisely, the maximum number of layers, since not all parts of the structure will have the same number of layers.

Organizational structures are often described as flat or, in contrast, deep or tall, according to whether the depth is small or large. For a given number of people, the depth of the structure will depend on the number of people reporting directly to each manager; this is sometimes known as the manager's span of control.

CENTRALIZATION

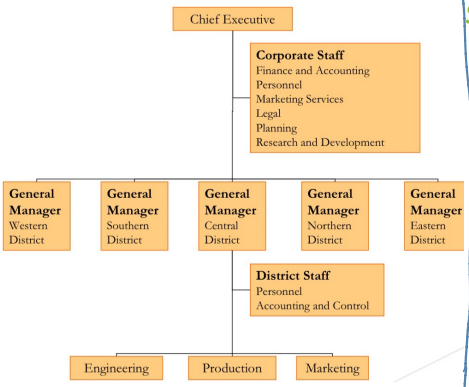
► Organizations may be centralized or decentralized. In a centralized company, as much power as possible is kept at the top of the company, with delegation only when essential.

► In a decentralized company, as much power and control as possible is delegated to the lowest level.

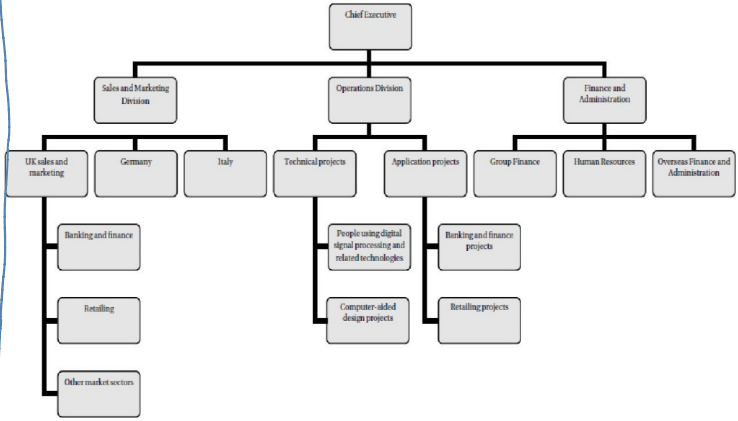
SETTING UP A STRUCTURE IN PRACTICE

In most cases, an organization of any size will have a structure that includes elements of several of the different types of structure. A combination of different structures would help when adopted.

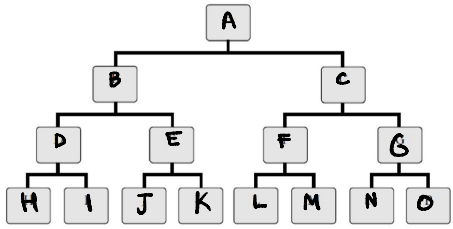
Geographic Organizational Structure



An organizational structure for a bespoke software house



Fifteen people organized into a four-level structure



HUMAN RESOURCES ISSUES

Together
Everyone
Achives
More

Human resources

► What is a resource?
► What is human resource?
► The people who work for an organization are an indispensable part of the organization's resources and most of the time, the most important part.

Why do we need Human Resources in an organization?
► Any organization that employs staff will be faced with the need to handle administrative issues relating to their employment.
► The cost of recruiting new staff is high and the loss of continuity when staff leave can also be very expensive. Accordingly, the organization will want to keep staff turnover low.
► A full-time personnel officer or human resources manager is required.

THE LEGAL CONTEXT

► In the 20th century, industrial relations in the UK were based on collective bargaining and were conceived about relations between trade unions and employers. In particular, the rights of trade unions received much more prominence than the rights of individual employees.
► Strikes were a common weapon for bargaining.

Individual employee/ unions

The greater attention paid to the rights of individual employees and the need to comply with anti-discrimination legislation have very considerably increased the workload of human resources departments in the UK..

HR Activities

The following list is a summary of the tasks that are expected to be undertaken with the overall aim of ensuring that the organization has the workforce that it needs:
► ensuring that recruitment, selection, and promotion procedures comply
► with anti-discrimination legislation;
► staff training and development;
► setting up and monitoring remuneration policy;
► setting up and monitoring appraisal procedures;
► administering dismissal and redundancy procedures;
► dealing with contracts of employment;
► workforce planning;
► administering grievance procedures;
► being aware of new legislation affecting employment rights and advising management of what the organization must do to comply with it;
► dealing with health and safety;
► administering consultative committees

Selection tools

A wide range of selection techniques is available and is used in making professional appointments:
► A series of one-to-one interviews with senior management and senior technical staff.
► Interview by a panel: A number of interviewers are involved. This technique is widely used, particularly in the public sector. It tends to favour applicants who are smooth talkers. It is unreliable.
► Assessment of references: Great importance is usually attached to references for academic posts and some other posts in public bodies.
► Psychometric tests: These are of three types.
1. Ability tests measure an individual's ability in a general area, such as verbal or numerical skills.
2. Aptitude tests measure a person's potential to learn the skills needed for a job.
3. Personality tests attempt to assess the characteristics of a person that significantly affect how they behave in their relationships with other people.

► Situational assessment: Real time situations are given to shortlisted candidates. Its most expensive and used in military officers selection.
► Task assessment: Candidates are asked to carry out some of the tasks that they will be required to do in the job. People usually are able to do small tasks but unable to do large task so this is unfavourable.

RECRUITMENT AND SELECTION

Human resources managers often make a distinction between the two terms recruitment and selection, using recruitment is to mean soliciting applications and selection is to mean selecting the applicants to whom offers will be made.
Selection is kept in the hands of the employer, although a member of the recruitment agency staff may sometimes be invited to advise.

STAFF TRAINING AND DEVELOPMENT

? Training and development encompasses three main activities: training, education, and development.
? It is a function concerned with organizational activity aimed at bettering the performance of individuals and groups in the organization. It has been known by several names, including "Human Resource Development", "Human Capital Development" and "Learning and Development".
? Staff training and development are of particular importance in high technology companies, where failure in this respect can threaten the company's performance.
? It is unfortunate that, when money is tight, it is often the first thing to be cut.

REMUNERATION POLICIES AND JOB EVALUATION

► Remuneration is the compensation that one receives in exchange for the work or services performed. Typically, this consists of monetary rewards, also called wages or salaries. Several complementary benefits, however, are increasingly popular remuneration mechanisms.
► For grading and scaling policies are developed and job evaluations are held.

Unfair dismissal vs wrongful dismissal

► Dismissal of an employee without valid reasons is unfair
► A fair dismissal of an employee but violating a contract is wrongful dismissal

APPRAISAL SCHEMES

► Appraisal (Performance appraisal)is a method by which the job performance of an employee is documented and evaluated
► Need for Appraisal?
► Appraisal schemes usually involve an appraiser and an appraisee meeting
regularly (every six months, every year, even every two years) to discuss the employee's performance and career development under several headings. The result is a report signed by both parties; if they cannot agree on certain points this will be recorded in the report.
The person responsible for undertaking an appraisal of an employee (the appraisee). The appraiser is often the employee's line manager since he or she is thought to have the best knowledge of the employee's performance, attitude, and competency.
► Appraisals derive from the idea of Management by Objectives (MBO). MBOs were developed by Peter Drucker, one of the most distinguished management theorists, in the 1970s, and it rapidly became popular in the industry. It was seized on by the government in the 1980s as a way of dealing with what they saw as poor performance and indolence in many state-funded jobs.
► The essence of MBO is that managers and their subordinates agree on a set of objectives for the subordinate to achieve over the next period, typically six months. These objectives should be precise, objectively verifiable, and, ideally, quantifiable.

REDUNDANCY and DISMISSAL

► Redundancy is a form of termination caused by changes in the business,
while dismissal is a form of termination caused by employee misconduct or poor performance.
► Unfair dismissal
► Reasons justifying dismissal:
  ► lack of capability;
  ► misconduct;
  ► breach of the law
  ► Redundancy
  ► Constructive dismissal

CONTRACTS OF EMPLOYMENT

► What is a contract?
The written agreement between an employee and their employer can be
enforced in a court of law.
► A good contract of employment should be written in terms that are easily understood and should avoid legal conflicts.
► Prospective employees should not need to consult a lawyer to understand it. They should, however, read it carefully before signing it.

Public interest disclosures

► Whistle blowers
► The Public Interest Disclosure Act 1998 (PIDA) applies to people at work who raise concerns about criminal behavior, certain types of civil offenses, miscarriages of justice, activities that endanger health and safety or the environment, and attempts to cover up such malpractice.
► Whistleblowing (also whistle-blowing or whistle-blowing) is the activity of a person, often an employee, revealing information about activity within a private or public organization that is deemed illegal, immoral, illicit, unsafe, or fraudulent.
► A whistleblower is someone who reports workplace conditions that they believe to be unsafe or illegal. As a whistleblower, you have the right to be protected from workplace retaliation by your employer for reporting injuries, safety concerns, or other protected activities.

Take overs and outsourcing

► Employees employed by the previous employer when the undertaking changes hands automatically become employees of the new employer on the same terms and conditions. It is as if their contracts of employment had originally been made with the new employer. Thus, employees' continuity of employment is preserved, as are their terms and conditions of employment under their contracts of employment (except for certain occupational pension rights).
► Representatives of employees affected have a right to be informed about the transfer. They must also be consulted about any measures which the old or new employer envisages taking concerning affected employees.

HUMAN RESOURCE PLANNING

► If the human resources department is to ensure that the organization always has available the staff it needs, it must be able to forecast the needs some time ahead.
► In a software house, there are three inputs to the human resource planning process:
► Human resource plans from existing projects,
► Sales forecasts
► Forecasts of the likely staff losses in the coming months

JOB DESIGN

► **Job rotation:** Job rotation, that is, rotating staff through a series of jobs, is the most obvious way of preventing employees from becoming bored with a very narrow and specialized task.
► **Job enlargement:** Job enlargement means increasing the scope of a job through extending the range of its job duties and responsibilities generally within the same level and periphery. Job enlargement involves combining various activities at the same level in the organization and adding them to the existing job
► **Job enrichment:** Job enrichment can be described as a medium through which management can motivate self-driven employees by assigning them additional responsibilities normally reserved for higher-level employees. By doing this, employees feel like their work has meaning and is important to the company

ANTI DISCRIMINATION LEGISLATION

WHAT IS DISCRIMINATION?
► Discrimination means treating one person or one group of people less favorably than another on the grounds of personal characteristics.
► Discrimination can be direct or indirect.

Discrimination Grounds
In Europe, the USA, and many other countries prohibit discrimination on grounds such as:
► sex, Gender;
► race, color, ethnic origin, or nationality;
► disability;
► sexual orientation;
► religion;
► age.

Direct discrimination
► Direct discrimination occurs when one person is treated less favorably than another specifically because of their sex or race, and so on.
Examples
► A woman does the same job as a man but is paid less than he is.
► A doctor refuses to treat a Chinese patient on the grounds that he has no room for any more patients but then accepts an English patient.
► A company advertises for a secretary and automatically rejects all the male applicants.
► A company advertises for 'a mature woman to act as the Chief
► Executive's personal assistant' or 'a strong young man to work as a trainee zoo-keeper'.

Indirect discrimination
Indirect discrimination occurs when an employer imposes conditions that apply
to all employees or applicants but disproportionately affect one group
Examples
►Advertising a job with the requirement that applicants must be at least 180 cm tall. In the UK, there are many men over 180 cm tall but very few women. The result is that few women can apply for the job.
► When allocating public housing, a local authority has a policy of giving priority to the children of existing tenants.
► An employer insisting that all employees work on Saturdays. This might be held to be indirect discrimination against those who practice Judaism, since Saturday is their Sabbath. This would be discrimination on grounds of religion but, since the practitioners of Judaism are overwhelmingly of the Jewish race, it might also be regarded as racial discrimination.

It can be justified if the employer demonstrates that there is a genuine occupational requirement that the offending condition be satisfied.

