Requirements and Testing Procedures		Guidance
2.2 System components are configured and managed securely.		
Defined Approach Requirements **2.2.1** Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment. **Customized Approach Objective** All system components are configured securely and consistently and in accordance with industry-accepted hardening standards or vendor recommendations.	**Defined Approach Testing Procedures** **2.2.1.a** Examine system configuration standards to verify they define processes that include all elements specified in this requirement. **2.2.1.b** Examine policies and procedures and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. **2.2.1.c** Examine configuration settings and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before or immediately after a system component is connected to a production environment.	**Purpose** There are known weaknesses with many operating systems, databases, network devices, software, applications, container images, and other devices used by an entity or within an entity's environment. There are also known ways to configure these system components to fix security vulnerabilities. Fixing security vulnerabilities reduces the opportunities available to an attacker. By developing standards, entities ensure their system components will be configured consistently and securely, and address the protection of devices for which full hardening may be more difficult. **Good Practice** Keeping up to date with current industry guidance will help the entity maintain secure configurations. The specific controls to be applied to a system will vary and should be appropriate for the type and function of the system. Numerous security organizations have established system-hardening guidelines and recommendations, which advise how to correct common, known weaknesses. **Further Information** Sources for guidance on configuration standards include but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Cloud Security Alliance, and product vendors.

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.