COALFIRE

WHITE PAPER

Migration from MARS-E to ARC-AMPE Configuration Management (CM) controls

CMS requirements for Administering Entities

JESSICA PAYNE, CONSULTANT
IAN WALTERS, PRINCIPAL

877-224-8077 | info@coalfire.com | Coalfire.com

Table of contents

Purpose **2**
Background **3**
Affordable Care Act 3
CMS oversight 3
ARC-AMPE 3
Control mapping **4**
Configuration Management (CM) 4
References **15**
Legal disclaimer **16**

Purpose

This white paper provides a guide for Administering Entities (AEs) to upgrade their System Security and Privacy Plans (SSPPs) from the Minimum Acceptable Risk Standards for Exchanges (MARS-E) to the Acceptable Risk Controls for ACA, Medicaid, and Provider Entities (ARC-AMPE).

Due to the substantial number of controls, and to facilitate ease of use, this white paper is one of a series of 20 which divides the ARC-AMPE by control family. This white paper addresses the Configuration Management (CM) controls.

ARC-AMPE Control Families	
Control Family	**Number of Controls**
Access Control	51
Awareness and Training	9
Audit and Accountability	19
Assessment, Authorization, and Monitoring	12
Configuration Management (This Document)	**31**
Contingency Planning	23
Identification and Authentication	24
Incident Response	16
Maintenance	16
Media Protection	9
Physical and Environmental Protection	19
Planning	6
Program Management	28
Personnel Security	9
Personally Identifiable Information Processing and Transparency	10
Risk Assessment	12
System and Services Acquisition	34
System and Communications Protection	34
System and Information Integrity	34
Supply Chain Risk Management	6

Background

Affordable Care Act

The Affordable Care Act (ACA) revolutionized access to healthcare in the United States by establishing Health Insurance Marketplaces (HIMs). Enhanced Direct Enrollment (EDE) is an ACA innovation that allows third-party entities, such as insurers and web-brokers, to offer consumers a seamless application and enrollment experience directly through their platforms. This approach improves accessibility to the marketplace while maintaining compliance with federal regulations.

CMS oversight

The Centers for Medicare & Medicaid Services (CMS) exercises oversight of AEs, which are responsible for overseeing and managing marketplace operations to ensure compliance with federal regulations, safeguard consumer data, and maintain the integrity of the HIM. Key aspects of CMS's oversight include:

- Requiring AEs to undergo rigorous audit processes, including demonstrating compliance with security and privacy control requirements.
- Enforcing strict data protection measures in the AE environment to ensure the confidentiality, integrity, and availability of consumer data and requiring entities to implement cybersecurity controls, conduct regular risk assessments, and submit independent security audits.
- Requiring AEs to adhere to operational policies and procedures, such as providing accurate plan information, maintaining transparent consumer interactions, and facilitating HIM enrollment without bias.
- Requiring AEs to report any data breaches or system incidents promptly and to take corrective actions as directed by CMS and the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR).
- Requiring AEs to renew their Authority to Connect (ATC) or Authority to Operate (ATO) annually, providing updated documentation and evidence of continued compliance with all requirements.

Through these oversight mechanisms, CMS ensures that AEs in the healthcare.gov environment deliver secure, compliant, and user-friendly services, aligning with the ACA's mission to expand access to quality health coverage.

ARC-AMPE

CMS published the ARC-AMPE Version 1.02 on April 9, 2025. This framework is slated to replace the Minimum Acceptable Risk Standards for Exchange (MARS-E) security and privacy guidelines:

- ARC-AMPE Volume 1 contains high-level guidance, and Volume 2 has the minimum-level security and privacy controls.
- ARC-AMPE Volume 2 is the new format for the SSPP for ACA AEs.
- AEs must have ARC-AMPE implemented by March 4, 2026.
- The implementation date for EDE entities has yet to be announced as of the date of this white paper.

The minimum control baseline for ARC-AMPE compliance consists of 402 controls which have been derived from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations."

The number of controls required represents a significant increase from the MARS-E baseline, and AEs should be prepared for an increased level of effort for developing the SSPP and to submit more artifacts during audits.

Another major change is the format of the SSPP template. MARS-E uses a Microsoft Word format whereas ARC-AMPE is an Excel spreadsheet.

Control mapping

The mapping of the controls found in MARS-E Version 2.2 (based on NIST SP 800-53 Revision 4) to their new locations in ARC-AMPE (based on NIST SP 800-53 Revision 5) are included in the table below. The table lists the MARS-E control directly compared with the ARC-AMPE equivalent control name, as applicable. The table also documents any new ARC-AMPE controls that do not have MARS-E equivalents, as well as those controls that have been combined or withdrawn for ARC-AMPE.