DISCRIMINATION ON GROUNDS OF Gender
► Formally women got low salaries and men got extra allowances and more if they are married
► Married women were either to lose their job or transferred to temporary status
► Women after having kids were not allowed to rejoin
► it was very difficult for women to gain entry to academic and professional courses in fields such as medicine or the law that would have qualified them for senior positions.

Act of Parliament
In UK, this situation was dramatically changed by two Acts of Parliament: ► the Equal Pay Act of 1970 and
► the Sex Discrimination Act of 1975.
The most important features of the law as it stands can be summarized as follows:
1. ► Regarding Employment
2. ► Regarding Education
3. ► Regarding Provision of services

1 Act of Parliament Regarding Employment
► It is unlawful for an employer to discriminate against a person on grounds of their sex or marital status in terms of the arrangements made for recruitment and selection and the terms on which employment is offered.
► It is unlawful for an employer to discriminate against an employee on grounds of their sex or marital status regarding opportunities for promotion, transfer, or training or to any other benefits.
► It is unlawful for an employer to discriminate against an employee on grounds of their sex or marital status regarding dismissal or redundancy.
► It is unlawful for an employer employer to victimize an employee for bringing a complaint of sex discrimination or for giving evidence in support of another employee's complaint.
► It is unlawful for any of the following to discriminate against a person on grounds of sex or marital status:
a trade union, a professional body, a registration authority, an employment agency, or a provider of vocational training.

2 Act of Parliament Regarding Education
► It is unlawful for a provider of education (public or private, school, college or university) to discriminate against a person person based on their sex, in offering admission to the establishment or to specific courses, and in providing access to the other benefits and facilities it offers.
► The main exceptions to this are that allowance is made for single-sex establishments and that provision for physical education may be different for the two sexes.

3 Act of Parliament Regarding Provision of services
► It is unlawful to discriminate on grounds of sex in the provision of goods, facilities, or services. The Act gives several examples including accommodation in a hotel, facilities for entertainment, recreation or refreshment, banking and insurance services, and so on.
► It is unlawful to discriminate on grounds of sex in selling or letting property.
The main exception to these provisions is for charities that have been founded to help a specific group of people who are all the same sex, for example, single mothers.

Remedies
Bring the matter to an employment tribunal. If the tribunal favors the complainant, it can award damages and make recommendations to the respondent. If the respondent fails to act on the recommendations, the amount of the damages may be increased.

DISCRIMINATION ON GROUNDS OF RELIGION OR BELIEF, OR SEXUAL ORIENTATION
As regards discrimination on grounds of sexual orientation and religious belief, that the EU directive is implemented in the UK by the Employment Equality (Sexual Orientation) Regulations 2003 and the Employment Equality (Religion or Belief) Regulations 2003, both of which came into effect in December 2003. These regulations follow the pattern established by the Sexual Discrimination Act 1975 and the Race Relations Act 1976.

DISCRIMINATION ON RACIAL GROUNDS
► The present law is based on the Race Relations Act 1976 and subsequent amendments to it.
► It makes it unlawful to discriminate on grounds of race, color, ethnic origin or nationality.
► It introduced the idea of indirect discrimination based on race. It established the Commission for Racial Equality by the merger of the Race Relations Board and the Community Relations Commission.

** Commission for Racial Equality (CRE) was a non-departmental public body in the United Kingdom that aimed to address racial discrimination and promote racial equality.

DISCRIMINATION ON GROUNDS OF AGE
The Equal Treatment Directive is careful to be quite explicit in allowing for discrimination on the grounds of age in several important cases. It allows, for example:
► special treatment of different age groups to protect them (e.g., not allowing children under a certain age to be employed);
► different premiums for life insurance policies, depending on the age of the person at the time the policy is taken out, and different pension rates depending on the age of retirement (but these must not amount to sex discrimination);
► fixing a maximum age for recruitment based on the need for a reasonable period of employment after training and before retirement;
► fixing a minimum age, a minimum amount of professional experience or a minimum number of years with the company before a person will be regarded as eligible for a given post or eligible for certain employment benefits (e.g., additional annual leave).

DISCRIMINATION ON GROUNDS OF DISABILITY
► From the 1970s onwards, the government had been encouraging the recruitment of disabled employees into the Civil Service and encouraging employers to take on disabled workers by withholding government contracts from companies that could not demonstrate a commitment to offering opportunities to the disabled.

Disability Discrimination Act 1995
The Act makes it unlawful to treat a disabled employee or applicant less favorably because of their disability without justification.
► The justification must be serious and substantial. Thus, it would be justified to reject a blind applicant for a job as a bus driver or a paraplegic for a job as a lifeguard.

Survey
The Disability Rights Commission commissioned a study of web accessibility for the disabled, which resulted in a report entitled The Web: Access and Inclusion for Disabled People. The study included a survey of 1,000 home pages and found that 81 percent, including many government sites, failed to comply with even the lowest level of the W3C guidelines. Among the most common reasons why disabled users had trouble were:
► page layout was unclear and confusing;
► the navigation mechanisms were confusing and disorienting;
► there was poor contrast between the text and the background and colors were used inappropriately;
► graphics and text were too small;
► links and images were poorly labeled;
► the web pages were incompatible with the software designed to assist disabled users (screen readers, magnification software).

Employment Equality (Sexual Orientation and Religion or Belief) Regulations 2003,
► They are limited to discrimination in employment, education, and related matters, and do not refer to discrimination in the provision of services or accommodation, for example.
► They explicitly make harassment unlawful, defining it as 'unwanted conduct which has the purpose or effect of violating a person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment. Although the courts and industrial tribunals had accepted that racial or sexual harassment constituted discrimination, this was not explicitly covered by previous anti-discrimination legislation.
► They do not make any body, such as the Commission for Racial Equality, responsible for promoting the implementation of the legislation nor do they create any new body for this purpose. However, in October 2003, the government announced its plans for a single equality body for the UK to take over the responsibilities of the Equal Opportunities Commission, the Commission for Racial Equality, and the Disability Rights Commission.

AVOIDING DISCRIMINATION
Effective compliance with anti-discrimination legislation in the workplace requires three things:
► a suitable written policy, well-publicized, and freely and easily available;
► a training program for new and existing staff, to ensure that they are all aware of the policy and its importance;
► effective procedures for implementing the policy.

SOFTWARE CONTRACTS 1

Definition of a Contract

A contract is an enforceable agreement between two or more parties (legal or natural persons).
It is binding in a court of law.

Essentials for a Valid Contract

Intention: All parties must intend to enter into a contract.
Competency: All parties must:
Be competent (understand what they are doing).
Consideration:
There must be a value exchange—each party gives and receives something.

Bespoke Systems

Definition: Tailor-made/custom-designed systems created for the unique requirements of a specific organization or individual.
Examples:
Small: Single PC with custom macros for specific tasks.
Large: Thousands of PCs across global offices connected via networks, using custom databases and millions of lines of software code.
Purpose:
Automating business processes.
Managing customer data.
Enhancing employee collaboration.
Advantages:
Customized for specific needs.
Increases efficiency, effectiveness, and productivity.

Fixed Price Contracts for Bespoke Systems

The contract for the supply of a requirements system consists of three parts:
1.Short Agreement:
Identifies the parties involved.
States that prior discussions or writings do not form part of the contract.
2.Standard Terms and Conditions:
Usual business terms of the supplier.
3.Schedules/Annexes:
Specifies requirements, deliverables, timelines, payment terms, and other details.

Key Issues in the Contract

1.What is to be produced:
Clear definition of the deliverables in the requirements specification.
Reference to the specification should include date and issue number for uniqueness.
Challenge: Managing changes during the contract lifecycle.

2.What is to be delivered (examples):
The following is a non-exhaustive list of possibilities:
Source code, command files, design documentation.
Manuals (reference, training, operations).
Maintenance tools, user training, and deployment materials.
Test cases and test results.

3.Ownership of Rights:
Contract must clearly state:
Who owns the rights.
Which rights are transferred from the software house to the client.
Types of Rights:
Physical Items: Usually passed to the client.
Intellectual Property (IP) Rights: Often more complex and contentious.
Examples:
- **Copyright**: Protects the source code.
- **Design Rights**: Protect software interface or architecture.
- **Confidentiality**: Protects proprietary information.
- **Trademarks**: Protects branding within the software.

4.Confidentiality:
Significance:
Developing bespoke systems often requires the exchange of sensitive information:
1. The client shares business details.
2. The software house may share proprietary techniques or content.

Mutual Protection:
Both parties agree not to disclose the other's secrets.
A clause in the contract explicitly addresses confidentiality.
Common Provisions:
Clients protect information on business operations.
Software houses safeguard the software's design, code, and content.
Objective:
Ensures neither party's sensitive data is misused or leaked.

6.Penalty Clauses:
Delays in delivering working software are notoriously common; it might therefore
be expected that contracts for the supply of software would normally include
such a penalty clause. There are three reasons for this:
Reluctance: Suppliers often resist penalty clauses; stricter clauses may deter reputable suppliers from bidding.
Increased Costs: Inclusion of penalty clauses can raise bid prices, typically by at least half the penalty's maximum value.
Severe Delays:If penalties approach their maximum, suppliers may lose motivation to complete the project as stage payments may already cover their potential earnings.

5.Payment Terms:
Typical structure:
-15%: On signing the contract (requirements gathering).
-50%: Stage payments during development/testing.
-25%: On acceptance of software (deployment).
-10%: After warranty period (final sign-off).
Includes provisions for extra payments for delays, wasted effort, or requested changes.

Calculating Payments for Delays and Changes
1.Impact of Delays:
Both parties may experience losses if timelines are not met.
Delays often require extra work, which must be compensated.
2.Provisions for Extra Payments:
Contracts must clearly define:
1. The process for calculating payments for delays.
2. Compensation for additional work or wasted effort.

Examples of Situations Requiring Compensation:
3.Client Delays:
Failure to provide required information or approvals by agreed deadlines.
Requested Changes:
Variations to the original requirements that necessitate extra work.
4.Common Issues:
Disputes: Delay payments and changes to requirements are frequent causes of disagreement between parties.
Transparency: Clear processes and formulas for determining extra payments help prevent disputes.
Resolution Strategies
Specify timelines and responsibilities for both parties.
Include detailed terms for managing:
Delay penalties for suppliers.
Additional payments for client-induced delays or changes.
Maintain records of changes and approvals to support claims for extra work.

7.Obligations of the Client:
Client usually has some responsibilities to help get the work done smoothly.
These might include:
-Provide business documents and system environment details.
-Grant access to staff, equipment, and workspace if required.
-Providing computers and equipment for development and testing.
-Offering workspace, phone, and administrative support if work is done at their location.
-Setting up data communication as needed.
These obligations and deadlines are usually listed in the contract.
If the client doesn't meet these, they might have to pay for any delays.

8.Standards and Methods of Working:
Suppliers prefer their established processes and quality assurance procedures.
Some clients may require adherence to their own standards.
The contract specifies which standards/methods will apply.

SOFTWARE CONTRACTS 2

Common Challenges in contracts
Managing changes and variations to the original requirements.
Addressing delays caused by both parties.
Negotiating ownership of intellectual property rights.
Ensuring mutual confidentiality.
Resolving disputes over payments and penalties.

Project Meetings
1.Importance:
Regular progress meetings are crucial for the success of fixed-price contracts.
Standard terms should mandate these meetings.
2.Minutes of Meetings:
Approved and signed minutes should:
Serve as contractual evidence of milestone achievement (triggering stage payments).
Document agreed delay payments.

Project Managers
1.Role and Responsibility:
Each party must appoint a project manager in writing.
The project manager handles day-to-day responsibilities and ensures contract obligations are met.
2.Authority:
Project managers must have sufficient authority to fulfil their duties.
Their financial authority limits should be explicitly defined, particularly regarding cost changes to the contract.

