14.2.2 Control Categories and Types Facts

This lesson covers the following topics:

- Control categories
- Control types

Control Categories

Control categories define techniques used to protect network data and security. Three major categories have been defined for network security: managerial, operational, and technical.

- Managerial controls (consist of management techniques and administrative procedures)
- Operational controls (performed everyday by the security team)
- Technical controls (based around software, applications, and security appliances)

Control Types

Control types consist of different strategies to prevent, detect, mitigate, and correct any network breach. A company's size and financial budget are determining factors in the selection of applications for these control types.

Control Type	Description
Preventative	Preventative controls are used to prevent security breaches. Many tools used in these controls are also used in other control types. The easiest preventative control is an advanced network appliance, which is sometimes called an adaptive security appliance (ASA). This is a firewall and router combination that is capable of hosting IDSs and IPSs. A less expensive preventative control is an updated antivirus, which have improved drastically over the years. Office access control is also an excellent preventative control, especially if biometrics are used.
Detective	Detective controls inform the security team of an event that is occurring and provide logs and other artifacts to help investigate the event. Examples would be intrusion detection systems (IPSs), network monitoring applications, log collectors, and real-time monitoring alerts.
Corrective	Corrective controls are those that attempt to fix any damage caused by an event. These tools work during the event and after the event is over. Think of this as a form of risk mitigation. For example, an intrusion prevention system is designed to intercept data that is potentially malicious and either drop the packet or isolate it. Another example is endpoint protection that works to stop malicious data identified by its signature, behavior, or other known identifiers.
Deterrent	The deterrent type of control discourages malicious actors from attempting to try to breach a network. The more deterrents, the less likely an event will occur. This could include security policies, access-protected doors for a server room, entry-point access restriction, biometric sensors, man traps, security cameras, security training, and security

	guards. Remember that the stronger the deterrents, the less likely a breach will occur.
Compensating	A compensating control is one that does not stop an event, but it helps by making up for damage done. The perfect example is data backups. If a company gets hit with malware that deletes data, locks files, or otherwise makes the company's data inaccessible, the IT team can revert to the latest backup. Depending on the extent of the damage, good backups can have critical servers back online within minutes.
Physical	Physical deterrents keep unauthorized people from physically accessing a company's assets. Locked doors, proximity cards, fences, cameras, and guards are all ways to physically protect your network. Motion detectors for after-hours monitoring is another example. Device management is often overlooked. With the prevalence of mobile devices, a company must be able to remotely wipe devices that are lost or stolen.

This table gives a high-level view of each control type, but there are many more variations available. Selecting the right application requires research and trials to ensure the proper application is found for a specific need.