Welcome to the Third Chapter.

Domain 3: What we will be covering.

- **Physical Controls:**

  Locks, fences, guards, dogs, gates, bollards, ...
- **Technical Controls:**

  Hardware/software/firmware – Firewalls, routers, encryption, ...

Access Control Categories and Types:

- **Access Control Categories:**

  Administrative (Directive) Controls:
  - Organizational policies and procedures.
  - Regulation.
  - Training and awareness.

  Technical Controls:
  - Hardware/software/firmware – Firewalls, routers, encryption.

  Physical Controls:
  - Locks, fences, guards, dogs, gates, bollards.

- **Access Control Types** (Many can be multiple types – On the exam look at question content to see which type it is).

  Preventative:
  - Prevents action from happening – Least privilege, drug tests, IPS, firewalls, encryption.

  Detective:
  - Controls that Detect during or after an attack – IDS, CCTV, alarms, anti-virus.

  Corrective:
  - Controls that Correct an attack – Anti-virus, patches, IPS.

  Recovery:
  - Controls that help us Recover after an attack – DR Environment, backups, HA Environments.

  Deterrent:
  - Controls that Deter an attack – Fences, security guards, dogs, lights, Beware of the dog signs.

  Compensating:

  Controls that Compensate – other controls that are impossible or too costly to implement.

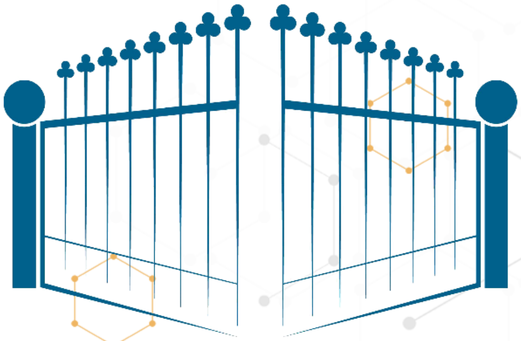
Physical Security Controls:

- **Perimeter defense:**

Fences (Deterrence, Preventative):

- Smaller fences such as 3ft. (1m) can be a deterrence, while taller ones, such as 8ft. (2.4m) can be a prevention mechanism.
- The idea of the fences is to ensure entrance/exits from the facility happen through only a few entry points (doors, gates, turnstiles).

Gates (Deterrence, Preventative):



- Placed at control points at the perimeter.
- Used with the fences to ensure access only happens through a few entry points.
- **ASTM Standard:**
  - □ Class I Residential (your house)
  - □ Class II Commercial/General Access (parking garage).
  - □ Class III Industrial/Limited Access (loading dock for 18-wheeler trucks).
  - □ Class IV Restricted Access (airport or prison).

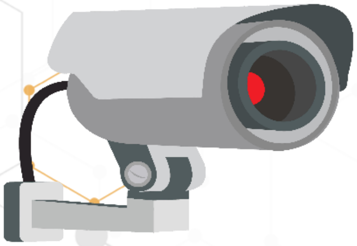
Bollards (Preventative):

- Used to prevent cars or trucks from entering an area while allowing foot traffic to pass.
- Often shops use planters or similar; it looks prettier but achieves the same goal.
- Most are static heavy-duty objects, but some cylindrical versions can also be electronically raised or lowered to allow authorized traffic past a "no traffic" point. Some are permanent fixtures and can be removed with a key or other unlock functions.

Lights (Detective and Deterrence):

- Lights should be used to fully illuminate the entire area.
- Lights can be static, motion activated (static) or automatic/manual Fresnel lights (search lights).
- Measured in lumen - 1 lumen per square foot or lux - 1 lumen per square meter more commonly used.

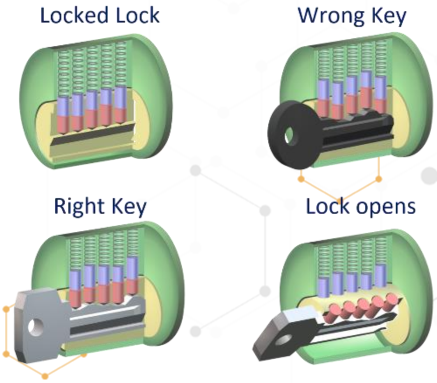
CCTV (Closed Circuit Television) (Detective, Deterrence) - used to monitor the facility's perimeter and inside it.