Termination of Contract
1.Reasons for Termination:
Client acquisition by a company with an existing system.
Change in client policy rendering the system irrelevant.
2.Termination Terms:
Supplier must be compensated for:
Work completed up to termination.
Time needed to reassign staff to other revenue-earning work.
Ownership of partially completed work must be clarified.

Acceptance Procedures
1.Purpose:
Define criteria for judging contract completion.
Acceptance based on client-provided tests and expected results.
2.Test Process:
Tests must be provided before the acceptance procedure begins.
Extra tests cannot be added after submission to ensure timely completion.
3.Additional Terms:
Specify who will be present during tests.
Define actions if tests fail (exception handling).

Warranty and Maintenance
1.Warranty Period:
Begins after deployment and acceptance, typically lasts 90 days.
Errors reported within this period are corrected for free.
Adjusting warranty duration affects contract cost (longer = higher, shorter = lower).
2.Maintenance Post-Warranty:
Typically offered on a request basis and charged by time and materials.
Maintenance may involve enhancements beyond simple error corrections, making fixed prices unsuitable.

Inflation
1.Protection Against Inflation:
Long-term contracts should include an inflation clause.
Allows charges to increase with rising costs.
2.Terms of the Clause:
Specify frequency of adjustments (e.g., annually).
Define calculation methods for price increases.

Indemnity
1.Purpose:
Protect parties from liability due to the other's actions.
2.Common Scenarios:
Supplier infringes third-party intellectual property rights (knowingly or unknowingly).
Client instructions lead to unintentional infringement.
3.Clause Terms:
Each party indemnifies the other for costs arising from its faults.

Software Arbitration
Purpose:
Clause to resolve disputes through independent arbitration.
Arbitrator Appointment:
Arbitrator appointed by the President of the BCS or President of the IEE.
Both bodies maintain lists of technically qualified arbitrators.

Arbitration Act 1996
Application:
Governs arbitration proceedings when required.
Provides a default set of rules unless overridden by specific contract provisions.
Key Feature:
Optional provisions activate only if the contract has no alternative arrangements.

Applicable Law
Necessity:
Required for contracts involving parties in different jurisdictions.
Specifies the legal system under which the contract will be interpreted.

Contract Hire
Definition:
Supplier provides staff at daily/hourly rates.
Customer manages the staff.
Termination:
Either party can terminate at short notice.
Supplier Responsibility:
Provide competent staff and replace unsuitable or unavailable personnel.
Payment:
Based on fixed rates determined by staff experience and qualifications.
Intellectual Property:
Ownership of IP generated during work must be addressed in the contract.

Consultancy
Definition:
Experts assess operations or strategies and propose improvements.
Consultancy Projects:
Provide expert advice or reports for a fixed price.
Contracts are simpler than fixed-price contracts due to lower risks.
Approaches:
1.Simplified Contracts: Reflect minimal financial risks.
2.Reputation: Ensures quality as suppliers aim to maintain professional credibility.

Key Aspects of Consultancy Contracts
Confidentiality:
Safeguards prevent misuse of sensitive information for personal gain.
Terms of Reference:
Define the scope of work clearly to avoid disputes.
Liability:
Consultants often limit liability for losses caused by their advice.
Clients may require professional liability insurance.
Control Over Final Report:
Draft report reviewed by the client for changes.
Final version submitted after revisions.

Time and Materials Contracts
Definition:
A contract where the supplier is paid based on costs incurred (similar to contract hire).
Supplier is not committed to a fixed price, though a maximum payment may be established.
Payment:
Based on labor and materials costs, as in contract hire.
Review:
Project may be reviewed if the maximum payment is exceeded.

Outsourcing
Definition:
Outsourcing (or facilities management) is when a company transfers planning, management, and operation of functions to another organization (the supplier).
Complexity:
IT outsourcing contracts are complex and depend on individual circumstances.
Key Points in Outsourcing Contracts:
Performance monitoring and management.
Consequences of unsatisfactory performance.
Asset transfer details.
Staff transfers.
Audit rights.
Contingency planning and disaster recovery.
Intellectual property rights for software developed during the contract.
Duration and termination provisions.

Health and Safety
Key Concerns for Software Engineers:
Provision and maintenance of safe plant and systems.
Information, instruction, training, and supervision for safety.
Ensuring the workplace is safe and properly maintained.
Safe working environment and adequate welfare arrangements.
Legal Responsibility:
Employers must ensure their activities don't pose health and safety risks to the public.
Manufacturers must ensure equipment used at work is safe.
Non-Compliance:
Failure to comply with the Health and Safety at Work Act is a criminal offense, and serious violations may result in criminal proceedings.

A software developer creates an app that streams music tracks they purchased legally from an online store. The developer claims that streaming the tracks is covered under fair use.
The developer's claim is incorrect. Purchasing music grants a license for personal use only, such as listening privately on personal devices. Copyright law protects the creator's exclusive rights, including reproduction, distribution, and public performance. The right to stream the music publicly or use it commercially is not included in the purchase, and fair use does not apply in this case.

A startup develops a fitness tracking wearable with a unique skin conductivity sensor for monitoring hydration levels. Another company creates a similar device and argues that the sensor design is obvious.
To be patentable, the wearable must be novel, involve an inventive step, and have industrial applicability. The competing company's claim of obviousness challenges the inventive step, which requires the invention not to be obvious based on prior art. If the sensor is just a minor tweak, the patent could be invalid. However, if it offers a significant technical improvement, the patent is stronger. Prior art and novelty are key factors in defending the patent.

A biotechnology company is negotiating a joint venture with a university for a cancer treatment. The university accidentally publishes preliminary results online, revealing proprietary methods.
The accidental disclosure breaches confidentiality and could jeopardize the biotechnology company's ability to secure a patent due to loss of novelty. If an NDA existed, the company could seek damages or injunctive relief. Exceptions like the Public Interest Disclosure Act may not apply, so legal action for the breach is possible.

"NextVision," a tech firm, finds its domain name nextvision.com registered by a cybersquatter who demands a high price. What to do?
This is a case of cybersquatting, where the squatter profits from the trademark's goodwill. NextVision can file a complaint under the Uniform Domain Name Dispute Resolution Policy (UDRP), which requires proving:
1.The domain is identical or confusingly similar to NextVision's trademark.
2.The squatter lacks legitimate rights to the domain.
3.The domain was registered in bad faith.

If NextVision's trademark is strong, it may also pursue recovery under the U.S. Anti-Cybersquatting Consumer Protection Act (ACPA). Legal action or negotiation for the domain is possible, similar to the Tesla v. Tesla.com case.

Two companies collaborate to develop a SaaS platform and agree to jointly own the intellectual property. One company later licenses the platform to a third party without consulting the other, leading to a dispute.
In joint ownership, IP rights are shared, and licensing usually requires mutual consent unless specified otherwise. If the contract doesn't allow unilateral licensing, the licensing company may breach the agreement. The aggrieved party can seek damages or an injunction to stop the unauthorized license.

INTELLECTUAL PROPERTY RIGHTS

Intellectual Property Rights

If someone takes your bike, it's gone—you don't have it anymore. If a company loses a computer, it's gone too.
But imagine you create a formula for a medicine that cures all diseases. If someone reads it off your desk, they can use it to make lots of money. The difference is, you still have the formula, even though they now know it too.
This shows the difference between intellectual property (like ideas and formulas) and physical property (like bikes and computers).

Intellectual Property vs. Physical Property

• Physical property (like a bike or computer) is something you can touch. It's protected by laws against theft and damage.
• Intellectual property (like ideas, inventions, or software) can't be touched. It's protected by special laws called intellectual property rights, which control how ideas can be used, copied, or shared.
For example, software is an idea you can't touch. Companies use intellectual property rights to protect their software, because regular theft laws don't apply.

Laws

1. The international law relating to trademarks and patents is based on the Paris Convention,
which was signed in 1883.
2. The Berne Convention, which lies at the basis of international copyright law, was signed in
1886.

DIFFERENT TYPES OF INTELLECTUAL PROPERTY RIGHTS

1. Copyright
• What it is: Protects the right to copy and use creative works like books, music, photos, software, and more.
• How it works: You automatically own copyright when the work is written, recorded, or saved. No registration is needed.
• Key example: A computer program is protected under copyright as a "literary work."

2.Patents
• What it is: Protects inventions, giving the inventor the exclusive right to use, make, or sell the invention for a certain time (usually 20 years).
• Key example: A new type of drug or machine.

3.Confidential Information
• What it is: Protects private information shared in trust, like trade secrets or company strategies.
• Key example: A secret recipe for a product.

4.Trademarks
• What it is: Protects symbols, names, or logos that identify a brand or company.
• Key example: The Nike "swoosh" logo or Coca-Cola's brand name.

1.COPYRIGHT

What Copyright Protects

•Creative works like books, music, art, and computer programs.
•Copyright doesn't need registration—it applies as soon as the work is saved in some form (written, recorded, or saved digitally).

Rights of a Copyright Owner

1.Copying the Work:
•Includes making digital copies, like loading software into a computer's memory or downloading a webpage.
2.Sharing Copies with the Public:
•Selling or distributing the work (even free) is covered under copyright law.
3.Adapting the Work:
•Includes translations (e.g., from English to Chinese or from one programming language to another).

How Long Copyright Lasts

•Generally, it lasts for 70 years after the author's death. However, exceptions exist (e.g., old software or special cases).

What Copyright Does Not Protect

•You can't stop someone from creating identical work if they didn't copy yours. For example, if two people independently create the same program, both are legal.

Databases

Databases can be protected in two ways: copyright or database rights.
1.Copyright for Databases:
•A database is protected by copyright if its contents are a result of the creator's intellectual effort (like organizing unique data in a creative way).
•Example: A database of original research findings.
2.Database Right:
•Created to protect databases that may not qualify for copyright but still required a lot of work or money to make.
•Example: Lists of hotels, pop songs, or geographic data that required significant investment in gathering and organizing.
•Protection Length: The database right lasts 15 years and stops others from copying or reusing significant parts of the database without permission.

What You Can Legally Do with Copyrighted Works

Some actions are allowed by copyright law, especially for software:
1.Backup Copies:
•You can make one backup of software you own.
2.Decompiling Software:
•Allowed to fix errors or to make your program work with another one (only if this information isn't available in any other way).
3.Selling Software You Own:
•You can sell your right to use the software, but you must delete all your copies.

Conclusion

Copyright laws aim to balance protecting creators while allowing limited use for practical purposes like backups or fixing errors. Understanding these rules is essential for working with intellectual property, especially software.

Copyright Case Studies

•**Authors Guild v. Google, Inc. (2015)**: The Authors Guild sued Google over its Google Books project,which scanned millions of books and made portions of them searchable online. Google argued that itsuse was fair use, as it was transforming the content to create a searchable database, which would helpusers discover books.
•**Google Inc. v. Oracle America, Inc. (2021)**: Oracle sued Google, claiming that Google had copied Java'sAPI (Application Programming Interface) code when developing the Android operating system. Oracleargued that Java's API was copyrighted and that Google's use of it without a license was infringement.Google, on the other hand, argued that its use was fair use, as it involved using the Java code to create anew

Copyright Infringement

Copyright infringement happens when someone uses or copies a copyrighted work without the owner's permission.

1.Primary Infringement:

•Occurs when someone directly violates the copyright owner's rights, such as copying, distributing, or adapting their work.

•**Example**: Downloading software without paying for it.

•**Legal Consequences**: Handled in civil courts; remedies include paying damages or being forced to stop the infringement.

2.Secondary Infringement:

•Happens in a business or commercial setting, where pirated content is distributed or used.

•**Examples**:

- •Selling pirated software.
- •Using unlicensed software in a company.

•**Legal Consequences**: Treated as a criminal matter, with penalties like large fines or imprisonment.

Basically Infringement:

Direct use of copyrighted works is primary infringement; commercial or business-related misuse can lead to secondary infringement, with more serious penalties.

Licensing

1.What is Licensing?

•Licensing is when the owner of a copyrighted work allows someone else to use it, but without giving up ownership.