Note also that all references to NIST SP 800-53 Revision 5 included below are based on version 5.1.1, which was issued on November 7, 2023.

Configuration Management (CM)

The set of controls in this family focus on how the Exchange shall: (1) establish and maintain baseline configurations and inventories of Exchange IT systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (2) establish and enforce security configuration settings for IT technology products employed in Exchange IT systems.

MARS-E		ARC-AMPE	
Control	**Configuration Management Policy and Procedures**	**Control**	**Policy and Procedures**
CM-1: Configuration Management Policy and Procedures The organization: **a.** Develops, documents, and disseminates to applicable personnel: **1.** A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and **b.** Reviews and updates (as necessary) the current: **1.** Configuration management policy within every three hundred sixty-five (365) days; and **2.** Configuration management procedures within every three hundred sixty-five (365) days. **Implementation Standards** The organization documents the configuration management process and procedures to: **1.** Define configuration items at t he system and component level (e.g., hardware, software, and workstation); **2.** Monitor configurations; and **3.** Track and approve changes prior to implementation, including but not limited to, flaw remediation, security		**CM-01: Policy and Procedures** **a.** Develop, document, and disseminate to organization-defined personnel and roles: **1.** Organization-level configuration management policy that: **(a)** Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **(b)** Is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and **2.** Procedures to facilitate the implementation of the configuration management policy and the associated configuration management procedures; **b.** Designate an organization-defined officials to manage the development, documentation, and dissemination of the configuration management policy and procedures; and **c.** Review and update the current configuration management: **1.** Policy at least every one (1) year and following organization-defined events; and **2.** Procedures at least every one (1) year and following organization-defined events.	

MARS-E		ARC-AMPE	
patches, and emergency changes (e.g., unscheduled changes such as mitigating newly discovered security vulnerabilities, system crashes, and replacement of critical hardware components).			
Control	**Baseline Configuration**	**Control**	**Baseline Configuration**
CM-2: Baseline Configuration The organization develops, documents, and maintains under configuration control a current baseline configuration of the information system. **Implementation Standards** **1.** Baseline configurations will be based upon government, industry, and vendor standards and best practices. **2.** Baseline configurations must include security updates. **3.** Baseline configuration requirements apply to all systems, devices, appliances, and applications.		**CM-02: Baseline Configuration** **a.** Develop, document, and maintain under configuration control, a current baseline configuration of the system; and **b.** Review and update the baseline configuration of the system: **1.** At least every one (1) year. **2.** When required due to major system changes/ upgrades, critical security patches, and/or emergency changes ; and **3.** When system components are installed or upgraded.	
Control	**Reviews and Updates**	**Control**	**N/A**
CM-2 (1): Reviews and Updates The organization reviews and updates the baseline configuration of the information system: **a.** At least every three hundred sixty-five (365) days; **b.** When configuration settings change due to critical security patches, upgrades, and emergency changes (e.g., unscheduled changes, system crashes, and replacement of critical hardware components), and significant system changes/upgrades; **c.** As an integral part of: **1.** Information system component installations; **2.** Upgrades; and **3.** Updates to applicable governing standards (implemented within the 365 days); and **4.** Supporting baseline configuration documentation reflects ongoing implementation of operational baseline configuration updates, either directly or by policy.		**Withdrawn control**: Incorporated into **CM-02**.	
Control	**Automation Support for Accuracy/Currency**	**Control**	**Automation Support for Accuracy and Currency**
CM-2 (2): Automation Support for Accuracy/Currency The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.		**CM-02(02): Automation Support for Accuracy and Currency** Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms.	
Control	**Retention of Previous Configurations**	**Control**	**Retention of Previous Configurations**
CM-2 (3): Retention of Previous Configurations The organization retains older versions of baseline configurations of the information system as deemed necessary to support rollback. **Implementation Standards**		**CM-02(03): Retention of Previous Configurations** Retain at least one (1) of the previous versions of baseline configurations of the system to support rollback.	