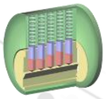
- **Older cameras** are analog and use video tapes for storage (often VHS); quality is often bad, unclear.
- **Modern cameras** are digital and use CCD (Charged Couple Discharge); also use a **DVR** (Digital Video Recorder).
- Organizations may have retention requirements either from policies or legislation that require a certain retention of their video (this could be bank ATM, data center or entry point footage).
- Cameras can be either static or non-static (automatic or manual).

- □ We have all seen the spy or heist movies where they avoid them by knowing the patterns and timers.
- □ This risk can be mitigated with a randomizer or pseudo randomizer, we want to ensure full coverage.

Locks (Preventative):



- ◆ **Key locks:**
  - □ Requires a physical key to unlock; keys can be shared/copied.
  - □ **Key Bitting Code** (How far the key is bitten down for that section.) – Can be copied and replicated without the key from either the numbers or a photo of it.
  - □ **Pin Tumbler Lock** (or Yale lock) – A lock mechanism that uses pins of varying lengths to prevent the lock from opening without the correct key.
  - □ **Lock Picking** - with a lock pick set or bumping, opening a lock without the key.
    - □ Any key lock can be picked or bumped, how long it takes depends on the quality of the lock.
    - □ Lock pick sets lift the pins in the tumbler, opening the lock.
  - □ **Lock Bumping** - Using a shaved-down key that matches the lock, the attacker "bumps" the key handle with a hammer or screwdriver which makes the pins jump, then the attacker quickly turns the key.
  - □ **Master Keys** open any lock in a given area or security zone.
    - □ Both who has them and where they are kept should be very closely guarded at all times.
  - □ **Core Key** is used to remove a lock core in "interchangeable core locks."
    - □ An interchangeable core, or IC, is a compact keying mechanism in a specific figure-eight shape.
    - □ Relies upon a specialized "control" key for insertion and extraction of the core.
    - □ Should be kept secure and access should be very restricted.



Lock picking

Bumping key

Interchangeable core lock

- ◆ **Combination Locks:**
  - □ Not very secure and have limited accountability even with unique codes.
  - □ Should be used for low security areas.
  - □ Can be Dial type (think safe), Button or Keypad.

- □ Very susceptible to brute force, shoulder surfing and are often configured with weak security (I know of a good deal of places where the code is the street number).
- □ Over time, the buttons used for the code will have more wear and tear.
- □ For 4-number PIN where 4 keys are used, the possible combinations are no longer 10,000, but 256: if 3 keys, then 81 options.

Smart Cards (contact or contactless):

- ◆ They contain a computer circuit, using ICC (Integrated Circuit Card).
- ◆ **Contact Cards** - Inserted into a machine to be read.
  - □ This can be credit cards you insert into the chip reader or the DOD CAC (Common Access Card).
- ◆ **Contactless Cards** - can be read by proximity.
  - □ Key fobs or credit cards where you just hold it close to a reader.
  - □ They use an RFID (Radio Frequency Identification) tag (transponder) which is then read by an RFID Transceiver.

Magnetic Stripe Cards:

- ◆ Swiped through a reader, no circuit.
- ◆ Very easy to duplicate.

Tailgating/Piggybacking:

- ◆ Following someone authorized into an area you are not authorized to be in.
- ◆ Often combined with Social Engineering.
- ◆ It is easy to do if your reason for being there seems plausible.
- ◆ Bring a lot of food, a cake, and some balloons, have on clothes, ID badge and tools that a repairman would, the options are endless.

Mantrap:

- ◆ A Mantrap is a room with 2 doors; Door 1 must close completely before Door 2 can be opened.
- ◆ Each door has a different authentication method (something you know, something you have, something you are).
- ◆ They can at times use weight sensors - Bob weighs 220lbs (100kg), the weight measured by the pressure plate is 390lbs (177kg), someone is probably in the room with Bob. Door 2 won't open until Bob is confirmed alone in the Mantrap with a cart of old servers, normally done by the cameras in the trap.

