Incident summary (GRC, 16 Sep 2026)

Stage 4 evidence

Open only after you have completed Build (Stage 3).

From: Leah Voss (SOX ITGC, on site) To: Fatima Al-Sayed, Jordan Ellis

Yesterday's walkthrough of Cloud-prod-A looked consistent with the weekly job: privileged MFA mostly green.

This morning Cloud Security forwarded an alert on **Cloud-legacy-B**. A privileged console session succeeded for a user who is not in the weekly job's output. The account still has the CMDB tag `legacy`.

Westshore Clinics was acquired in 2025. Their patient-scheduling workload still runs there. Engineering said "legacy means old naming, not non-production." GRC's inventory still says confirm owner.

I need to know whether HL-CC-PRIV-MFA-01 was ever evaluated for that account, and what last week's 100 percent pass actually included.