**Types of Controls**

Central to information security is the concept of controls, which may be categorized by their functionality (preventive, detective, corrective, deterrent, recovery, and compensating, in this order) and plane of application (physical, administrative, or technical). Physical controls include doors, secure facilities, fire extinguishers, flood protection, and air conditioning. Administrative controls are the organization’s policies, procedures, and guidelines intended to facilitate information security. Technical controls are the various technical measures, such as firewalls, authentication systems, intrusion detection systems, and file encryption, among others.

**Preventive Controls**

Preventive controls are the first controls met by the adversary. Preventive controls try to prevent security violations and enforce access control. Like other controls, preventive controls may be physical, administrative, or technical: doors, security procedures, and authentication requirements are examples of physical, administrative, and technical preventive controls, respectively.

**Detective Controls**

Detective controls are in place to detect security violations and alert the defenders. They come into play when preventive controls have failed or have been circumvented and are no less crucial than detective controls. Detective controls include cryptographic checksums, file integrity checkers, audit trails and logs, and similar mechanisms.

**Corrective Controls**

Corrective controls try to correct the situation after a security violation has occurred. Although a violation occurred, not all is lost, so it makes sense to try and fix the situation. Corrective controls vary widely, depending on the area being targeted, and they may be technical or administrative in nature.

**Deterrent Controls**

Deterrent controls are intended to discourage potential attackers and send the message that it is better not to attack, but even if you decide to attack we are able to defend ourselves. Examples of deterrent controls include notices of monitoring and logging as well as the visible practice of sound information security management.

**Recovery Controls**

Recovery controls are somewhat like corrective controls, but they are applied in more serious situations to recover from security violations and restore information and information processing resources. Recovery controls may include disaster recovery and business continuity mechanisms, backup systems and data, emergency key management arrangements, and similar controls.

**Compensating Controls**

Compensating controls are intended to be alternative arrangements for other controls when the original controls have failed or cannot be used. When a second set of controls addresses the same threats that are addressed by another set of controls, the second set of controls are compensating controls.

<https://infosecprimer.wordpress.com/2012/11/03/types-of-controls/>