

What are the primary distinguishing features between technical, operational, and managerial controls? In terms of their implementation and primary objectives, how do each of these controls uniquely contribute to an organization's security posture?

Answer: A technical control is one that uses technology to reduce vulnerabilities, such as AV, IDS, etc. Operational control implements help to ensure the day-to-day operations of an org comply with security plan. This could be in the form of end user training or configuration and change management. Managerial controls use planning and assessment methods to reduce and manage risk such as risk assessments, vuln testing and penetration testing. This is how they contribute to the security posture of an organization.

How do the roles of preventative, detective, corrective, and compensating controls differ in an integrated security framework? While they all contribute to the overall security posture, in what specific ways does each control uniquely address potential threats, and how might their functions overlap?

Answer: These controls will differ in an integrated security framework by the functionality. Detective controls are tools that can help you identify errors or irregularities that may have occurred. Corrective controls attempt to correct errors or irregularities that have been detected. Compensating controls are an alternative method that supports the requirement of actual security control.