Turnstiles (Preventative, Deterrence):

- ◆ Also prevents tailgating, by allowing only 1 person to enter per Authentication (think like in US subway systems or amusement park entries, but for secure areas they are often floor to ceiling turnstiles with interlocking blades).

Both Mantraps and Turnstiles should be designed to allow safe evacuation in case of an emergency. (Remember that people are more important to protect than stuff.)

Contraband Checks (Preventative, Detective, Deterrent):

- Often seen in airports, courthouses, intelligence offices or other higher security facilities.
- Checking what you are bringing in or out of the building to ensure nothing dangerous gets in or anything confidential gets out.
- With technology becoming much smaller, these are less effective when it comes to data theft; it is easy to hide a microSD memory card, which can contain up to 1TB+ of data per card.

Motion Detectors (Detective, Deterrence):

- Used to alert staff by triggering an alarm (silent or not).
- Someone is here, did an authorized person pass the checkpoint?
  - □ IF yes, then log the event and do nothing else
IF no, then alert/alarm.
- Basic ones are light-based - They require light, making them not very reliable.
- **Ultrasound, Microwave, Infrared or Laser** (*pew-pew!!*)
  - □ Active sensors, they send energy (sound, wave or light).
  - □ If the sound takes less time to return or the pattern it receives back is altered, it means someone is somewhere they should not be.
  - □ Photoelectric motion sensors send a beam of light to a sensor, if broken the alarm sounds. These are the *pew-pew* lasers and sorry, no, they are not green or red and they are rarely visible.

Perimeter Alarms:

- Door/window sensors – these are the thin strips around the edges of either or contact sensors.
  - □ If opened, an alarm sounds; if broken, same effect.
  - □ Can be circumvented, but they are part of a layered defense.
- Walls, windows, doors, and any other openings should be considered equally strong.
- Walls are inherently stronger; the rest need compensating measures implemented (locks, alarms, sensors).
- Glass is normally easy to break, but can be bullet and/or explosion proof, or have a wire mesh in the middle.
- Plexiglass can also be used, as it is stronger and does not shatter, but can be melted.
- Door hinges should always be on the inside (or hidden in the door).
- Just like the turnstiles and mantraps, doors (and in some cases windows) should be designed to allow safe exit from the building in case of an emergency. Often there is a "Panic Bar" that opens the door, but

they are also connected to alarms that sound when opened (clearly labeled Emergency Only - Alarm WILL Sound).

Walls, Floors, and Ceilings:

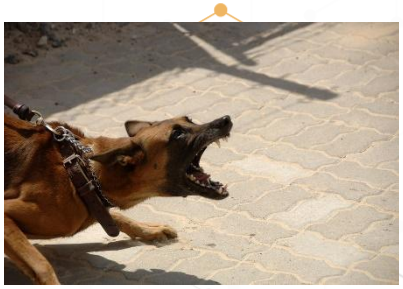
- In line with our layered defense strategy, the strong security encountered in getting to a data center does nothing if there is a crawl space that an attacker can use.
- We need to secure all possible ways into our Data Center or other secure location.
- Walls should be "slab to slab" (from the REAL floor to the REAL ceiling); if sub-flooring or sub-ceilings are used, then they should be contained within the slab-to-slab walls.
- Walls, floors, and ceilings should be made of materials (where it makes sense) that are secure enough for that location, e.g., don't have sheetrock around your Data Center because I can cut that with a knife.
- Walls, floors, and ceilings should have an appropriate fire rating.
  - □ So should your doors, but walls, floors and ceilings are more often overlooked.
  - □ This is to protect the Data Center from outside fire and just as well the rest of the building from a Data Center fire.

Guards – (Deterrent, Detective, Preventative, Compensating)

- Guards can serve many diverse purposes for an organization.
- They can check credentials/ID Cards, monitor CCTV cameras, monitor environmental controls (HVAC), react to incidents, act as a deterrent, and so much more.
- **Professional Guards** - Professional training and/or schooling; armed.
- **Amateur Guards** - No professional training or schooling; armed.
- **Pseudo Guard** - Unarmed guard.
- Guards should have a very clear set of rules and regulations.
- Social engineering attacks are common and should be prevented with training to raise awareness.

