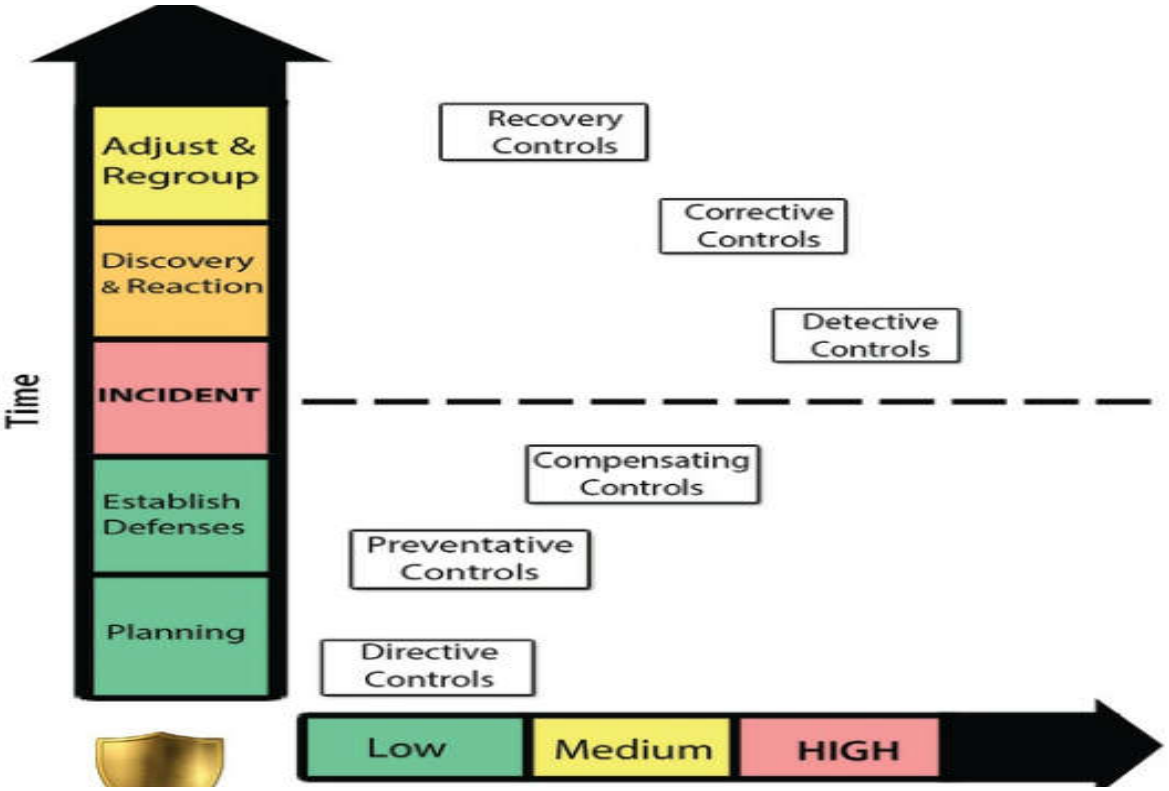
ACCESS CONTROL TYPES



	Administrative	*Technical*	*Physical*
Directive	- Policy	- Configuration Standards	- Authorized Personnel Only Signs - Traffic Lights
Deterrent	- Policy	- Warning Banner	- Beware of Dog Sign
Preventative	- User Registration Procedure	- Password Based Login	- Fence
Detective	- Review Violation Reports	- Logs	- Sentry - CCTV
Corrective	- Termination	- Unplug, isolate, and terminate connection	- Fire Extinguisher
Recovery	- DR Plan	- Backups	- Rebuild
Compensating	- Supervision - Job Rotation - Logging	- CCTV - Keystroke Logging	- Layered Defense

Preventative access control - Deployed to **stop** or block before it happens.

Fences, **locks**, **biometrics**, **mantraps**, **lighting**, **alarm systems**, separation of duties, **job rotation**, data classification, **penetration testing**, **encryption**, **auditing**, **closed circuit television (CCTV)**, **smart cards**, **callback**, **security policies**, **security awareness training**, and **antivirus software**.

Deterrent access control - Deployed to **discourage bad behavior**

Locks, fences, **security badges**, **security guards**, **mantraps**, security cameras, trespass or **intrusion alarms**, **separation of duties**, work task procedures, **awareness training**, encryption, **auditing**, and firewalls.