2.How it Works:

•The owner keeps the copyright, but licensees (the people using the work) gain permission to perform certain actions, like using or modifying the software.

3.Example:

•A company that creates a software program can license it to users, allowing them to install and use it under certain conditions, such as paying a fee or agreeing not to distribute it.

Licensing: Licensing lets others use the work while the copyright owner still retains full control.

Secondary Copyright Infringement and Online Platforms

•**Platforms like YouTube or Facebook** can face secondary infringement claims when they host user-uploaded content that violates copyright (e.g., music, movies).

•**Key Points:**

- •Platforms are liable if they know about the infringement but fail to remove or block it.
- •This is why platforms often use tools like copyright filters to prevent illegal content from being shared.

•**Online Content**: Websites must actively prevent and remove infringing content to avoid liability.

Ownership of Copyright

1.Who Owns the Copyright?

•The person who creates the work (the author) usually owns the copyright.

•If multiple people create a work together, they share the copyright.

2.Employees vs. Independent Contractors

•**Employees**:

•If an employee creates a work as part of their job, the employer owns the copyright unless there's a written agreement saying otherwise.

•**Independent Contractors (Freelancers):**

•A freelancer owns the copyright for the work they create, unless the company hiring them makes a formal agreement that transfers ownership.

•Key Example: A freelance programmer writing software for a company needs a contract that clearly states who owns the copyright.

Ownership: Copyright usually belongs to the author, but for employees, the employer gets the rights unless stated otherwise. Freelancers, however, retain ownership unless a contract says differently.

2. PATENTS

What is a Patent?

A patent is a legal right that protects inventions. It gives the inventor control, letting them stop others from using, selling, or copying the invention without permission.

•**Temporary Right**: Patents last for a specific time (usually 20 years).

•**Stronger than Copyright**: It protects the invention even if someone else independently discovers it.

Why Do We Need Patents?

1.Encourages Innovation:

•Inventors may fear sharing their ideas because others could copy them. A patent protects the invention, motivating inventors to reveal their work.

2.Temporary Monopoly:

•During the patent's life, inventors can profit exclusively, recover their costs, and block competitors.

•After the patent expires, others can use the invention freely.

3.Monetization:

•Inventors can make money by licensing their patent to others or by using it to dominate a market.

What Can Be Patented?

An invention must meet these four conditions:

1.New:It hasn't been made or shared before.

2.Inventive:It isn't obvious; it requires creativity.

3.Useful:It works in real-world applications.

4.Allowed by Law:It doesn't fall under excluded categories like natural laws or abstract ideas.

Key Takeaways

Purpose: Patents encourage sharing inventions by protecting inventors with a temporary monopoly.

Criteria: To qualify, inventions must be new, inventive, useful, and legally allowed.

Exclusions: Abstract ideas, artistic works, or business schemes can't be patented.

Process: Getting a patent is complex and requires time, money, and professional expertise.

What Can't Be Patented?

Certain things are excluded under the European Patent Convention and the UK Patents Act 1977:

•Scientific Theories: Ideas like gravity can't be patented, but inventions using those theories can.

•Mathematical Methods: You can't patent calculations, but machines using them in a unique way might qualify.

•Artistic Creations: Literary or musical works are protected by copyright, not patents.

•Information Presentation: Data organization or layouts can't be patented.

•Business Schemes or Computer Programs: General methods for games, mental tasks, or business processes are excluded. However, if a program performs a technical function, it might qualify.

How to Obtain a Patent

1.Application Process:

•Unlike copyright, patents don't happen automatically—you must apply.

2.Costs and Time:

•Applying for a patent can be expensive and take up to four years.

3.Patent Offices:

•Patents are granted by national offices.

•If international protection is needed, separate applications must be made in each country.

4.Specialist Help:

•A patent attorney usually prepares the detailed application, ensuring it meets all legal and technical requirements.

Enforcing a Patent

1.A Patent Doesn't Automatically Stop Infringement:

•Owning a patent means you have the right to stop others from using your invention, but you must enforce it yourself, often through legal action.

2.Challenges in Enforcement:

•Proving Prior Art: You must show your invention is unique and wasn't already known before you filed for the patent.

•Costly Legal Battles: Patent disputes can be expensive, involving court cases and lengthy legal procedures.

Key Takeaways

•Patents require enforcement, which can be costly and complex.

•Software patents focus on functionality (e.g., methods, systems, or processes), not just the code.

•Regional Differences: The USA and Europe handle software patents differently, and European policies are often inconsistent.

•Value of Patents: They protect innovation, secure investment, and ensure fairness between software and hardware systems.

Software Patents

1.What Can Be Patented in Software?

In the USA, software can be patented if it meets certain criteria:

•Part of a Patentable Product: The software is part of something already eligible for a patent (e.g., a machine).

•Controls Physical Effects: It causes a physical change (e.g., software controlling a robot or manufacturing process).

•Handles Real-World Data: It processes data that comes from physical events (e.g., monitoring weather or medical data).

2.Example:

•A new algorithm that speeds up image processing in medical imaging software could be patented if it's a novel and technically complex solution. However, the code itself is protected by copyright, not the patent.

3.Software Patents in Europe:

•Since 1998, the European Patent Office (EPO) and the UK Patent Office have granted patents for software.

•However, different European countries have inconsistent policies, leading to confusion and legal conflicts about what qualifies as patentable software.

Why Patents for Software Are Important

1.Encourages Innovation:

•Patents help secure funding for research and development because they provide a clear and legally recognized asset.

•Investors can be confident that their money is creating something valuable that competitors can't easily copy.

2.Fairness:

•It is reasonable that a system implemented in hardware should be patentable, and the same should apply if the system is implemented in software.

Example of a Software Patent

•An MRI machine that uses software to enhance image clarity:

- •The software isn't just a standalone program but a key component of the machine.
- •Its technical contribution (improving image quality) is innovative, making it eligible for a patent.

3 CONFEDENTIALITY

What is Confidential Information?

•**Key Idea**: Confidential information refers to private details shared in a setting where the recipient is expected to keep them secret. This expectation is called an obligation of confidence (اعتماد کی ذمہ داری, رازداری).

•**Not an Intellectual Property Right**: Unlike patents or copyrights, confidentiality rights aren't legally considered intellectual property, but they are treated similarly in practice.

How Confidentiality Works

1.Contracts and Agreements:

•Often, a contract clause or a Non-Disclosure Agreement (NDA) creates this obligation.

•Example: Two companies discussing a partnership may sign an NDA to protect sensitive information shared during the talks.

2.Protecting Potential Patents:

•Sharing an invention idea publicly before filing a patent could disqualify it.

•Inventors should only share such ideas under a confidentiality agreement to protect their future patent rights.

3.Other Business Examples:

•Sales negotiations: While software companies might not have many trade secrets, sales discussions are crucial. Competitors could gain an advantage if they learn about these plans.

Confidential Information vs. Professional Knowledge

•**Confidential information** refers to specific, sensitive details that must be kept private.

•**Professional knowledge** and skills are general expertise gained through experience and are not considered confidential.

When Confidentiality Can Be Broken

1.Public Interest:

•Courts may decide to reveal confidential information if it benefits the public.

•Example: Whistleblowing cases where an employee exposes a company's wrongdoing.

2.Legal Protection for Whistleblowers:

•The Public Interest Disclosure Act (1998) protects workers who expose issues like:

- •Criminal activity.
- •Breaking the law.
- •Threats to health and safety.
- •Environmental harm.
- •Hiding any of the above.

3.Protected Disclosure:

•A worker is safeguarded from retaliation if their disclosure is made in good faith and under the correct legal circumstances.

Key Takeaways

•**Obligation of Confidence**: Arises through agreements like NDAs or implied trust.

•**Patent Protection**: Sharing ideas under confidentiality safeguards potential patents.

•**Whistleblowing Protection**: Employees exposing serious wrongdoing have legal rights under specific conditions.

•**Professional Knowledge**: General skills are not confidential and are excluded from these rules.

4. TRADEMARKS

What Are Trademarks?

•**Definition**: A trademark is any symbol, word, design, or packaging that helps people tell one product or service apart from another.
  •**Example**: Logos, brand names, and product shapes can all be trademarks.
  •**Legal Basis**: The Trademarks Act 1994 governs trademarks in the UK.

What Can Be a Trademark?

•**Words**: Including personal names.
•**Designs and Shapes**: Like logos or product packaging.
•**Letters and Numbers**: Example: "BMW" or "007."

Registering a Trademark

How It's Done:
•Trademarks can be registered through the UK Intellectual Property Office (UKIPO).
•Registered trademarks are listed in a searchable online database.
Why Register?
•Makes it easier to protect your brand from imitation or misuse.
•Helps combat software piracy by protecting brand identity on packaging and products.

Rules for Trademarks

What Can't Be Trademarked?
•Place names (e.g., "London").
•Common personal names (e.g., "John Smith") unless proven distinctive.
What's Illegal Under the Trademarks Act?
•Using someone else's trademark on products without permission.
•Selling, importing, or exporting items with an unauthorized trademark.
•Keeping goods with fake trademarks for sale or business purposes.

Passing Off

What is Passing Off?
•Passing off happens when a business tries to imitate the look or "feel" of another product to confuse customers.
•Example: Packaging that looks very similar to a well-known brand, even if the trademark isn't copied.
How It's Different from Trademarks:
•A registered trademark gives automatic protection.
•If a trademark isn't registered, the owner must rely on passing off claims in civil court to protect their brand.

Key Takeaways

•**Trademarks**: Protect symbols, logos, and designs that make products or services unique.
•**Registration**: Provides stronger legal protection and makes enforcement easier.
•**Passing Off:** Protects unregistered trademarks or the general appearance of a product if someone tries to imitate it.
•**Illegal Use**: Unauthorized use, sale, or trade of trademarks is prohibited.

DOMAIN NAMES

What Are Domain Names?

Purpose: Domain names are the website addresses people use to connect to specific online locations (e.g., www.example.com).
Management: A global organization called ICANN oversees domain names.
  •ICANN's Role: Ensures that a domain name always leads to the same website, no matter where you access it from.
  •ICANN assigns the job of managing domain names to other organizations that follow strict rules.

Why Are Domain Names Important?

•Originally created to help computers connect more easily on the internet.
•Now, businesses use domain names as part of their identity (e.g., to match their brand name or trademark).
•Domain names are often featured in advertising because they are easier to remember than technical computer addresses.

Domain Names vs. Trademarks

Trademarks:
•Registered in specific countries or regions.
•Can belong to different companies as long as they are in different industries or locations.
•Example: "Delta" can be an airline and a faucet company because they sell different products.
Domain Names:
•Globally unique: Only one company can own a specific domain name.
•Allocated on a first come, first served basis.

Conflicts Between Trademarks and Domain Names

•If multiple companies have the same trademark in different areas or industries, only the first one to register the domain name gets it.
•Example: Both an airline and a hardware company named "Delta" might want delta.com, but only the first to apply can use it.
•Domain names aren't directly tied to trademark laws, which can cause disputes between companies over who gets to use a particular name online.

Key Points

•Domain names are essential for online identity and branding.
•They are managed globally by ICANN and its delegates.
•Trademarks and domain names operate under different systems, leading to potential conflicts.
•Domain names are unique and assigned on a first-come, first-served basis, unlike trademarks, which can be shared across industries or regions.

Cyber Squatting: A Problem in Domain Name Registration

What is Cyber Squatting?

Definition: Cyber squatting happens when someone registers a domain name that is similar to a well-known trademark or brand name, with the intention of selling it to the actual trademark owner at a high price.

Why Does Cyber Squatting Happen?

•**Inconsistent Systems**: Since trademarks and domain names are managed by different systems, people can take advantage of these inconsistencies.
•**Profit Motive**: Cybersquatters register domain names that resemble popular brands, hoping the brand owner will pay a large sum to get it back.

How Does Cyber Squatting Impact Brands?

