Requirements and Testing Procedures		Guidance
1.4 Network connections between trusted and untrusted networks are controlled.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Implementing NSCs at every connection coming into and out of trusted networks allows the entity to monitor and control access and minimizes the chances of a malicious individual obtaining access to the internal network via an unprotected connection. **Examples** An entity could implement a DMZ, which is a part of the network that manages connections between an untrusted network (for examples of untrusted networks refer to the Requirement 1 Overview) and services that an organization needs to have available to the public, such as a web server. Please note that if an entity's DMZ processes or transmits account data (for example, e-commerce website), it is also considered a CDE.
1.4.1 NSCs are implemented between trusted and untrusted networks.	**1.4.1.a** Examine configuration standards and network diagrams to verify that NSCs are defined between trusted and untrusted networks.	
	1.4.1.b Examine network configurations to verify that NSCs are in place between trusted and untrusted networks, in accordance with the documented configuration standards and network diagrams.	
Customized Approach Objective		
Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.		