

Are disaster-recovery (DR) sites in scope for PCI DSS?

PCI SSC FAQ | Article 1323 | March 2015

Whether a disaster-recovery (DR) site is in scope for PCI DSS will largely depend on how the site is configured and used. For example; "hot standby" or "warm standby" approaches, where a DR site contains a live or ready-to-use copy of CDE systems and data, or backups of cardholder data, or other component that impacts the security of cardholder data (such as cryptographic keys), are in scope for PCI DSS.

Alternatively, "cold standby" approaches, where the DR site does not contain any CDE systems or cardholder data and does not connect to the CDE, may be excluded from scope while the DR site is not in use. However, in the event that the DR site is activated, the entity must ensure that the DR site is configured to maintain all applicable PCI DSS requirements for the duration that it is used, and that all cardholder data is securely deleted from the DR site upon completion of its use.

Any testing activity performed on a DR site (for example, to simulate activation of the site) that includes the presence of cardholder data or other component that impacts the security of cardholder data, are also in scope for PCI DSS requirements.

Source: <https://www.pcisecuritystandards.org/faqs/1323/>