•**Confusion**: Some cybersquatters create websites that look like the official brand site. This can mislead customers and damage the brand's reputation.
•**Financial Losses**: The brand owner might have to pay a high price to recover the domain, even though they legally own the trademark.

Legal Protection Against Cyber Squatting

•**Laws**: For example, the Anti-Cybersquatting Consumer Protection Act (ACPA) in the U.S. helps trademark owners fight back.
•**How It Works**: If it can be proven that the cybersquatter intended to mislead or profit from the domain, legal action can be taken to get the domain back.

Key Points

•Cyber squatting involves registering a domain similar to a trademark with the intention to profit from it.
•It creates confusion for customers and damages a brand's reputation.
•Laws like the ACPA can help trademark owners recover domains if the cybersquatter's intent is proven.

WIPO Reports and Their Impact on Domain Name Disputes

WIPO Report I (1999)

Purpose: The World Intellectual Property Organization (WIPO) published a report in 1999, titled 'The management of internet names and addresses: Intellectual property issues'.
Recommendation: The report recommended that ICANN (Internet Corporation for Assigned Names and Numbers) implement a policy called the Uniform Domain Name Dispute Resolution Policy (UDRP).
Effectiveness: The UDRP was designed to handle disputes over domain names, particularly cyber squatting.
•**Outcome**: By 2001, over 3,000 complaints had been resolved through arbitration centers, with 80% of cases being successfully resolved.

WIPO Report II (2001)

Focus: In 2001, WIPO published a follow-up report, 'The recognition of rights and the use of names in the internet domain system'.
Issue Addressed: The report focused on conflicts between domain names and identifiers that are not trademarks.
•**Examples include:**
  •Personal names (e.g., people's names).
  •Geographic locations.
•These conflicts are more difficult to resolve than trademark-domain name disputes because there is no global system like trademarks to address such situations.

Use Cases of Domain Name Disputes

1.Tesla vs. Cyber Squatting (Tesla.com)
Background: For many years, Tesla Motors could not use Tesla.com because it was owned by a cybersquatter.
  •The squatter had registered the domain long before Tesla became famous.
  •Tesla had to use TeslaMotors.com instead.
Resolution: In 2016, Tesla acquired Tesla.com for an undisclosed sum, reportedly in the millions. The original owner was unwilling to sell the domain for a lower price.
2.Microsoft vs. MikeRoweSoft.com
Background: In 2003, a Canadian teenager, Mike Rowe, registered the domain MikeRoweSoft.com as a pun on his name.
  •Microsoft argued that the domain infringed on their trademark.
Resolution: After initial resistance, Microsoft and Mike Rowe reached a settlement.
•This case highlighted the challenge of balancing trademark rights with fair use and intent when the infringement may not be clear-cut.

Key Points

•**WIPO's Role**: WIPO has played an important role in addressing domain name disputes, particularly cyber squatting, through the UDRP.
•**Challenges**: While trademark-based disputes can be handled effectively, conflicts involving personal names or geographic locations are more complex.
•**Real-World Examples**: Cases like Tesla's acquisition of Tesla.com and Microsoft's dispute with MikeRoweSoft.com demonstrate the ongoing challenges in domain name management and the resolution of disputes.

Discussion

A novelist writes a book about space exploration. At the same time, an engineer develops a new kind of rocket engine that could revolutionize space travel.

Question1 :The novel is eligible for copyright protection. What specific parts of the novel would be covered under copyright law?
Ans: Copyright Protection for the Novel
A novel is a literary work, and under copyright law, the original expression of the work is protected. This includes:
•**The text** of the novel itself, including all the narrative, dialogue, and descriptions created by the novelist. The specific arrangement of words, phrases, and paragraphs are all part of the copyrighted work.
•**Original characters**: If the novel features original characters, their portrayal and development are also protected under copyright.
•**The plot and structure**: The specific storyline or the sequence of events within the novel, provided it's original and not copied from another source, is protected. This would include the novel's theme, setting, and how the story unfolds.
•**The setting**: The particular world or environment the novelist creates in the novel, as long as it's original and not a copy of pre-existing worlds or environments.
However, ideas, themes, or factual elements of the novel (such as space exploration itself) are not protected under copyright law. For instance, the general concept of space travel, or any scientific or factual concepts about rocket engines, is not protected. Only the specific expression of those ideas in the novel—like the author's unique description or world-building—is protected.

Question2: The rocket engine could be patented. How does a patent differ from a copyright in protecting the engineer's work?
Answer: Patent Protection for the Rocket Engine
A patent is a form of intellectual property that protects inventions—specifically, new and useful inventions, processes, or designs.
What can be patented?
The engineer's rocket engine could be patented if it meets the legal requirements for patentability:
  •**Novelty**: The rocket engine must be new and not have been previously known or used.
  •**Inventive step**: The rocket engine must involve an inventive step, meaning it is not obvious to someone skilled in the field.
  •**Industrial applicability**: The invention must be useful in industry or have a practical application, which the rocket engine clearly does.

Differences Between Patent and Copyright:
•**Scope**: Copyright protects expressions of ideas (the novel's text, characters, plot), while a patent protects the underlying invention (the technical design, function, and method of operation of the rocket engine).
•**Duration**: Copyright lasts for the life of the author plus a certain number of years (usually 70 years), whereas a patent provides protection for a limited period (usually 20 years) and is only available for inventions that meet the specific requirements.
•**Purpose**: Copyright encourages creativity and protects artistic expression, while patents incentivize innovation by protecting technical inventions and promoting their disclosure to the public.
What is protected by a patent?
The engineer's rocket engine would be protected by patent law in terms of:
•The mechanical design and how the components function together to create a novel and effective engine.
•Any new method or process for creating or operating the engine.

Unlike a copyright, which protects the expression (such as the novel's text), a patent protects the invention's functional aspects, ensuring that the engineer's specific technical design and methods cannot be copied without permission.

Summary of Key Differences:

Copyright: Protects the expression of ideas (the novel's writing, characters, plot) and lasts for the life of the author plus 70 years.
Patent: Protects inventions, such as the engineer's rocket engine, and lasts for up to 20 years from the date of filing, provided the invention meets the criteria of novelty, inventive step, and industrial applicability.
Both forms of intellectual property provide different types of protection suited to their respective domains—copyright for literary works and patents for technical inventions.

1.What are the advantages and disadvantages of each contract type for both the supplier and the client in this situation?

In a **fixed-price contract**, the supplier agrees to deliver the software for a pre-agreed cost regardless of the time and resources involved.
The main **advantage** for the client is that they know the total cost upfront, providing predictability and control over their budget.
However, the supplier bears the risk of cost overruns due to unforeseen challenges, which may incentivize them to cut corners. The disadvantage for the client is that they have less flexibility to change the project scope, as any additional features would likely require renegotiating the contract.

In a **time-and-materials contract**, the client pays for the actual time and resources spent on the project.
The main **advantage** for the supplier is that they are compensated for all their time and effort, with flexibility to adjust the scope as needed. For the client, this model allows for more flexibility in the project, enabling scope changes and adjustments without needing to renegotiate the entire contract.
However, the **disadvantage** is that costs can escalate without strict oversight, making it harder for the client to predict the final price.

2.Differentiate between fixed-price contracts and time-and-materials contracts in software development.

Fixed-price contracts involve a predetermined cost and scope, requiring detailed planning and limited flexibility.
Time-and-materials contracts charge based on resources and time spent, offering adaptability but with less predictability in cost.

3.Why might a client demand professional liability insurance in a consultancy project?

Professional liability insurance protects the client from financial losses due to the consultant's negligence or incorrect advice. It mitigates risks associated with critical decisions based on the consultant's recommendations.

4.How should the contract handle unexpected changes in requirements?

Include a change management clause detailing the process for handling scope changes, including submitting requests, assessing impacts, and revising costs and timelines. Specify pricing for out-of-scope work to ensure clarity and minimize disruptions.

5.How should the parties proceed with arbitration in case of multiple jurisdictions?

Arbitration should follow the contract's arbitration clause, detailing the resolution process for disputes. It may specify a location or arbitration body (e.g., International Chamber of Commerce). An arbitrator, ideally with technical expertise in software contracts, is chosen to ensure contextual understanding. The process involves written statements and an oral hearing for presenting evidence. The arbitrator's decision is typically binding, emphasizing the importance of drafting clear terms in the contract.

Data Protection, Privacy, and Freedom of Information

- **Background:**

  Public concern about data protection arose in the 1970s when it became evident that vast amounts of personal data were being collected, stored in computers, and used in ways that were not only unexpected but also potentially harmful. There were growing fears that this data could be accessed by unauthorized individuals, misused, or even manipulated. Moreover, the data might be outdated, incomplete, or incorrect, leading to further concerns about privacy violations and the potential for abuse.

Data Protection Act 1984

The public concerns about the collection and misuse of personal data in the 1970s prompted action, particularly in the UK and Europe. This culminated in the **Council of Europe Convention** on the matter. The first **UK Data Protection Act** was passed in 1984, and it was designed to address these concerns and to align with the provisions of the Convention.

Purpose of the 1984 Data Protection Act:

- **•Accuracy of Information:** The Act aimed to protect individuals from the misuse of inaccurate or incomplete personal information.
- **•Unauthorized Access:** It sought to prevent personal information from being accessed by unauthorized individuals or organizations.
- **•Purpose Limitation:** The Act also ensured that personal information could only be used for the specific purposes for which it was collected, preventing its use for unrelated or unapproved activities.

Progression of the Act

By the **mid-1990s**, the rapid growth of the **internet** created new challenges. The digital age made it easier to gather data about individuals' online behaviors, allowing organizations to create detailed profiles of personal habits. These profiles could be used for **marketing** purposes, but there were growing concerns about their potential misuse, including risks such as **blackmail**.

This new danger prompted further legislation to address emerging issues in data protection. The **European Directive on Data Protection (1995)** was introduced to provide a framework for handling personal data across member states. This, in turn, led to the adoption of the **Data Protection Act of 1998** in the UK, which aimed to modernize and strengthen the protections introduced by the 1984 Act.

The 1998 Act also took into account the challenges and risks presented by the **internet** and **digital technologies**, reflecting the need for greater control over personal information in a rapidly evolving technological landscape. This legislation reinforced the principles of data protection while expanding protections to include digital data and online activities.

Key Rules of Data Protection Laws (1984 - 1998)

1. **1.Data Collection and Use:** Personal data must be collected for **legitimate purposes** and not used for other purposes that were not disclosed when the data was gathered.
2. **2.Accuracy:** Personal information must be **accurate** and kept up to date. Inaccurate or outdated data must be corrected or erased.
3. **3.Data Security:** Personal data must be kept secure, preventing unauthorized access, disclosure, or modification of information.
4. **4.Access Rights:** Individuals have the **right to access** the personal data held about them, ensuring transparency and control over their own information.
5. **5.Accountability:** Organizations that collect and store personal data are held accountable for adhering to these principles and ensuring that data is handled in compliance with the law.

- ## Challenges in the Digital Age

The introduction of **digital technologies** and the **internet** presented new challenges, including:

- **•Data Profiling:** The ability to track individuals' behavior online and compile detailed personal profiles for targeted advertising and other purposes.
- **•Small, Shadowy Organizations:** The ease with which even small or poorly regulated organizations could gather and misuse personal data.
- **•Globalization of Data:** With the internet, data can cross borders easily, creating challenges in terms of jurisdiction and enforcement of data protection laws.

These challenges led to the introduction of newer frameworks, including the **General Data Protection Regulation (GDPR)** in 2018, which modernized and strengthened data protection across the EU, extending protections even further in the face of increasing digital activity and technological advancements.

–

- The **Data Protection Principles** outlined in the **1998 Data Protection Act** are essential for safeguarding personal data and ensuring that it is processed in a fair, lawful, and transparent manner. These principles provide clear guidelines for how data controllers must handle personal information.