Detective access control - Deployed to **discover after it happens.**

Security guards, guard dogs, motion detectors, recording and reviewing of events seen by security cameras or **CCTV**, **job rotation**, **mandatory vacations**, **audit trails**, **intrusion detection systems**, violation reports, **honey pots**, **supervision and reviews of users**, **incident investigations**, and intrusion detection systems.

Corrective access control - Deployed to **fix the problem**

Antivirus solutions, a**larms**, **mantraps**, **business continuity planning**, and **security policies**.

Recovery access control – Deployed to **repair or restore** damaged systems.

Backups and restores, **fault tolerant drive systems**, **server clustering**, **antivirus software**, and **database shadowing**.

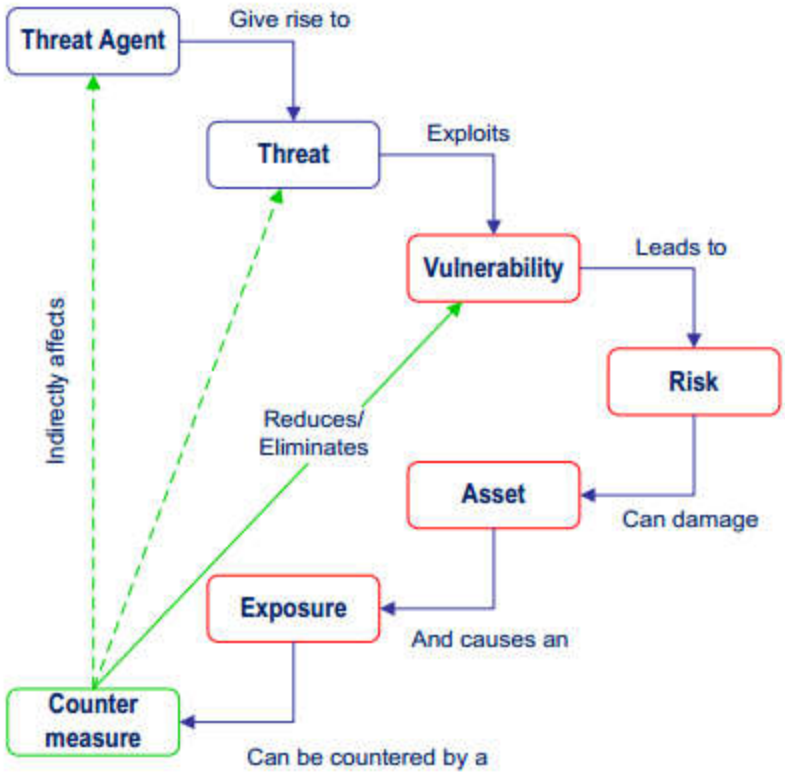
Compensation access control - Deployed **to assist other existing controls**

Security policy, **personnel supervision**, **monitoring**, and **work task proce**dures. a motion **detector with a spotlight** and a **barking sound playback device**.

Directive access control - Deployed to **direct**, **confine**, **control**, **force or encourage compliance** with security policies.

Security guards, **guard dogs**, **security policy**, **posted notifications**, **escape route exit signs**, **monitoring**, **supervising**, **work task procedures**, and **awareness training**.

Administrative / Management access controls Administrative access controls are the policies and procedures defined by an organizations security policy to implement and enforce overall access control. Administrative access controls focus on two areas: personnel and business practices (e.g., people and policies). Examples of administrative access controls include policies, procedures, hiring practices, background checks, data classification, security training, vacation history, reviews, work supervision, personnel controls, and testing.

Logical/technical access controls Logical access controls and technical access controls are the hardware or software mechanisms used to manage access to resources and systems and provide protection for those resources and systems. Examples of logical or technical access controls include encryption, smart cards, passwords, biometrics, constrained interfaces, access control lists (ACLs), protocols, firewalls, routers, intrusion detection systems, and clipping levels.

Physical access controls Physical access controls are the physical barriers deployed to prevent direct contact with systems or portions of a facility. Examples of physical access controls include guards, fences, motion detectors, locked doors, sealed windows, lights, cable protections, laptop locks, swipe cards, guard dogs, video cameras, mantraps, and alarms.