

Are operating systems that are no longer supported by the vendor non-compliant with the PCI DSS?

PCI SSC FAQ | Article 1130 | June 2013

PCI DSS Requirements 6.1 and 6.2 address the need to keep systems up to date with vendor-supplied security patches in order to protect systems from known vulnerabilities. Where operating systems are no longer supported by the vendor, OEM or developer, security patches might not be available to protect the systems from known exploits, and these requirements would not be able to be met.

However, it may be possible to implement compensating controls to address risks posed by using unsupported operating systems in order to meet the intent of the requirements. To be effective, the compensating controls must protect the system from vulnerabilities that may lead to exploit of the unsupported code. For example, exhaustive reviews may need to be regularly performed to ensure that all known exploits for that operating system are continually identified and that system configurations, anti-virus, IDS/IPS, and firewall rules are continually updated to address those exploits. Examples of controls that may be combined to contribute to an overall compensating control include active monitoring of system logs and network traffic, properly-configured application whitelisting that only permits authenticated system files to execute, and isolating the unsupported systems from other systems and networks. Note that these examples may complement an overall compensating control, but these examples alone would not provide sufficient mitigation.

Additionally, if an unsupported operating system is Internet-facing, it will be detected and reported as an automatic failure by an ASV scan. Detection of unsupported operating systems in an ASV scan will need to be addressed according to Addressing Vulnerabilities with Compensating Controls section of the ASV Program Guide.

The use of compensating controls should be considered a temporary solution only, as the eventual solution is to upgrade to a supported operating system, and the entity should have an active migration plan for doing so. For assistance with compensating controls, and for questions about whether a specific implementation meets PCI DSS requirements, please contact a Qualified Security Assessor.

Source: <https://www.pcisecuritystandards.org/faqs/1130/>