  The 8 **eight Data Protection Principles**

  ### 1.1. Fair and Lawful Processing

  - Personal data must be processed fairly and lawfully. It cannot be processed unless specific conditions are met.
  - **•Condition for processing**:
    - **•Consent** from the data subject is one of the primary conditions.
    - •For **sensitive data**, explicit consent is required.
    - •Data can also be processed if there is a legal obligation or necessity.

  Data Protection, Privacy, and Freedom of Information

2. 2.Specified and Lawful Purpose

- •Data must only be obtained for specific, lawful purposes.
- •It cannot be used for other purposes that are incompatible with the original purpose for which it was collected.
- •**Data controllers** must inform the **Information Commissioner** of the purposes for which they are collecting data.

3. 3.Adequacy and Relevance

- •The personal data collected must be **adequate**, **relevant**, and **not excessive** for the purpose for which it is processed.
- •This ensures that only the necessary data is collected.

4. 4.Accuracy

- •Personal data must be **accurate** and, where necessary, kept up to date.
- •**Data controllers** are responsible for ensuring that the data is accurate. However, this can be challenging in some situations (e.g., keeping contact details for people who change addresses frequently).

5. 5.Retention

- •Personal data must not be kept longer than necessary for the purposes it was collected for.
- •**Data controllers** must determine the retention period and ensure that data is deleted when it is no longer required.
- •Some data may need to be kept for specific periods (e.g., financial data, legal requirements, or university records).

6. 6.Processing in Accordance with Data Subjects' Rights

- •Personal data must be processed in accordance with the rights of the **data subjects** (i.e., the individuals to whom the data relates).
- •This includes providing access to data, allowing corrections, and ensuring data is processed in line with legal requirements.

7. 7.Security Measures

- •Appropriate **technical** and **organizational measures** must be taken to prevent unauthorized or unlawful processing, accidental loss, or destruction of data.
- •This includes securing data with **access controls** (e.g., passwords), **backups**, **integrity checks**, and vetting personnel who have access to sensitive data.

8. 8.International Transfer

- •Personal data should not be transferred to countries outside the **European Economic Area (EEA)** unless the destination country offers **adequate protection** for the data.
- •This principle ensures that data subjects' rights are protected even when their data is transferred internationally.

These principles are designed to protect **individuals' privacy** while ensuring that personal data is handled responsibly and securely by organizations. Data controllers must comply with these rules, and failure to do so can result in penalties or legal consequences.

- The **1998 Data Protection Act** grants **data subjects** a range of rights designed to protect their personal information and ensure it is handled responsibly.

Rights of Data Subjects

Under the 1998 Act, **data subjects** (the individuals whose personal data is being processed) are granted several important rights:

1. **1.Right to Know**
    - •Data subjects have the **right to know** whether their personal data is being held by a data controller.
    - •If data is being held, data subjects have the right to access and obtain information about that data.
2. **2.Right to Receive Information**
    - •Data subjects are entitled to receive:
        - •A **description of the personal data** being held.
        - •An explanation of the **purpose** for which it is being processed.
        - •A list of the **people or organizations** to which their data may be disclosed.
        - •An **intelligible statement** of the specific data held about them.
        - •A description of the **source** of the data (i.e., where the data came from).
3. **3.Right to Rectify or Erase Data**
    - •If the personal data held is **inaccurate**, the data subject has the right to request its **correction** or **erasure**.
4. **4.Right to Prevent Processing**
    - •Data subjects have the right to prevent processing that could cause them **damage** or **distress**. For instance, they may stop certain uses of their data if they feel it may negatively impact them.
5. **5.Right to Prevent Direct Marketing**
    - •Data subjects can request that their data not be used for **direct marketing** purposes.
6. **6.Right to Compensation**
    - •If a data subject suffers damage (e.g., financial loss) due to the **unauthorized processing** of their personal data or a violation of the principles of the Act, they have the right to seek **compensation**.

- ### Scope of the Act

While the 1998 Data Protection Act grants extensive rights to data subjects, there are some **exceptions** and **limitations** to these rights, including:

1. **1.Exemptions from Subject Access**
    - •Certain conditions may prevent or limit the ability of data subjects to access their personal data:
        - •If disclosing the information would **infringe** someone else's rights (e.g., another individual's right to privacy).
        - •If the data consists of **references** given by the data controller (such as letters of recommendation).
        - •**Examination Results**: Data subjects (such as students) do not have the right to access their exam marks until after the results have been published.

2. **2.Exemption for Personal Data in Academic, Professional, or Other Examinations**

    - •Personal data related to **examination candidates**—such as information recorded during exams—may be exempt from the right of access until the results are made public.

These rights and exceptions ensure that **data subjects** are protected and have control over their personal information while also balancing the needs of organizations to process data for legitimate purposes. Organizations must comply with the Act, but there are specific situations where limitations to access or rights apply, typically in cases where disclosing the data could infringe upon other rights or privacy concerns.

- ## Privacy and Regulation of Investigatory Powers Act 2000

The **Regulation of Investigatory Powers Act (RIPA) 2000** establishes a legal framework in the UK for the surveillance and interception of communications. It is designed to control how law enforcement and security agencies access communications data, ensuring that such actions are carried out lawfully and only under specific circumstances.

Here's an overview of the key provisions of the Act as they relate to **privacy** and **monitoring communications**:

Key Provisions of the RIPA 2000:

1. **1.Lawful Interception of Communications:**

    - •The Act allows government security services and law enforcement authorities to intercept and monitor **computer, telephone, and postal communications**, but only under certain conditions such as crime prevention and detection.
    - •This **interception** can occur in specific situations where it is deemed necessary for national security, to prevent or detect crime, or for similar authorized purposes.
2. **2.Data Encryption:**

    - •The Act grants authorities the power to demand the disclosure of **data encryption keys**. This means that if an encrypted communication or data is intercepted, the authorities can compel the organization or individual responsible to provide the means to decrypt that data.
3. **3.Permitted Purposes for Monitoring Communications:**

    - •The Act permits organizations, including **Internet Service Providers (ISPs)**, **telecommunications providers**, and **employers**, to monitor and record communications without consent, but only for specific purposes. These include:
        - •**Establishing facts**: For example, verifying when an order was placed in an e-commerce transaction.
        - •**Ensuring compliance**: Monitoring communications to check if an organization's internal regulations and procedures are followed.
        - •**Setting standards**: To ascertain or demonstrate that standards (e.g., quality, customer service) are met.
        - •**Crime prevention and detection**: Both **computer-related crimes** (such as hacking) and other types of criminal activity.
        - •**Investigating unauthorized use** of telecommunication systems (e.g., illegal activities such as fraud or hacking).
        - •**Ensuring the effective operation** of systems: This could include monitoring communications to detect potential threats like **viruses** or **denial of service (DoS) attacks**.

- •**Distinguishing between business and private communications**: For example, an employer monitoring the emails of an employee on holiday to address urgent business matters.
- •**Monitoring confidential helplines**: Organizations may monitor calls to their confidential, counseling, or helplines, but only to ensure that users remain anonymous if they choose.

Privacy Considerations:

While RIPA 2000 enables a broad range of surveillance powers for security and law enforcement purposes, it also provides significant privacy protections for individuals and organizations:

- •The **purpose** of interception must be clearly defined (e.g., crime prevention, system maintenance).
- •The monitoring must be proportionate to the issue being investigated, and organizations must justify the necessity of monitoring in each instance.
- •Individuals are still protected under general privacy laws, such as those related to **data protection**, and must be informed when their communications may be monitored, where applicable.

However, there are some key **privacy concerns** regarding the scope of surveillance and the balance between national security, crime prevention, and individual rights to privacy. These concerns include:

- •**Transparency**: Organizations are generally not required to inform individuals that their communications are being monitored, particularly when the monitoring is for business-related purposes.
- •**Data misuse**: The collection and retention of communication data by organizations, especially without user consent, can raise issues related to how that data is stored and potentially misused.

In conclusion, the **RIPA 2000** establishes clear rules for the lawful interception of communications, aiming to balance privacy rights with the need for security and crime prevention. However, it highlights ongoing discussions about how to ensure privacy while maintaining the tools necessary for national security and law enforcement.

Freedom of Information Act: Key Features

The **Freedom of Information Act (FOIA)** is designed to promote transparency, accountability, and access to information held by public authorities. It provides the public with the right to access information held by bodies in the public sector, subject to certain exceptions. Below are the main features and provisions of the Act:

General Right of Access

- •The FOIA establishes a **general right of access** to information held by public authorities in the course of performing their public functions.
- •This right applies to a wide range of public bodies, including **government departments**, **local authorities**, **health trusts**, **universities**, **schools**, and other public sector organizations.
- •Any member of the public can make a request for information, and public authorities are required to respond to these requests.

Exemptions and Public Interest Test

- •While the FOIA grants broad access, there are certain **exemptions** to disclosure. These exemptions include matters related to national security, law enforcement, commercial interests, and personal privacy, among others.

- •However, even when information is exempt from disclosure, public authorities are still required to consider whether the **public interest** in releasing the information outweighs the need to keep it confidential.
    - •If the public interest favors disclosure, the information should be made available, despite being subject to an exemption.

Enforcement and Oversight Mechanisms

- •The FOIA creates the **Information Commissioner**, an independent office responsible for overseeing and enforcing compliance with the Act.
- •The **Information Commissioner** has the authority to investigate complaints and enforce the rights of individuals to access information.
- •In addition, an **Information Tribunal** was established under the Act to hear appeals against decisions made by the Information Commissioner or public authorities regarding information requests.

Publication Schemes

- •The FOIA imposes a **duty on public authorities** to adopt a **publication scheme**. This scheme must be approved by the Information Commissioner and must specify the types of information that the authority intends to make publicly available.
- •Public authorities must:
    - •Identify the **classes of information** they hold.
    - •State how the information will be published (e.g., online, in print, etc.).
    - •Indicate whether the information will be available for free or if a fee will be charged for access.
- •The publication scheme promotes proactive transparency, ensuring that much of the information is made available to the public without the need for formal requests.

Rights of Individuals

- •The public is granted the **right to request information**, and public authorities must respond to requests in a timely manner, typically within **20 working days**.
- •The Act applies to both **requested information** and information that is proactively published by public bodies.

• Key Exemptions Under the Act

Although the FOIA encourages transparency, some information is not automatically subject to disclosure:

- •**National Security**: Information that would harm national security.
- •**Law Enforcement**: Information that could prejudice law enforcement activities.
- •**Commercial Interests**: Information that could harm the commercial interests of an organization.
- •**Personal Data**: Information that would violate individual privacy under the Data Protection Act.
- •**Legal Professional Privilege**: Legal advice or communications covered by legal professional privilege.

In cases where an exemption applies, public authorities must still assess whether the public interest in withholding the information is greater than the public interest in disclosure. If the public interest favors disclosure, the information should be released.

Impact and Importance

- •The **FOIA** has enhanced the ability of the public to hold government and public authorities accountable for their actions by providing clear rights of access to information.
- •It promotes **openness** and transparency in public administration, which can improve public trust in government and public services.

- •The Act ensures that public authorities are not only reactive in releasing information but also proactive through publication schemes, which allows the public to access a wide range of data without needing to make individual requests.

Overall, the **Freedom of Information Act** plays a vital role in creating a more transparent, accountable, and democratic public sector by providing individuals with the tools to access information and ensuring that government actions are open to scrutiny.

1. **An online retailer collects personal information, including credit card details, during transactions. A hacker exploits a database vulnerability, accessing customer data, leading to complaints from customers.

Under the **Data Protection Act 1998** and **GDPR**, the retailer, as the **data controller**, must ensure the security of customer data. This breach violates the **seventh data protection principle**, which requires **appropriate technical and organizational measures** to protect data.

Key responsibilities include:
1. Implementing **access controls** (e.g., encryption, password protection).
2. Conducting regular **vulnerability assessments**.
3. Training employees on data security.

The retailer must notify affected customers.