Dogs (Deterrent, Detective, Compensating):

- Most often used in controlled, enclosed areas.
- Liability can be an issue.
- Dogs are trained to corner suspects and attack someone who's fleeing. People often panic when they encounter a dog and run.
- Even if they're in a secure area, the organization may still be liable for injuries.
- Can also be internal authorized employees walking out the wrong door or trying to take a shortcut.
- They panic and the dog attacks.



Restricted Work Areas and Escorts.

- To track and funnel authorized visitors, we can use visitor badges, visitor logs, and escorts.
- Non-electronic visitor badges are easy to make copies of and easy to fake.
- Electronic can be just a cheap re-programmable magnetic strip (like for hotel rooms, easy to copy). Make sure they have a short window of use, or more secure individually printed ones for each visit, and only used once.
- The return of all badges and physical sign-out should be enforced when the visitor leaves.
- When a vendor is coming to repair, install or remove something in your facility, they need to be checked in and escorted from the entry point to where they are going to work by an employee, and the employee should stay with the vendor until the work is completed.
- The vendor's employees should already have passed a security check when they were hired; the vendor is liable.
- This sounds and is boring, but it is more likely to prevent the vendor from compromising your security than if they were free to roam the facility and the data center unsupervised.

Technical or Logical Security Controls:

- **Access Control Categories:**

  Administrative (Directive) Controls:

  - Organizational policies and procedures.
  - Regulation.
  - Training and awareness.

  Logica/Technical Controls:

  - Hardware/software/firmware – Firewalls, routers, encryption.

  Physical Controls:

  - Locks, fences, guards, dogs, gates, bollards.

- **Access Control Types** (Many can be multiple types – On the exam look at question content to see which type it is).

  Preventative:

  - Prevents action from happening – Least privilege, drug tests, IPS, firewalls, encryption.

  Detective:

  - Controls that Detect during or after an attack – IDS, CCTV, alarms, anti-virus.

  Corrective:

  - Controls that Correct an attack – Anti-virus, patches, IPS.

Recovery:

- Controls that help us Recover after an attack – DR Environment, backups, HA Environments.

Deterrent:

- Controls that Deter an attack – Fences, security guards, dogs, lights, Beware of the dog signs.

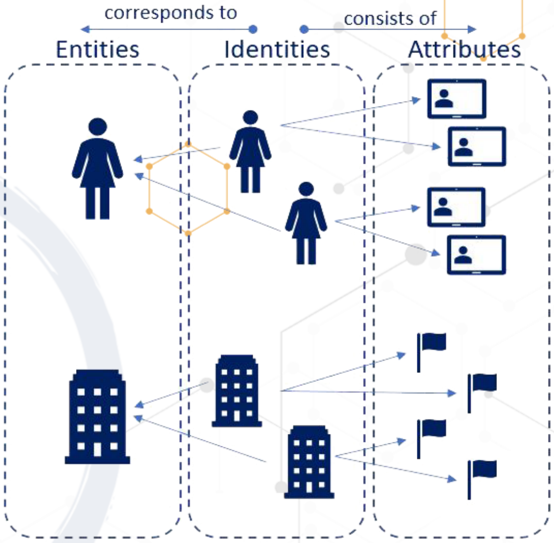
Compensating:

Controls that Compensate – other controls that are impossible or too costly to implement.

- **Identity and Access Provisioning:**

  We can have multiple identities per entity and each identity can have multiple attributes.

  - I can be staff, alumni, and enrolled student at a college.
  - As staff I could have access to different areas and data than I would as alumni and student.
  - Companies can have the same, they can be the parent company, then smaller companies under the parent umbrella, all with different attributes.



- **Identity and Access Provisioning Lifecycle:**

  This is a suggested lifecycle example from "Identity Management Design Guide with IBM Tivoli Identity Manager".

