

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