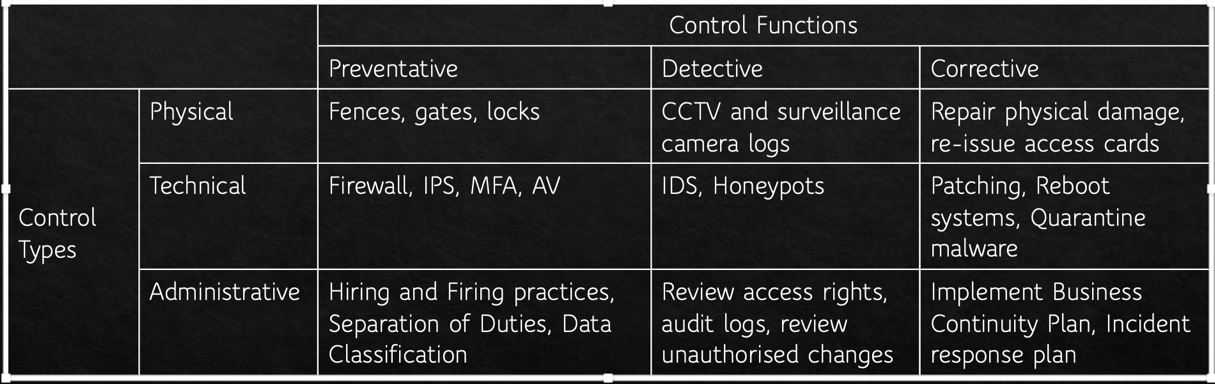
**Computers including cyber concepts in week 1 and lab 3**

# Cyber concepts in week1

* **Information CIA**: Confidentiality, Integrity and Availability. CIA is sometimes extended to include Authentication, Accountability, Non-Repudiation and Reliability
* **Confidentiality:** The property of information security that information is not made available or disclosed to unauthorised individuals, entities, or processes
* **Integrity:** Protects the reliability and correctness of data. Prevents unauthorized alterations of data. Protection against errors as well as deliberate changes
* **Availability:** Authorized subjects get timely and uninterrupted access to objects (the data and information they need)
* **Asset**: Anything of value to an organisation whose loss, or degradation of function would cause the organisation economic loss. Eg files, programs, databases, disks, laptops etc
* **Vulnerability**: weakness in an organisation’s assets that when exploited will lead to economic loss
* **Threat**: anything that can exploit a vulnerability in a way that leads to a negative impact
* **Risk:** the probable frequency and probable magnitude of future loss from a threat acting on a vulnerability.
* **Threat Actor**: Person, group or external force responsible for threats. External actors can be environmental: earthquakes, fire, flood, wind, etc. Internal actors may have motivation that is malicious or simply error
* **Threat Action**: What the threat actor did or caused e.g. malware, hacking, social, etc
* **Control**: measures that mitigate a risk. Types: physical, technical, administrative. Can be: Preventive, Detective, Corrective. Also known as a safeguard, security control, countermeasure, mitigation
* Once a risk has been identified, it can be: Reduced or mitigated; Assigned or transferred; Accepted; Deterred; Avoided; Rejected or ignored
* **Subject:** an entity such as a person, software process, computer, device that can access an object
* **Object**: an entity that provides information to a subject. eg files, databases, programs, storage media, processes
* **Identity** is about being able to prove to a system that you are who you say you are
* **Authentication** verifies the identity using authentication factors: Passwords, Smartcards, Tokens, Biometrics; 2FA (Two Factor Authentication): Something you know/have/do/ somewhere you are
* **Identity Management Systems** manage accounts and implement authentication schemes
* **Authorization**: Determines what actions a subject can carry out on an object
* Computer systems most commonly: Read, Write, eXecute; CRUD: Create, Read, Update/Insert, Delete
* other **access control schemes**: Discretionary Access Control (DAC); Mandatory Access Control (MAC); Role-Based Access Control (RBAC); Rule-Based Access Control; Attribute Based Access Control
* **Accountability**: To be able to identify all relevant information regarding actions in a system. Relies on identity and authorisation. Implemented with monitoring and logging
* **Risk Analysis**
* **Qualitative**: Assess risk in terms of rating risk on a scale
* Although simpler, it is not granular and so loses usefulness because of that
* How do you know what High, Medium, Low or 3.5/5 means? How much will you lose if you have a loss? How much will you spend to control this risk?
* **Quantitative**: Work out numbers for frequency of risk events based on detailed understanding of assets, threats and vulnerabilities
* More complicated. Needs maturity and access to detailed organisational information
* Asset Valuation AV; Exposure Factor EF %; Single Loss Expectancy SLE = AV \* EF; Annualized Rate of Occurrence ARO %; Annualized Loss Expectancy ALE = ARO% \* SLE; Cost/Benefit of countermeasures
* **Threat Analysis**: Who is the attacker; Why are they attacking; How are they attacking
* **Threat models:**
* PASTA: Process for Attack Simulation and Threat Analysis
* STRIDE (Microsoft) Threats related to software: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
* Attack Trees: Describe the steps needed for a threat to be actioned in a tree structure
* Hybrid Threat Modeling Model: (SEI): Persona non Grata
* **Vulnerability Assessment**
* Can be found through 3rd party information: US National Vulnerability Database; CVE (Common Vulnerability Exposures);CERTs (Computer Emergency Readiness/Response Team);VulnDB
* Identify vulnerabilities through: Asset management: what software, versions and patch levels; Vulnerability scans; Penetration Tests
* **Control examples**
* 