2. **A health insurance company uses patient data, including medical histories, to develop an AI-based risk assessment model without explicit consent, arguing it's necessary for public health improvement.
Under the **Data Protection Act 1998** and **GDPR**, processing **sensitive personal data** (like health info) requires **explicit consent** or a legal exemption, such as processing for **public interest** (if properly documented). The company must ensure the processing is **proportionate** and does not infringe on the data subjects' rights.

To comply, the company should:
1. Obtain **explicit consent** from patients.
2. Conduct a **Data Protection Impact Assessment (DPIA)**.
3. Consider anonymizing or pseudonymizing data.

Non-compliance could lead to penalties and legal claims.

3. **A company monitors employee emails and internet usage to ensure compliance with workplace policies. An employee claims this violates their privacy under the Regulation of Investigatory Powers Act 2000 (RIPA).
Under **RIPA**, employers can monitor employees' communications for specific, lawful purposes, such as preventing unauthorized system use, ensuring policy compliance, or detecting crimes. However, monitoring must be **proportionate** and not infringe on privacy rights.

The employer must:
1. Inform employees about monitoring through a **privacy notice** or policy.
2. Specify what data is monitored, the purpose, and how it's used/stored.

Excessive or invasive monitoring (e.g., reading personal emails) without clear justification could lead to complaints to the **ICO** or legal action.

**4. **A university keeps records of all enrolled students, including their addresses and contact details, indefinitely. A former student argues that their data is no longer necessary and should be deleted.*
University can hold the data indefinitely. So it's fine.
In case, if it was not an university then under the **fifth data protection principle** of the Data Protection Act 1998, personal data should not be kept longer than necessary for its purpose.

For example
- **Financial records** must be kept for a minimum of seven years (for tax compliance).
- **Academic records** (e.g., degrees) may be retained indefinitely for verification.
- **Contact details** should be deleted once the student is no longer enrolled, unless there's a legitimate reason (e.g., alumni communications)

The university should conduct a **data audit** and implement a **data retention policy** to justify retention periods and delete unnecessary data. Non-compliance could lead to enforcement by the **ICO** or legal claims.

5. **A journalist submits a request under the Freedom of Information Act (FOIA) to a local council, asking for details about contracts awarded to private companies for waste management. The council refuses, citing commercial confidentiality.
The **Freedom of Information Act 2000** grants the public the right to access information held by public authorities, but this right is subject to **exemptions** such as **commercial interests** or **personal data**.

In this case, the council must show that withholding the information is necessary to protect commercial interests. However, the **public interest test** requires the council to disclose information if the public benefit outweighs the need for confidentiality, especially if the contracts involve public funds.

To challenge the refusal, the journalist can appeal to the **Information Commissioner's Office (ICO)**, which can investigate and potentially order the release of the information if the refusal is unjustified. This situation highlights the balance between transparency and protecting sensitive information.

6. **A UK-based company stores customer data on servers located in a country outside the European Economic Area (EEA) with weak data protection laws. A customer challenges this practice, claiming it violates their data protection rights.
Under the **eighth data protection principle** of the **Data Protection Act 1998**, personal data must not be transferred outside the EEA unless the receiving country ensures an **adequate level of protection**.

The company must demonstrate safeguards such as:
1. Using **Standard Contractual Clauses (SCCs)** or **Binding Corporate Rules (BCRs)** approved by the ICO.
2. Ensuring compliance with international frameworks like the EU-US Data Privacy Framework (replacing the EU-US Privacy Shield).

If the company cannot prove adequate protection, it must either move the data to EEA servers or obtain **explicit consent** from customers for the transfer. Non-compliance could lead to regulatory fines and reputational damage.

7. **A financial services company monitors employee emails and phone calls for compliance with anti-money laundering laws. An employee learns their personal emails were accessed and claims this violates their privacy rights and the GDPR. The company argues monitoring is necessary for regulatory compliance.
This scenario involves balancing **employee privacy** under **RIPA** and **GDPR** with the employer's compliance obligations.

Privacy Rights:
Under **RIPA**, monitoring is allowed for legitimate purposes, like ensuring regulatory compliance, but must be:
1. **Proportionate**: Monitoring should be limited to what is necessary.
2. **Transparent**: Employees must be informed about the monitoring scope and purpose.

Accessing personal emails without justification violates proportionality and employee privacy, unless there is explicit consent or a strong legal reason.

GDPR and Data Subject Rights:
Employees have the right to:
1. **Access their data** (Article 15).
2. **Rectify or erase** data if processed unlawfully (Articles 16 & 17).

The company must justify the monitoring under **Article 6** (lawful processing basis), such as compliance with anti-money laundering laws. If the monitoring was excessive, the employee can file a complaint with the **ICO** or take legal action.

Resolution:
The company should:
1. Limit monitoring to business-related communications.
2. Update the **employee monitoring policy** to ensure GDPR compliance.
3. Provide a detailed response to the employee's GDPR request, explaining the legal grounds for monitoring.

Internet Issues:

- **Benefits of the Internet**

  The internet has made life easier in many ways:

  - **Easy access to information**: We can quickly find all sorts of information online.
  - **Better communication**: People can communicate with each other more easily, whether one-on-one or in groups.
  - **Faster transactions**: Shopping, banking, and other commercial activities have become quicker and simpler.
  - **Wider availability**: These benefits are available to many people, not just a small privileged group, although internet access is still limited in some areas, even in developed countries.

  However, such a big development also brings its own set of problems.

- **Problems of Internet Availability**

  Different countries have laws about what can be shared or shown publicly. Here are some of the key issues caused by the internet:

  - **Defamation**: Spreading false information that harms someone's reputation.
  - **Sexual Content**: Offensive material, including pornography, that may not be acceptable in all cultures.
  - **Spam**: Unwanted emails or messages that flood users' inboxes.
  - **Political and Religious Comment**: Some countries restrict criticism of the government or religion.
  - **Violence**: Content that shows or encourages violence.

  These topics involve **social**, **cultural**, and **legal** concerns that can't just be talked about in technical terms. Different countries deal with these issues in different ways, but the internet doesn't have borders, so content from one country can easily affect others.

  For example:

  - Some countries find images of women in revealing clothes inappropriate and ban them in ads and publications, while in other countries, such pictures are fine.
  - Some nations don't allow any criticism of their government or religion, while others strongly protect the right to express such opinions.

- **The Role of the Internet in These Issues**

  - The rise of the internet (and satellite TV) has made these cultural and legal differences more noticeable and important.
  - Since content easily flows across countries, material that breaks local laws can enter a country easily, and it becomes harder to enforce local laws.
  - The role of **Internet Service Providers (ISPs)** is central in dealing with these issues, so it's important to understand the laws governing them.

- **Internet Service Providers (ISPs)**

  The main question is: **How responsible should ISPs be for what their customers post online?**

  In Europe, the rules are set by the **European Directive 2000/31/EC**, which the UK follows through the **Electronic Commerce (EC Directive) Regulations 2002**. According to these rules, an ISP can play three roles:

1. **Mere Conduit**: This means the ISP only helps transmit data but doesn't create, change, or select the content being shared.
2. **Caching**: ISPs temporarily store data to help speed up its delivery.
3. **Hosting**: The ISP stores data for users, like a website hosting service.

For the **mere conduit** role, the ISP just sends the data from one place to another and doesn't interfere with it. It is okay for the ISP to store the information briefly as part of this process, as long as it is not modifying the data or deciding who gets to see it.

Caching

The **caching role** happens when an ISP temporarily stores information to make it faster and more efficient to transmit to other users who request it. If an ISP is acting as a **cacher**, it is not responsible for any damage or legal issues arising from this storage, as long as it follows these rules:

- It does not change the information.
- It allows proper access to the information.
- It updates the information according to industry standards.
- It does not interfere with legal ways of tracking how the information is used.
- If the ISP knows that the original information has been removed or blocked (either by the source or a legal authority), it must quickly remove or block access to that cached information.

Hosting

When an ISP **hosts** information (i.e., stores content provided by its customers), it is not responsible for any damages or legal problems if:

- The ISP did not know that unlawful activity was happening.
- If someone claims damages, the ISP didn't know anything that would suggest unlawful activity.
- Once the ISP becomes aware of unlawful activity, it must act quickly to remove the information or stop access to it.
- The customer posting the content was not acting under the ISP's control or direction.

ISP Responsibilities

An ISP should **lose immunity** from legal responsibility if it fails to remove unlawful material after being informed about it.

Another issue is **anonymous or pseudonymous postings**. Many users of online platforms use fake names or aliases. The ISP knows the real identity of these users. The question is whether the ISP can release this information to someone who wants to take legal action against the user, or if it can be forced to release this information under legal pressure.

Law Across National Boundaries

1.Criminal Law

- **1. Extradition Treaty:** If someone commits a crime in one country (Country A) and then moves to another country (Country B), **Country A** can request the person's arrest in **Country B** to face trial, but only if there's an **extradition treaty** between the countries. The crime must also be considered a crime in both countries.
- **2. Extraterritorial Jurisdiction:** Some countries, like the **UK** and the **USA**, have **extraterritorial jurisdiction**, which means they can prosecute people for crimes committed in other countries. This is often used for serious crimes like sexual offences involving children committed abroad.
- However, in general, someone can't be prosecuted in **Country B** for a crime committed in **Country A**, unless the countries have agreed on specific terms or one claims extraterritorial rights.

Internet Crime

- If you live in **Country A** and publish something online that's legal in **Country A** but illegal in **Country B**, you can't be prosecuted in **Country A**. It's also unlikely you'd be extradited to **Country B** unless you travel there. However, it's still risky to visit **Country B**, as the authorities may act if you're within their borders.

2.Convention on Cybercrime

- In 2001, the **Council of Europe** introduced the **Convention on Cybercrime**, which targets internet crimes like online fraud, hacking, and child sexual abuse material. While the convention aims to create international laws for cybercrimes, it takes time to be enforced. Governments must sign and then **ratify** the convention before it becomes part of their domestic laws.

3.Civil Law

- Suppose an **ISP** (Internet Service Provider) based in the **USA** has a customer from **Italy**, who posts an accusation about a **French politician** on the ISP's website, which the politician finds offensive. The politician could theoretically sue in **Italy**, **France**, **England** (where the ISP has a branch), or the **USA**.
- In this case, **France** might be the best place to file the case, but if the ISP doesn't have a legal presence there, it might not help. The person seeking action will likely pursue the case in the country with the strongest legal presence or connection to the case.

Defamation

Defamation refers to making statements that harm someone's reputation, cause them to be disliked, or bring them into contempt.

In **England and Wales**, defamation is divided into two types:

- **Slander**: Spoken defamation.
- **Libel**: Written or recorded defamation.

Possible Defences Against Defamation

There are several possible defences if you're accused of defamation:

1. **Not the Author, Editor, or Publisher**: The defendant wasn't responsible for making or publishing the statement.
2. **Truth**: The statement is mostly true.
3. **Opinion**: The statement was a personal opinion, and the basis for the opinion was made clear.
4. **Public Interest**: The statement was made in the public interest.

5. **Website Operator**: If the statement was posted on a website, the website operator may not be responsible for it.
6. **Peer-Reviewed Journal**: The statement was published in a peer-reviewed scientific or academic journal.
7. **Privilege**: The statement was part of an official report (e.g., a court report) that is protected by privilege.

- ### The Defamation Act 2013

Before 2014, **UK law** allowed anyone to bring a defamation case if their reputation was harmed. However, the **Defamation Act 2013** changed this. Now, for a defamation case to be valid, it must show that the statement caused or is likely to cause **serious harm**—typically involving significant financial loss.

- ### The Internet Content Rating Association (ICRA)

The **Internet Content Rating Association (ICRA)** is an independent international organization. Its goal is to help parents protect children from harmful content on the internet while also respecting the freedom of expression for content creators. The board of ICRA includes representatives from major companies in the internet and communications industries, such as AOL, BT, Cable and Wireless, IBM, Microsoft, and Novell.

- ### Spam

Spam refers to **unsolicited email** sent to recipients without their consent. It is typically sent in bulk, with little or no effort to target recipients who may be interested in the content of the email.

