**Maintenance (MA)**

MA-1: System Maintenance Policy And Procedures

NIST SP 800-53 Objective: The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]:

a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

Control Translation: Ensure system maintenance policy and procedures are in place.

Notes: The organizational risk management strategy is a key factor in the development of the system maintenance policy. Related control: PM-9. This control can be applied at the General level.

How to test and evaluate: Examine SSP and System Maintenance Policy (if available). Verify that the policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance of organization/agency.

Technology specific: General

**MA-2: Controlled Maintenance**

NIST SP 800-53 Objective: The organization:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and

e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Control Translation: This is an overall control related to maintenance. Control is looking for documentation of all maintenance activities and their authorizations. This control is related to MP-6 (Media Sanitization) and SI-2 (Flaw Remediation).

Notes: Many of the documents collected in this control will apply throughout the MA family. Make sure to collect schedules, maintenance records, authorizations (if not a part of records), and other necessary documentation or evidence of compensating controls or lack of need for controls.

How to test and evaluate: Review Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records looking for evidence related to each of the sub-steps for this control. Some of the records may cover several of the sub-steps so you may have to identify where each are covered in your write-ups. Again, make sure to collect as much of this evidence as you can because it may be usable for further MA controls.

Technology specific: All

**MA-3: Maintenance Tools**

NIST SP 800-53 Objective: The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.

Control Translation: This control is looking for an inventory and rationale for internal organization-controlled security tools. Not to be confused with tools brought in by 3rd parties or contractors. There should be list of tools and an approval letter or statement that these have been reviewed and signed off. This control is related to MP-6 (Media Sanitization).

Notes: This could be documented in an unexpected location such as in an internal testing Rules of Engagement document or elsewhere, however many orgs do not have such a list created. These tools include software, hardware, or firmware used for diagnostic and/or repair purposes.

How to test and evaluate: Review Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records looking for a defined set of tools that have been approved for maintenance.

Technology specific: All

**MA-4: Non-Local Maintenance**

NIST SP 800-53 Objective: The organization:

a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities;

b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;

d. Maintains records for non-local maintenance and diagnostic activities; and

e. Terminates all sessions and network connections when non-local maintenance is completed.

Control Translation: This control is commonly assessed in cloud environments as most maintenance is performed non-locally. Documentation of non-local maintenance procedures should be reviewed as well as any tools to be used to monitor these connections and sessions. This control is related to AC-2 (Account Management), AC-3 (Access Enforcement), AC-6 (Least Privilege), AC-17 (Remote Access), AU-2 (Auditable Events), AU-3 (Content of Audit Records), IA-2 (Identification and Authentication (Organizational Users)), IA-8 (Identification and Authentication (Non-Organizational Users)), MA-5 (Maintenance Personnel), MP-6 (Media Sanitization), and SC-7 (Boundary Protection).

Notes: Non-local maintenance does not only apply to 3rd party or contractor staff. If the user is not physically located at the hardware being maintained (e.g. admin accessing a server in a datacenter from the home office) this is non-local maintenance. Keep this in mind while assessing this control.

How to test and evaluate: Review Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; information system design documentation; information system configuration settings and associated documentation; maintenance records looking for methods to track non-local maintenance (logs, session controls, etc.) and documentation of non-local maintenance procedures and policies that users and 3rd parties should follow to complete this maintenance.

Technology specific: All

**MA-5: Maintenance Personnel**

NIST SP 800-53 Objective: The organization:

a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and

b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

Control Translation: This control is looking for a defined list of maintenance personnel and a defined method of authorization and documentation of that authorization. This control is related to IA-8 (Identification and Authentication (Non-Organizational Users)) and MA-5 (Maintenance Personnel).

Notes: This control is for internal maintenance personnel as well as 3rd party.

How to test and evaluate: Review Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; access control records review for documentation of the list of authorized maintenance personnel (maybe a user access list from each technology) and a documentation of approvals for each access (e.g. a user access request form or another signed maintenance form).

Technology specific: All

**MA-6: Timely Maintenance**

NIST SP 800-53 Objective: The organization obtains maintenance support and/or spare parts for security-critical information system components and/or key information technology components within the organization-defined time period of failure.

Control Translation: This control is looking for a defined timeframe for maintenance and the planned actions to support this timeframe. It is important to ensure that the timeframe is defined first prior to assessing actions. Such actions to support the timeframe may include service level agreements (internal or external), parts supplies on-site or parts supply agreements, maintenance windows or turnaround agreements. This control is related to CP-2 (Contingency Plan).

Notes: It is possible in some environments that there is a redundancy element that is a compensating control and parts turnaround can be longer as a result.

How to test and evaluate: Review Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; security plan first for the timeframe that is critical to the system. Then review for measures to be taken in the event of issues and the timeframes in which these measures need to be completed.

Technology specific: All