

Watching the Watchers: Management Reviews and Privileged Access

Fri, Aug 28, 10:00 AM EDT · <https://scottslab.io/posts/management-reviews-and-privileged-access>



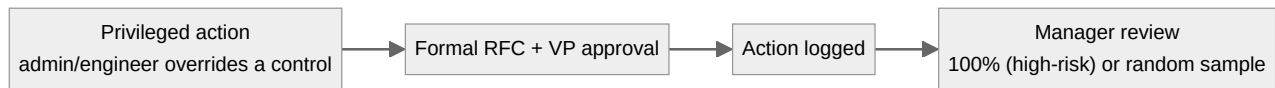
TL;DR

Management reviews do two jobs: catch errors in people's work, and deter fraud by making oversight normal. The sharpest scrutiny goes to privileged actions: admins and engineers who can override the controls everyone else obeys. Their exceptions should ride a formal RFC with VP approval, with a manager reviewing the logs (100% for the highest-risk, or a random sample). And account reviews confirm three things: the person still works here, their permissions match their current role, and every change since last time was authorized.

Management review is one of those controls that sounds like bureaucracy and is actually load-bearing. It does two things at once. First, it's a correctness check: a second set of eyes confirming an employee's work is accurate and complete. Second, and less obvious, it deters fraud simply by existing: when people know their work gets reviewed, the culture shifts, and most would-be shortcuts never get taken. The review that never catches anything is still working. It's why there was nothing to catch.

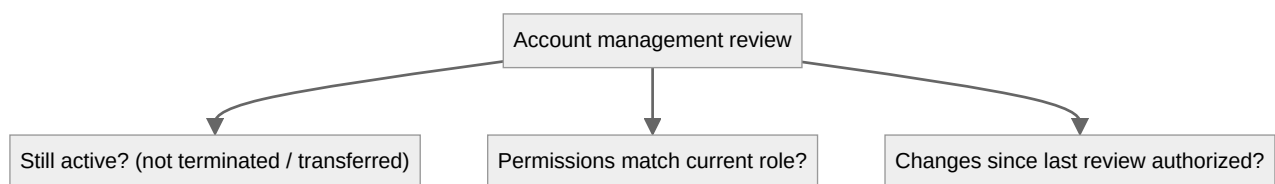
The scrutiny should scale with power, and nobody has more power than the privileged users. System engineers and admins can override the very controls everyone else is bound by, which makes their actions the highest-risk thing happening on your network. So privileged exceptions

shouldn't happen casually. They ride a formal RFC (request for change) with VP-level approval, so there's a paper trail and a senior name attached. And a manager reviews the privileged-action logs afterward: for the highest-risk systems, that means verifying 100% of privileged actions; for lower-risk ones, a random sample is enough to keep everyone honest without drowning the reviewer.



Watching the Watchers: Management Reviews and Privileged Access

The other recurring review is over accounts themselves, and it's a checklist worth memorizing because it maps exactly to how access goes wrong. Is the user still active: not terminated, not transferred out? Do their permissions match their *current* role, or are they carrying access from a job they left two moves ago (the privilege creep problem)? And were the changes since the last review, every escalation, creation, and revocation, actually authorized? Done with the manager who owns those people, this is the control that catches the orphaned admin account and the quietly over-privileged veteran before an attacker does.



Watching the Watchers: Management Reviews and Privileged Access

The theme under all of it: trust is fine, but unverified trust in the people who can override your controls is just hope. Review scales with privilege, and the highest privilege gets the closest look.