  You obviously don't have to implement it verbatim but find a clear policy that works for your organization.

  - Life cycle rules provide administrators with the ability to define life cycle operations to be executed as the result of an event. Life cycle rules are especially useful in automating recurring administrative tasks.
    - Password policy compliance checking.
    - Notifying users to change their passwords before they expire.
    - Identifying life cycle changes such as accounts that are inactive for more than 30 consecutive days.
    - Identifying new accounts that have not been used for more than 10 days following their creation.
    - Identifying accounts that are candidates for deletion because they have been suspended for more than 30 days.

    - When a contract expires, identifying all accounts belonging to a business partner or contractor's employees and revoking their access rights.

- **Federated Identity:**

  How we link a person's electronic identity and attributes across multiple distinct identity management systems.

  FIDM (Federated Identity Management):

  - Having a common set of policies, practices, and protocols in place to manage the identity and trust into IT users and devices across organizations.
  - **SSO:** A subset of federated identity management. Users use a single sign-on for multiple systems.

- **Access Control Systems:**

  We can use centralized and/or decentralized (distributed) access control systems, depending on which type makes the most sense. Both options provide different benefits.

  Access control decisions are made by comparing the credential to an access control list.

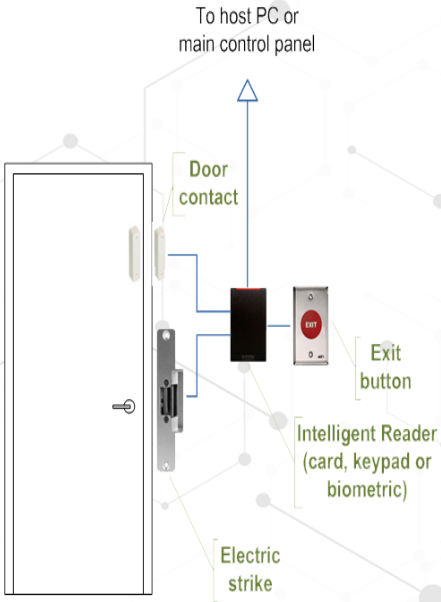
  This look-up can be done by a host or server, by an access control panel, or by a reader.

  Most common is hub and spoke with a control panel as the hub, and the readers as the spokes.

  Today most private organizations use Role Based Access Control (RBAC).

  - You are in Payroll you get the payroll staff access and permissions, if you move to HR, you lose your payroll access and get HR access assigned.

  Normal systems are much larger, but you get the idea from this drawing how they would connect.


To host PC or main control panel
Door contact
Exit button
Intelligent Reader (card, keypad or biometric)
Electric strike
EXIT

  In a perfect world, access control systems should be physically and logically segmented from the rest of our IP Network, in reality it is most often segmented logically with VLANs, but in many cases not even that.

  Centralized Pro's (Decentralized Con's):

  - All systems and locations have the same security posture.
  - Easier to manage: All records, configurations and policies are centralized and only configured once per policy.

        - Attackers look for the weakest link in our chain, if a small satellite office is not following our security posture, they can be an easy way onto our network.
    - It is more secure, only a few people have access and can make changes to the system.
    - It can also provide separation of duties, the local admin can't edit/delete logs from their facility.
    - SSO can be used for user access to multiple systems with one login.

  Centralized Con's (Decentralized Pro's):

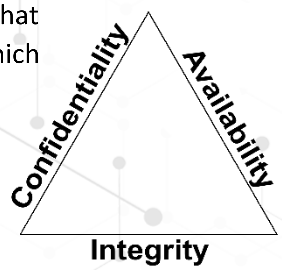
    - Traffic overhead and response time, how long does it take for a door lock to authenticate the user against the database at the head office?
    - Is connectivity to the head office stable, is important equipment on redundant power and internet?

  Hybrid:

    - Centrally controlled; access lists for that location are pushed to a local server on a daily/hourly basis; local administrators have no access.
    - We must still ensure that the local site follows the organization's security posture in all other areas.

