

- Professionalism:
  - Code of ethics will govern the activities of a professional
  - These codes will be enforced by the profession and acknowledged and accepted by community
  - Certification by governing body
  - Level of proficiency or competency (measured by set standard & achieved by completion of course)
  
- Ethics: is the principles of right & wrong that individuals use to make choices that govern their behaviour.
  
- For people part of the Australian Computer Society our code of professional conduct/ethic identifies six values and associated requirements for professional conduct
  - Primary Interest of public:
    - Place the interest of public above those of personal, business or sectional interests.
  - The enhancement of quality of life:
    - Strive to enhance quality of life of those affected by your work
  - Honesty:
    - You are honest in your representation of skills, knowledge, service, and products
  - Competence:
    - You will work completely and diligently for your stakeholders
  - Professional development:
    - You will enhance your own professional development & that of your staff
  - Professionalism:
    - You will enhance the integrity of ACS and respect of its members for each other
  
- A professional will be needing to keep different types of relationship in a working environment.
  - Professional & client: So this relationship is where professional will provide a service for compensation. Issues
    - Client makes decision against your advice
    - Conflict of interest in professional (recommending product and professional gets money)
  - Professional & employer: this is a complex but most regulated. Condition of employment + expectation + responsibilities are normally well laid out. Conflicts:
    - Privacy
    - Whistleblowing
    - Piracy
  - Professional & Supplier: Is where innovation and cost effectiveness are enhanced when there is a good working relationship. Conflict
    - Contract negotiation.
  
- Ethical Organisation Characteristics:
  - Obey all laws and regulations
  - Honour contracts with: employees, customers, and suppliers

- Maintain occupational health & safety
- Support the development of employee's skill
- Categories of cybersecurity are:
  - Data security: Unauthorised access to data
    - Affects the confidentiality, integrity, and availability of information.
  - System security: attacks on resources by malicious computer programs (may be minor announce to individual computers)
  - Network security: attacks on network & infrastructure
- Organisation orientation to ethics:
  - Survivalist: focus is on profit, financial survival, and conquest. Disregard rules & laws
  - Paternal: focus on profit aswell but has developed who's on our side. Disregard rules & laws
  - Ordely: orderly structure + tradition. Laws and reg honour but in literalist way
  - Participative: honours laws and look for principle behind laws.
- Cloud computing: Is on demand network access to shared resources. Characteristics:
  - On demand self-service: no need for human interaction with service providers to access computing facilitates
  - Broad network access: can use nearly any computer device for network
  - Measured service: resource usage can be monitored, controlled, reported both to consumers + providers
- Benefits of cloud computing:
  - Reduce costs: since we are using a pay for use model instead of paying for capital cost
  - Making individual more productive: information is also available when/where needed
  - Facilitate collaboration: group of people can collaborate & share resources information and processes.
- Negatives of cloud computer:
  - Reliability: outages in cloud server will hurt business functioning
  - Legacy IT system: A lot of old It systems may not be able to be transferred to cloud without effort in simplifying
  - Regulatory and legal environment: so vendors must follow rules of the country they host In
- BYOD: Bring your own device. And use equipment for work
  - Benefits:
    - More productive since they are use of set up.
    - Employee satisfaction
  - Negatives:
    - Security: since data is on their device. And the organisation has no control over the security of device. And if lost
    - Relying on workers to bring their device all the time

- Higher cost potentially: since it may cost money to make sure their device is compatible with device used.