Control: AU-6 – Audit Review

The organization enables auditing of privileged command execution using auditd.

A rule is configured to track every execution of the sudo command using the key sudo\_monitoring.

Log data was verified using ausearch, saved to text, and screenshots were captured for documentation.

This satisfies audit review requirements for privileged access attempts.