- **Authorization:**

  We use Access Control models to determine what a subject is allowed to access. What and how we implement depends on the organization and what our security goals are, type can often be chosen dependent on which leg of the CIA Triad is the most important one to us.
  If it is **Confidentiality,** we would most likely go with Mandatory Access Control.
  If it is **Availability,** we would most likely go with Discretionary Access Control.
  If it is **Integrity,** we would most likely go with Role Based Access Control or Attribute Based Access Control.



- There technically is also RUBAC (Rule Based Access Control), it is mostly used on firewalls with IF/THEN statements but can be used in conjunction with the other models to provide defense in depth.

- **DAC (Discretionary Access Control)** - Often used when Availability is most important:

  Access to an object is assigned at the discretion of the object owner.
  The owner can add, remove rights, commonly used by most OS's'.
  Uses DACL's (Discretionary ACL), based on user identity.
- **MAC (Mandatory Access Control)** - Often used when Confidentiality is most important:

  Access to an object is determined by labels and clearance, this is often used in the military or in organizations where confidentiality is very important.

Labels: Objects have Labels assigned to them; the subject's clearance must dominate the object's label.

- The label is used to allow Subjects with the right clearance access them.
- Labels are often more granular than just “Top Secret”, they can be “Top Secret – Nuclear”.

Clearance: Subjects have Clearance assigned to them.

- Based on a formal decision on a subject's current and future trustworthiness.
- The higher the clearance the more in depth the background checks should be.

- **RBAC (Role-Based Access Control)** - Often used when Integrity is most important:

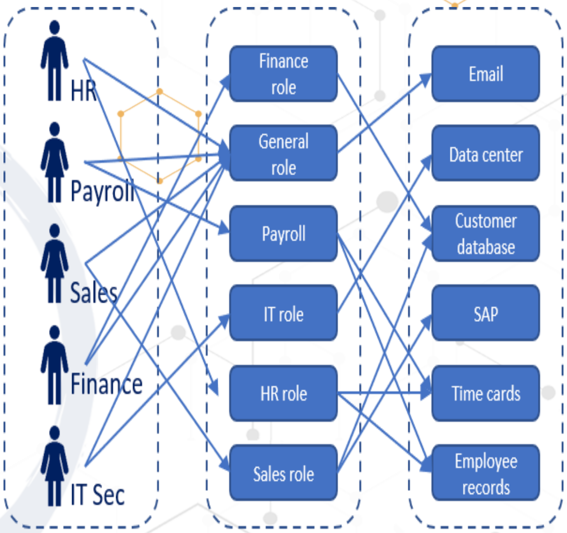
Policy neutral access control mechanism defined around roles and privileges.

A role is assigned permissions, and subjects in that role are added to the group, if they move to another position they are moved to the permissions group for that position.

It makes administration of 1,000's of users and 10,000's of permissions much easier to manage.

The most commonly used form of access control.

If implemented right it can also enforce separation of duties and prevent authorization/privilege creep .



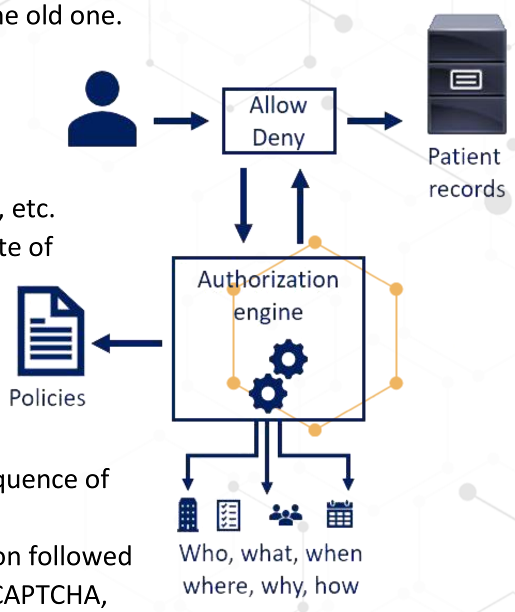
We move employees transferring within the organization from one role to another and we do not just add the new role to the old one.

- **ABAC (Attribute-Based Access Control):**

Access to objects is granted based on subjects, objects, AND environmental conditions.

