Requirements and Testing Procedures		Guidance
		• The source of all account data received (for example, customers, third party, etc.), and any entities with which account data is shared. • Date of last update, and names of people that made and approved the updates.
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Compromises often happen due to unused or insecure services (for example, telnet and FTP), protocols, and ports, since these can lead to unnecessary points of access being opened into the CDE. Additionally, services, protocols, and ports that are enabled but not in use are often overlooked and left unsecured and unpatched. By identifying the services, protocols, and ports necessary for business, entities can ensure that all other services, protocols, and ports are disabled or removed. **Good Practice** The security risk associated with each service, protocol, and port allowed should be understood. Approvals should be granted by personnel independent of those managing the configuration. Approving personnel should possess knowledge and accountability appropriate for making approval decisions.
1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.	**1.2.5.a** Examine documentation to verify that a list exists of all allowed services, protocols, and ports, including business justification and approval for each.	
	1.2.5.b Examine configuration settings for NSCs to verify that only approved services, protocols, and ports are in use.	
Customized Approach Objective		
Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.		