- ### Stopping Spam

There are several technical methods to help fight against spam, including:

1. **Closing Loopholes**: Preventing spammers from using other people's computers to send bulk messages.
2. **Machine Learning**: Using algorithms to identify suspicious patterns in email headers.
3. **Virus Detection**: Using antivirus software to block emails that may contain harmful viruses.
4. **Stop Lists**: Maintaining lists of websites known to send spam, to help block them.

- ### European Legislation: Privacy and Electronic Communications

The **European Community Directive on Privacy and Electronic Communications (2002/58/EC)**, issued in 2002, required member countries to introduce regulations by December 2003. In the UK, it was implemented through the **Privacy and Electronic Communications (EC Directive) Regulations 2003**.

Key Features:

- **Consent for Unsolicited Email**: Unsolicited emails can only be sent to individuals (not companies) if they have given their consent beforehand.

- **Clear Sender Information**: Sending unsolicited emails that hide the sender's address or do not include a valid address for the recipient to request to stop receiving such emails is illegal.
- **Use of Email for Direct Mailings**: If a seller obtained an email address during the sale of goods or services, they may use it for future direct mailings. However, each email must give the recipient an easy and free way to request that further mailings stop.

Legislation in the USA: The CAN-SPAM Act

The **CAN-SPAM Act** (Controlling the Assault of Non-Solicited Pornography and Marketing Act), passed in 2003 and effective in 2004, is the U.S. equivalent, but it has some notable weaknesses.

Key Features:

- **Permission Not Required**: The Act allows spam to be sent as long as the sender has not been informed by the receiver that they do not wish to receive it, and the spam includes an address for the recipient to request that no more spam is sent.
- **ISP Rights to Sue**: Internet Service Providers (ISPs) can sue spammers for damages. In 2005, Microsoft won a $7.8 million civil judgment against a spammer, and other ISPs have similarly taken successful legal action.

Registration for Do-Not-Call and Anti-Spam Schemes

Both the **USA** and the **UK** have systems allowing people to register their telephone numbers to avoid unsolicited direct marketing calls. These systems are effective because telephone operators maintain records of calls, making it easy to track down and stop illegal marketing calls.

However, **email communication** is more difficult to track. The internet often doesn't charge by individual communication (like email), but rather by data transfer limits, making it harder to identify and regulate spam. Additionally, spammers can use **spoofing** (forging the sender's email address) and **relaying** (sending emails through other people's mail servers) to evade detection.

Cookies and User Tracking

- **What Are Cookies?**
  Cookies are small pieces of data stored in a browser when a user visits a website. They can be used by the website to store information like login details or to track site usage for analytics. Some websites also use **third-party cookies**, which track users across different websites.

- **Legal Requirements Under PECR**
  The **Privacy and Electronic Communications Regulations (PECR)** require websites to inform users that cookies are being used and to offer an option to accept or decline them. If a user refuses cookies, it might affect the website's functionality, as some features may rely on them.

- **Cookie Notifications**
  Following the PECR, websites that use cookies have begun including messages to inform users, with

options to accept or decline cookies being stored in their browser.

The Computer Misuse Act 1990

The **Computer Misuse Act 1990** introduces three main criminal offences related to computer security:

1. **Unauthorized Access to a Computer**
   Gaining access to a computer system without permission.

2. **Unauthorized Access with Intent to Commit a Serious Crime**
   Gaining unauthorized access with the intent to carry out a crime, such as theft or blackmail.

3. **Unauthorized Modification of Computer Data**
   Making changes to data or software on a computer without permission.

Key Sections of the Act

- **Section 1: Unauthorized Access to a Computer**
  A person commits an offense if they cause a computer to perform any action to access programs or data on another computer without permission. This is illegal even if the person only intends to access data without causing damage.

- **Section 2: Unauthorized Access to Commit a Serious Crime**
  This section targets those who access computer systems to carry out crimes. Examples include:
  - A blackmailer accessing medical records to identify high-profile individuals to blackmail.
  - A terrorist trying to access air traffic control systems to cause accidents.
- **Section 3: Unauthorized Modification of Computer Contents**
  A person commits an offense if they intentionally modify computer data or programs in a way that harms the system or data. This could include:
  - Spreading viruses or worms.
  - Ransomware attacks, where data is encrypted and a ransom is demanded for the decryption key.
  - Redirecting browser homepages without consent.
  - Installing programs that connect to premium-rate services without the user's knowledge.

These offenses aim to prevent malicious activities that could damage or disrupt computer systems and networks.

Computer Fraud

Definition of Computer Fraud
The Law Commission defines computer fraud as actions that involve manipulating a computer to dishonestly obtain money, property, services, or other valuable advantages, or to cause a loss. Essentially, it refers to using a computer in a dishonest way to gain something of value or to cause harm.

Examples of Computer Fraud
Computer fraud can involve:

- **Obtaining money or property** dishonestly using computer systems.
- **Causing financial loss** or other damage to individuals or organizations through computer manipulation.

• Fraud Techniques

Old Tricks with New Technology
Many fraud techniques used in computer fraud are actually much older and were used before computers existed. Some of the common examples include:

- **Fictitious employees**: Adding fake employees to a company's payroll and siphoning off their wages.
- **False supplier accounts**: Creating fake supplier accounts and generating false invoices to steal money.

These fraudulent methods remain common, even though they now rely on computers for execution.

• Computer Crime (Cybercrime)

Definition of Computer Crime
Also known as **cybercrime, e-crime, electronic crime,** or **hi-tech crime,** computer crime refers to any illegal activity that involves the use of a computer or network. This can include a variety of actions, such as:

- **Hacking**: A computer user (often referred to as a hacker) illegally accesses a company's or individual's private data.
- **Stealing information**: Gaining unauthorized access to sensitive or private information for personal gain.
- **Malicious activities**: In some cases, criminals may destroy, alter, or corrupt data intentionally.

Computer crimes can range from simple information theft to more complex and damaging activities like causing a company to lose data or shutting down systems entirely.

1. **A UK individual posts defamatory content about a French politician on a website hosted by a US-based ISP. The French politician demands removal, but the ISP refuses to act without a court order. The ISP receives a French court request for the poster's identity.**

-**Defamation and ISP Liability**: Under UK law, ISPs are not liable for user-generated content unless they are aware of its unlawfulness and fail to act.
If the ISP is informed of the defamatory content, it must act quickly to remove it.

-**Releasing the Identity**: ISPs can only release user info if required by a court order. The French court's request presents jurisdictional issues since the ISP operates under US law, but cross-border frameworks like the **Convention on Cybercrime (2001)** may apply.

****Resolution:**
- The ISP must act promptly if the content is proven defamatory.
- The politician can pursue legal action in the UK or France, depending on the ISP's legal presence.
- The ISP should follow formal legal processes for releasing user info to protect privacy.

2. **An e-commerce website using third-party cookies for targeted advertising receives complaints from EU users, stating the site doesn't inform them about cookies or allow opting out. The website's US operations claim compliance with local laws and argue no changes are needed.**

- EU Regulations: Under **PECR** and **GDPR**, the website must:
1. Inform users about cookies.
2. Obtain explicit consent for non-essential cookies

Failure to comply risks violations of EU privacy laws, including fines up to €20 million or 4% of annual turnover.

- **US Regulations****: While the **CCPA** allows more flexibility, it still requires transparency and an opt-out option for users.

The website needs to adopt a **geolocation-aware approach**, ensuring compliance with EU laws for European users while adapting to US regulations for global consistency. Ignoring these requirements could lead to reputational damage and legal consequences.

3. **A social media platform hosts a user post accusing a public figure of corruption. The public figure sues, claiming the platform failed to remove the post after multiple complaints. The platform argues it isn't liable since it didn't create the content.**

Under the **Electronic Commerce (EC Directive) Regulations 2002**, platforms are generally not liable for user-generated content unless they have knowledge of unlawful material and fail to act. Once notified of defamatory content, the platform must act **quickly** to remove it.

The **Defamation Act 2013** requires proof of "serious harm" to reputation. If the post caused harm, the public figure has a case. The platform's liability depends on whether it acted on complaints promptly.

To reduce risks, the platform should implement an effective **content moderation system** to address complaints swiftly.
Failure to act could lead to legal penalties and reputational damage.

4. **A payroll manager at a company manipulates the payroll system to create fictitious employees and divert funds to personal accounts. The fraud is discovered after significant financial losses. The company blames inadequate external security, while investigators point to poor internal controls.**

This case involves **computer fraud**, as outlined in the **Computer Misuse Act 1990**, where the payroll manager's actions of unauthorized access and data modification violate **Sections 1 and 3** of the Act.

The main issue is **inadequate internal controls, including:**
1. Lack of separation of duties (one employee had complete control over the payroll system).
2. No regular audits to detect discrepancies in payroll.
3. Absence of multi-factor authentication or role-based access controls.

To prevent such fraud, the company should:
1. Strengthen internal policies by segregating key responsibilities.
2. Implement **real-time monitoring systems** to detect unusual activity.
3.Conduct regular **external audits** to identify fraudulent behavior.

5. **A ransomware attack from Country A targets financial institutions in Country B, encrypting their data and demanding cryptocurrency payments. Country B identifies the attackers but cannot prosecute them locally because they reside in Country A, which lacks cybercrime laws and refuses extradition.**

This case illustrates the difficulties of **cross-border cybercrime** and the challenges of prosecuting attackers when countries have differing laws or lack cooperation. Since Country A has no cybercrime laws and refuses extradition, Country B faces obstacles in prosecuting the criminals locally.

To address this, Country B can:
1. Use **diplomatic channels** to encourage Country A to prosecute the criminals locally.
2. Collaborate with other countries to impose **sanctions** or penalties on jurisdictions that harbor cybercriminals.
3. Strengthen **cyber defenses** and implement better reporting systems to deter future attacks, including international data-sharing agreements.

This highlights the need for **global harmonization** of cybercrime laws and treaties to close jurisdictional gaps and enhance cooperation in tackling cybercrime.

6. **A company's employees receive a surge of phishing emails disguised as internal communications. Several employees click malicious links, exposing sensitive data. The attackers are traced to a spam operation in another country.**

Phishing emails are governed by **spam laws** and anti-fraud statutes, including the **Privacy and Electronic Communications Regulations (PECR)** and **GDPR** in the EU, and the **CAN-SPAM Act** in the US. These laws require senders to:
1. Avoid deceptive headers or subject lines.
2. Provide accurate sender details and opt-out options.

The company's vulnerability lies in **insufficient employee training** and weak email security. To prevent future incidents:
1. Implement **cybersecurity awareness training** for employees to detect phishing.
2. Use advanced **email filtering tools** to block suspicious emails.
3. Adopt **multi-factor authentication** for sensitive systems.

Though the attackers are in another country, **international agreements** like the **Convention on Cybercrime** may assist in investigations, but enforcement depends on cooperation between jurisdictions.

7. **A US-based streaming platform provides sexually explicit content that complies with US First Amendment protections but violates the UK Obscene Publications Act 1959. UK authorities issue a takedown notice, which the platform refuses, citing US law. Separately, the Internet Watch Foundation (IWF) reports child abuse material on the platform, triggering an international investigation.**

This case highlights **jurisdictional conflicts** in regulating pornography:
1. **UK Law**: The **Obscene Publications Act 1959** prohibits distributing content that could "deprave and corrupt." The platform violates UK law by hosting such content.
2. **US Law**: The **First Amendment** protects free speech, limiting regulation of explicit material unless it involves child abuse or illegal content.
3. **IWF Action**: Reports of **child abuse material** escalate the case internationally. Platforms must adhere to global agreements, such as the **Convention on Cybercrime**, to address such violations.
4. **Child abuse material** is universally illegal, and platforms are required to remove it regardless of the country in which they operate.

To resolve, the UK can work through **Interpol** or pressure the platform's hosting ISPs, leveraging **international cooperation** to ensure the removal of illegal content and protect child welfare.