An Auditor's Guide to Evaluating Firmware Security

As an auditor, you meticulously comb through the requirements and keep organizations accountable for compliance. Recently, you may have noticed firmware and hardware introduced in compliance standards, including NIST 800-53 Rev. 5, PCI DSS, FedRAMP, NIST 800-171, and Cybersecurity Maturity Model Certification (CMMC). But what does this mean, and what should you be looking for?

Firmware and hardware are subject to many of the same bugs and vulnerabilities that plague software, and the risk management process should extend down to these levels. In the past, this has been difficult because tools to enumerate the many components of a device, inspect firmware for vulnerabilities, or check for unauthorized modifications are specialized. While most organizations cannot afford teams of firmware experts, attackers continue to take advantage of this gap. Auditors can identify these gaps and help organizations resolve them before they are exploited.

With new tools now available, it is appropriate for an auditor to ask how an organization is achieving the same level of compliance discipline at the firmware and hardware layer as they do the operating system and application. Below are examples of some questions to ask during an audit based on NIST 800-53 Rev. 5 and ways organizations can provide proof of compliance.

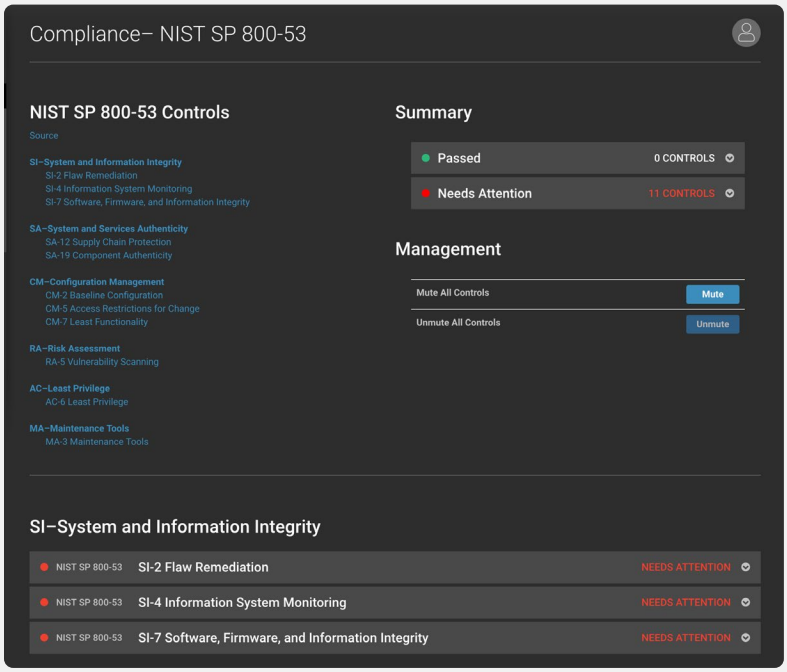
©2021 Eclypsium, Inc.

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.

©2021 Eclypsium, Inc.

Tools make all the difference both in verifying due diligence and implementing these controls within an organization. When working to bring an organization into compliance, a scan tool on each endpoint can coalesce these device details into one place for analysis. From there, the inventory becomes clear, vulnerabilities can be identified, remediation steps can be prioritized, and threats can be hunted down.

Questions can quickly reveal the actionable next steps organizations must take to become compliant. For example, if a critical issue or backdoor were found in a particular network card or chipset, would the organization be able to find all the affected devices? If OS and application updates are being managed, will the same process also cover BIOS and other component firmware? Are any checks in place to discover firmware-level tampering or counterfeiting? This allows auditors to build a path forward and ensure compliance is being met.



Eclypsium enables component-level inventory, risk management, and threat detection across the enterprise. Findings are automatically mapped to NIST Special Publications relevant to firmware and hardware. This information supports evidence of relevant controls in the environment.

Eclypsium delivers device-level visibility, risk management, and advanced threat detection and prevention. Contact **info@eclypsium.com** to learn more.

Company Information

Headquartered in Portland, Oregon, Eclypsium brings together an unmatched combination of talent and expertise dedicated to stopping the threats to the foundation of devices. Founded in 2017, the company currently includes almost over 50 employees and is trusted by customers that include Fortune 50 financial services, data center operators, and government. To support the needs of government customers, Eclypsium maintains a team of experts in the Washington DC region as well as a network of trusted partners. With the backing of top tier investors including Andreessen-Horowitz, Madrona Venture Group, Intel Capital, and Ubiquity Ventures, Eclypsium continues to grow by leaps and bounds. In 2020, Eclypsium raised an additional 13M of capital to continue realizing the vision of defending the firmware and hardware foundation of every device.

©2021 Eclypsium, Inc.