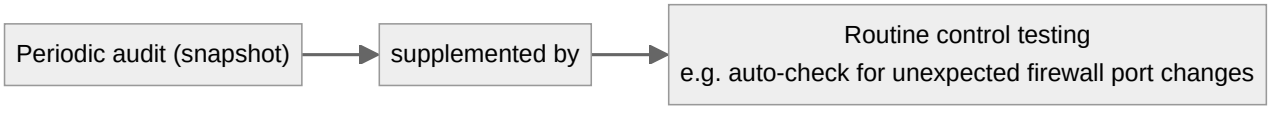
Control Testing, Exceptions, and Compensating Controls

Mon, Aug 31, 6:00 PM EDT · https://scottslab.io/posts/control-management-and-exceptions

TL;DR

Periodic audits aren't enough; supplement them with routine control testing: automated checks that catch, say, an unexpected firewall port change the day it happens, not at the next audit. When a control genuinely can't be met, the exception has to be written down (justification, risks, residual risk) and approved by a defined authority. It doesn't get waved through in a hallway. And a compensating control has to earn it: PCI's bar is that it meets the intent and rigor of the original requirement, provides similar defense, and isn't already being counted for something else.

An audit is a snapshot, and snapshots miss everything that happens between them. That's why routine control testing has to supplement periodic audits: continuous or automated checks that flag drift as it happens. The classic example is an automated check for unexpected firewall port changes: an audit would catch that open port next quarter; a routine test catches it the afternoon someone opens it. Audits prove the program on a schedule; routine testing keeps it honest in between.



Control Testing, Exceptions, and Compensating Controls

Sometimes a control genuinely can't be met: a legacy system that can't do the required encryption, a business process that breaks under the rule. That's allowed, but only through a real exception process, and the two requirements are what keep "we made an exception" from becoming "we ignored it." First, formal written documentation: something like Washington State's exception request form, which forces you to spell out the justification, the risks, and the residual risk you're accepting. Second, a defined approval authority: a specific role empowered to accept that risk on the organization's behalf. An exception nobody signed and nobody wrote down isn't an exception, it's a gap you've decided not to look at.

Control Testing, Exceptions, and Compensating Controls

When an exception is granted, you don't just accept the naked risk. You put a compensating control in its place, an alternative that covers what the original requirement would have. But a compensating control has to genuinely stand in, not just look like effort, and PCI DSS spells out the bar cleanly: it must meet the intent and rigor of the original requirement, provide a similar level of defense, and not already be counted toward some other requirement (no double-dipping one control across two obligations). Meet that bar and the exception is defensible; miss it and you've just documented, in writing, that you knew about the gap and left it open. That's worse than not documenting at all.

Written by Scott S. — Contact: scott@scottschlangen.com — scottslab.io — https://scottslab.io/posts/control-management-and-exceptions