Questions Auditors Should Ask When Evaluating Firmware Security

Framework: 800-53 Rev. 5	Audit Questions	Evidence to Look For
CM-8 Component Inventory	For each device, what components are included? Which component manufacturers, models, and versions are used in critical equipment?	Records including vendor, model, and version of device and internal components (e.g., CPU, BIOS, storage media, add-in devices) from each department or team of the organization.
CM-2 Baseline Config	What firmware version and configuration options are used in critical equipment?	Examine baselined system results/reports to see version, integrity, and configuration settings that are part of the baseline. Unnecessary features should be disabled, and device security features should be enabled/running. When was the last update to this configuration?
SI-2 Flaw Remediation	For each device and component, is firmware up to date? Are there known vulnerabilities in that model/version?	Compare gathered versions against the manufacturer's website, CVEs for respective device/component. When was the most recent deployment of firmware updates?
IR-4 Incident Handling	What playbook, tools, or capabilities check firmware in compromised systems? Has the team trained or investigated firmware issues?	Playbook, training, or similar documentation for investigating firmware-level compromise.
RA-5 Vulnerability Scanning	Can the vulnerability scanning capability discover firmware vulnerabilities?	Scan results including CPU, ME, TPM, BMC, and network appliance vulnerabilities. Ensure that these checks are updated regularly to include the latest vulnerabilities.
SI-2 Flaw Remediation **SI-4 Information System Monitoring**	How are firmware vulnerabilities and updates managed? Will firmware/hardware changes be detected by monitoring?	Documented risk management process includes device firmware/hardware vulnerabilities. Devices that are not up to date have an appropriate justification.
MA-3 Maintenance Tools	What maintenance tools are approved for use to manage firmware?	List of approved tools and versions.
SI-7 Software, Firmware, and Information Integrity	What checks are in place to detect unauthorized firmware changes or indicators of compromise?	Device scan report includes firmware integrity and change detection status.
SR-9 Tamper Resistance and Detection	How would vulnerable or unauthorized components be detected?	Examine results for mechanisms to check firmware integrity and expected hardware. Ensure that these checks are updated regularly to include new components or detection methods.