MARS-E		ARC-AMPE	
1. Following baseline configuration updates, no less than one (1) older baseline configuration must be maintained (e.g., for emergency rollback).			
Control	**N/A**	**Control**	**Development and Test Environments**
Existing NIST SP 800-53 Rev. 4 control and new to ARC-AMPE.		**CM-02(06): Development and Test Environments** Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.	
Control	**Configure Systems, Components, or Devices for High-Risk Areas**	**Control**	**Configure Systems and Components for High-Risk Areas**
CM-2 (7): Configure Systems, Components, or Devices for High-Risk Areas The organization: **a.** Issues dedicated information systems, system components, or devices with stringent configurations (e.g., FIPS 140-2 for encryption) to individuals traveling to locations that the organization deems to be of significant risk; and **b.** Applies security safeguards to the devices (i.e., detailed inspection of the device for physical tampering, purging, or reimaging the hard disk drive/removable media) when the individuals return.		**CM-02(07): Configure Systems and Components for High-Risk Areas** **a.** Issue systems, system components, or devices to individuals traveling to locations that the organization deems to be of significant risk; and **b.** Apply the following controls to the systems or components when the individuals return from travel: organization-defined security safeguards to systems, system components, or devices.	
Control	**Configuration Change Control**	**Control**	**Configuration Change Control**
CM-3: Configuration Change Control The organization: **a.** Determines the types of changes to the information system that are configuration-controlled; **b.** Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; **c.** Documents configuration change decisions associated with the information system; **d.** Implements approved configuration-controlled changes to the information system; **e.** Retains records of configuration-controlled changes to the information system for a minimum of three (3) years after the change; **f.** Audits and reviews activities associated with configuration-controlled changes to the information system; and **g.** Coordinates and provides oversight for configuration change control activities through change request forms which must be approved by an organizational change control board that convenes frequently enough to accommodate proposed change requests, and by other appropriate organization officials including, but not limited to, the System Developer/Maintainer and information system support staff. **Implementation Standards** **1.** The system owner coordinates and provides oversight for configuration change control activities through		**CM-03: Configuration Change Control** **a.** Determine and document the types of changes to the system that are configuration-controlled; **b.** Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; **c.** Document configuration change decisions associated with the system; **d.** Implement approved configuration-controlled changes to the system; **e.** Retain records of configuration-controlled changes to the system for no less than one (1) year after the change; **f.** Monitor and review activities associated with configuration-controlled changes to the system; and **g.** Coordinate and provide oversight for configuration change control activities through (1) change request forms that must be approved by an organizational configuration change control board that convenes sufficiently frequently to accommodate proposed change requests, and (2) requirements of other appropriate organization officials when configuration change control activities occur.	

MARS-E		ARC-AMPE	
organization-defined configuration change control element (e.g., committee or board) that convenes according to organization-defined frequency and according to organization-defined configuration change conditions. **2.** The system owner defines the configuration change control element and the frequency or conditions under which it is convened. **3.** The organization establishes a central means of communicating significant changes to or developments in the information system or environment of operations that may affect its business agreements/contracts with CMS and business partners, and services to the business owner and associated service consumers (e.g., electronic bulletin board, or web status page). The means of communication are approved and accepted by the system owner. The means of communication with CMS about significant changes must follow the Change Reporting Procedures for State-Based Administering Entities Systems Final established by CMS, which can be found at: https://zone.cms.gov/community/cms-aca-program-security-privacy-policy-guidance-templates.			
Control	**Test/Validate/Document Changes**	**Control**	**Testing, Validation, and Documentation of Changes**
CM-3 (2): Test/Validate/Document Changes The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.		**CM-03(02): Testing, Validation, and Documentation of Changes** Test, validate, and document changes to the system before finalizing the implementation of the changes.	
Control	**N/A**	**Control**	**Security and Privacy Representatives**
Existing NIST SP 800-53 Rev. 4 control and new to ARC-AMPE.		**CM-03(04): Security and Privacy Representatives** Require security and privacy representatives to be members of the organizational configuration change control board.	
Control	**Security Impact Analysis**	**Control**	**Impact Analyses**
CM-4: Security Impact Analysis The organization analyzes changes to the information system to determine potential security and privacy impacts prior to change implementation. Activities associated with configuration changes to the information system are audited. **Implementation Standards** A security Impact Analysis report is required as part of change reporting to CMS. The Change Reporting Procedures for State-Based Administering Entity Systems established by CMS can be found at: https://zone.cms.gov/community/cms-aca-program-security-privacy-policy-guidance-templates.		**CM-04: Impact Analyses** Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.	
Control	**Separate Test Environments**	**Control**	**Separate Test Environments**
CM-4 (1): Separate Test Environments The organization analyzes changes to the information system in a separate test environment before implementation in an		**CM-04(01): Separate Test Environments** Analyze changes to the system in a separate test environment before implementation in an operational environment. Focus on	

