PCI DSS Requirements	Testing Procedures	Guidance
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. ***Note:*** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.* *Effective immediately, new implementations must not use SSL or early TLS.* *POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016.*	**2.2.3.a** Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols.	Enabling security features before new servers are deployed will prevent servers being installed into the environment with insecure configurations. Ensuring that all insecure services, protocols, and daemons are adequately secured with appropriate security features makes it more difficult for malicious individuals to take advantage of commonly used points of compromise within a network. Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.). ***Regarding use of SSL/early TLS:*** Entities using SSL and early TLS must work towards upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where they don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment environments. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up-to-date with vulnerability trends and determine whether or not they are susceptible to any known exploits. Refer to the PCI SSC Information Supplement *Migrating from SSL and Early TLS* for further guidance on the use of SSL/early TLS.
	2.2.3.b *For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:* Confirm the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS.	
	2.2.3.c *For all other environments using SSL and/or early TLS:* Review the documented Risk Mitigation and Migration Plan to verify it includes: □ Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; □ Risk-assessment results and risk-reduction controls in place; □ Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; □ Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; □ Overview of migration project plan including target migration completion date no later than June 30, 2016.	