# Lab3 Linux

* Linux command
* pwd: print working directory
* ls -al：list all the contents and in a long version
* cd: change directory
* touch: create new file
* cp: copy file. cp file1 file2
* mv: rename file. mv file1 file2
* rm: delete file
* find: find <starting directory> -name <file to find>
* ps -AF: shows all processes and extended information
* kill -9 280: force the process with PID 280 to stop
* whoami: get the currently logged in user
* cat /etc/group: list all of the groups on the computer. the passwd file will list all of the users of the system
* chmod u+x file: To mark a program as being executable for a user
* -rwxrw-r-:
* - means it is a regular file. Other possible characters include d for directory, l for symbolic link
* Owner Permissions (rwx): owner of the file can read write execute
* Group Permissions (rw-): the group that the file belongs to can read and write
* Other Permissions (r-): other users who are not the file owner or part of the group can only read
* Linux file system
* /: the root directory and only the user root has access to write in this directory. The user root's home directory is /root.
* /bin: contains user binary executables like ps, ls, ping, grep etc. it is a symbolic link to /usr/bin
* /sbin: contains system binaries like iptables, reboot, fdisk, ifconfig, etc.
* /etc: contains configuration files and scripts for services running on the system. Also contains the passwd and shadow files that contain user and password information.
* /dev: contains device files that are the interface with physical devices on, or attached to, the system such as tty devices /dev/tty1.
* /proc: contains files that store information about system processes like uptime for example.
* /var: contains files like logs (/var/logs), backups (/var/backups), mail (/var/mail) and spool (printing; /var/spool). There is also a /var/tmp directory that can be used to run programs out of. This directory does survive reboots however. The directory /var/www/html is often used as the root directory of the web server.
* /tmp: contains temporary files as mentioned previously. Files get deleted on reboot.
* /usr: contains user binaries, libraries, documentation and source code
* /usr/local: contains users programs that you install from source.
* /home: contains user home directories
* /boot: contains boot loader files
* /lib: contains system libraries
* /opt: contains optional add-on applications
* /mnt: is a location for mounting temporary filesystems
* /media: is a location for mounting removable media devices like CDs
* /srv: contains specific service related data
* Users have a home directory which in Windows is usually located in c:\Users, on the Mac it is /Users and on Linux it is in /home. On this container, it will be empty because we only have one user, root, whose home directory is /root