Requirements and Testing Procedures		Guidance
1.2 Network security controls (NSCs) are configured and maintained.		
Defined Approach Requirements **1.2.1** Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained. **Customized Approach Objective** The way that NSCs are configured and operate are defined and consistently applied.	**Defined Approach Testing Procedures** **1.2.1.a** Examine the configuration standards for NSC rulesets to verify the standards are in accordance with all elements specified in this requirement. **1.2.1.b** Examine configuration settings for NSC rulesets to verify that rulesets are implemented according to the configuration standards.	**Purpose** The implementation of these configuration standards results in the NSC being configured and managed to properly perform their security function (often referred to as the ruleset). **Good Practice** These standards often define the requirements for acceptable protocols, ports that are permitted to be used, and specific configuration requirements that are acceptable. Configuration standards may also outline what the entity considers not acceptable or not permitted within its network. **Definitions** NSCs are key components of a network architecture. Most commonly, NSCs are used at the boundaries of the CDE to control network traffic flowing inbound and outbound from the CDE. Configuration standards outline an entity's minimum requirements for the configuration of its NSCs **Examples** Examples of NSCs covered by these configuration standards include, but are not limited to, firewalls, routers configured with access control lists, and cloud virtual networks.