Attributes could be:

- **Subject** (user) – Name, role, ID, clearance, etc.
- **Object** (resource) – Name, owner, and date of creation.
- **Environment** – Location and/or time of access, and threat levels.



- **Context-Based Access Control:**

Access to an object is controlled based on certain contextual parameters, such as location, time, sequence of responses, access history.

Providing the username and password combination followed by a challenge and response mechanism such as CAPTCHA, filtering the access based on MAC addresses on wireless, or a firewall filtering the data based on packet analysis are all examples of context-dependent access control mechanisms.

- **Content-Based Access Control:**

  Access is provided based on the attributes or content of an object, then it is known as a content-dependent access control.

  In this type of control, the value and attributes of the content that is being accessed determine the control requirements.

  Hiding or showing menus in an application, views in databases, and access to confidential information are all content-dependent.

- **Least Privilege and Need to Know.**

  Least Privilege - (Minimum necessary access) We give our users/systems exactly the access they need, no more, no less.

  Need to Know - Even if you have access, if you do not need to know, then you should not access the data.

  Separation of Duties - More than one individual in one single task is an internal control intended to prevent fraud and error.

- **Administrative Security:** 🐘

  Job Rotation:

  - For the exam think of it to detect errors and frauds. It is easier to detect fraud and there is less chance of collusion between individuals if they rotate jobs.
  - It also helps with employee's burnout and it helps employees understand the entire business.
  - This can be to cost prohibitive for the exam/real life, make sure on the exam the cost justifies the benefit.

  Mandatory Vacations:

  - Done to ensure one person is not always performing the same task, someone else has to cover and it can keep fraud from happening or help us detect it.
  - Their accounts are locked, and an audit is performed on the accounts.
  - If the employee has been conducting fraud and covering it up, the audit will discover it.
  - The best way to do this is to not give too much advance notice of vacations.

- **NDA (Non-Disclosure Agreement):**

  We covered NDAs between our and other organizations, it is also normal to have them for internal employees.

  Some employment agreements will include a clause restricting employees' use and dissemination of company-owned confidential information.
- **Background Checks:**

  References, Degrees, Employment, Criminal, Credit history (less common, more costly).

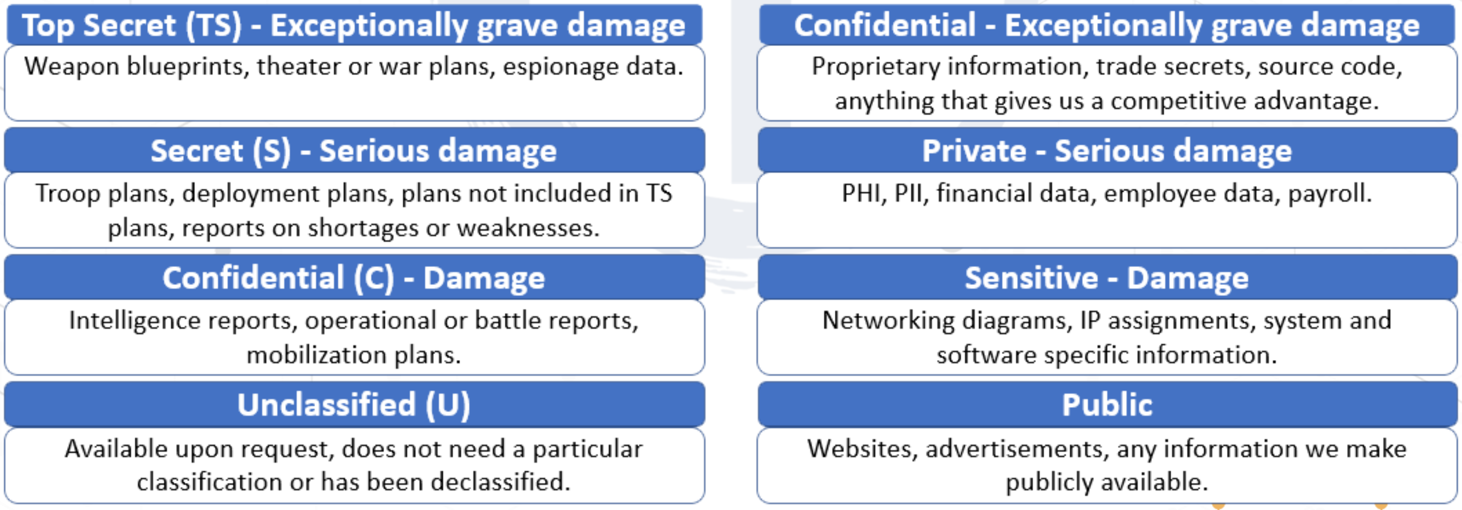
  For sensitive positions the background check is an ongoing process.
- **Privilege Monitoring:**

  The more access and privilege an employee has the more we keep an eye on their activity.

  They are already screened more in depth and consistently, but they also have access to many business-critical systems, we need to audit their use of that access.

  With more access comes more responsibility and scrutiny.

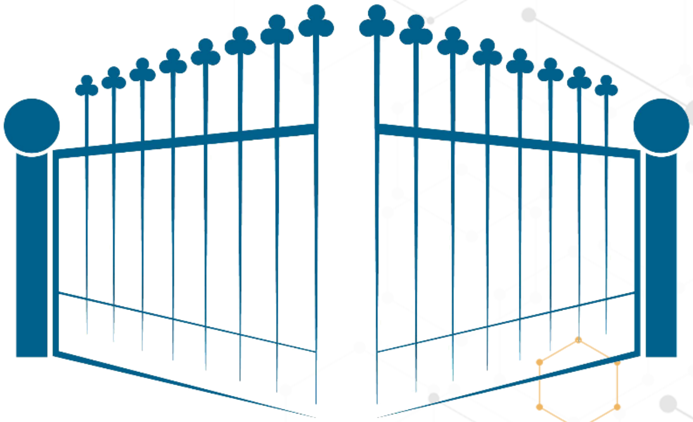
Data Classification Policies:

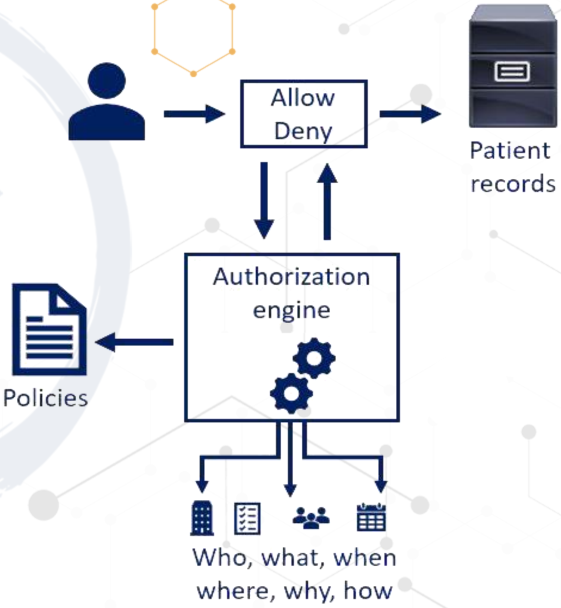


Top Secret (TS) - Exceptionally grave damage	**Confidential - Exceptionally grave damage**
Weapon blueprints, theater or war plans, espionage data.	Proprietary information, trade secrets, source code, anything that gives us a competitive advantage.
Secret (S) - Serious damage	**Private - Serious damage**
Troop plans, deployment plans, plans not included in TS plans, reports on shortages or weaknesses.	PHI, PII, financial data, employee data, payroll.
Confidential (C) - Damage	**Sensitive - Damage**
Intelligence reports, operational or battle reports, mobilization plans.	Networking diagrams, IP assignments, system and software specific information.
Unclassified (U)	**Public**
Available upon request, does not need a particular classification or has been declassified.	Websites, advertisements, any information we make publicly available.

➢ Domain 3: What we covered.

- **Physical Controls:**
  Locks, fences, guards, dogs, gates, bollards, ...





- **Technical Controls:**
  Hardware/software/firmware – Firewalls, routers, encryption, ...