MARS-E		ARC-AMPE	
operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. **Implementation Standards** If Personally Identifiable Information (PII) is used in the test environment, then the same controls required for systems containing PII must be applied to the test environment. Simulated PII information should be used to the maximum extent practicable when testing system functionality.		security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.	
Control	**Verification of Security Functions**	**Control**	**Verification of Controls**
CM-4 (2): Verification of Security Functions The organization must ensure changes in information system security functions are verified: **a.** To be implemented per approved design; **b.** To integrate and operate as intended; and **c.** To produce expected results. **Implementation Standards** **1.** Any system, including development and test, that contains and/or processes sensitive information (e.g., PII) must verify security functions as per this control. **2.** The system's security functions must be continuously monitored and evaluated to ensure they are operating as intended and changes do not have an adverse effect on system performance. **3.** Actions must be taken to verify that the provisioned security function implementation being assessed and/or monitored meets security function requirements and is an approved system configuration.		**CM-04(02): Verification of Controls** After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.	
Control	**Access Restrictions for Change**	**Control**	**Access Restrictions for Change**
CM-5: Access Restrictions for Change The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.		**CM-05: Access Restrictions for Change** Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.	
Control	**Automated Access Enforcement/Auditing**	**Control**	**Automated Access Enforcement and Audit Records**
CM-5 (1): Automated Access Enforcement/Auditing The information system enforces access restrictions and supports auditing of the enforcement actions.		**CM-05(01): Automated Access Enforcement and Audit Records** **a.** Enforce access restrictions using automated mechanisms to the fullest extent possible; and **b.** Automatically generate audit records of the enforcement actions.	
Control	**Signed Components**	**Control**	**N/A**
CM-5 (3): Signed Components The information system prevents the installation of network and server software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.		**Withdrawn control**: Incorporated into **CM-14**.	

MARS-E		ARC-AMPE	
Control	**Limit Production/Operational Privileges**	**Control**	**Privilege Limitation for Production and Operation**
CM-5 (5): Limit Production/Operational Privileges The organization: **a.** Limits privileges to change information system components and system-related information within a production or operational environment; and **b.** Reviews and reevaluates privileges at least quarterly.		**CM-05(05): Privilege Limitation for Production and Operation** **a.** Limit privileges to change system components and system-related information within a production or operational environment; and **b.** Review and reevaluate privileges at least quarterly.	
Control	**Configuration Settings**	**Control**	**Configuration Settings**
CM-6: Configuration Settings The organization: **a.** Establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration guidelines listed in Implementation Standards that reflect the most restrictive mode consistent with operational requirements; **b.** Implements the configuration settings; **c.** Identifies, documents, and approves any deviations from established configuration settings for individual components within the information system based on explicit operational requirements; and **d.** Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. **Implementation Standards** **1.** Security configuration guidelines may be developed by different federal agencies. Therefore, it is possible that a guideline could include configuration information that conflicts with another agency or the organization's guideline. To resolve configuration conflicts among multiple security guidelines, the organization's hierarchy for implementing all security configuration guidelines is as follows: **a.** National Institute of Standards and Technology (NIST) **b.** Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) **2.** If formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group, such as The Center for Internet Security (CIS) checklists. **3.** The organization ensures that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).		**CM-06: Configuration Settings** **a.** Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using the most current security configuration guidelines listed in the Supplemental Control Requirements & Guidance; **b.** Implement the configuration settings; **c.** Identify, document, and approve any deviations from established configuration settings for all configurable system components based on explicit operational requirements; and **d.** Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	
Control	**Automated Central Management/ Application/Verification**	**Control**	**Automated Management, Application, and Verification**
CM-6 (1): Automated Central Management/Application/ Verification The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for information technology products.		**CM-06(01): Automated Management, Application, and Verification** Manage, apply, and verify configuration settings for Information Technology products and organization-defined system components using automated mechanisms.	

MARS-E		ARC-AMPE	
Control	**Least Functionality**	**Control**	**Least Functionality**
CM-7: Least Functionality The organization: **a.** Configures the information system to provide only essential capabilities; and **b.** Prohibits or restricts the use of high-risk system services, ports, network protocols, and capabilities (e.g., Telnet FTP, etc.) across network boundaries that are not explicitly required for system or application functionality. **c.** A list of specifically needed system services, ports, and network protocols will be maintained and documented in the applicable security plan; all others will be disabled. **Implementation Standards** **1.** The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: United States Government Configuration Baseline (USGCB)-defined list of prohibited or restricted functions, ports, protocols, and/or services. **2.** The organization shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. **3.** Configuration review information sources include systems, appliances, devices, services, and applications (including databases).		**CM-07: Least Functionality** **a.** Configure the system to provide only essential capabilities; and **b.** Prohibit or restrict the use of the following functions, ports protocols, software, and/or services: high-risk system services, functions, ports, network protocols, and capabilities across network boundaries that are not explicitly required for system or application functionality or are identified to be unnecessary and/or nonsecure.	
Control	**Periodic Review**	**Control**	**Periodic Review**
CM-7 (1): Periodic Review The organization: **a.** Reviews the information system no less often than once every thirty (30) days to identify and eliminate unnecessary functions, ports, protocols, and/or services; **b.** Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure; and **c.** Configuration review information sources include systems, appliances, devices, services, and applications (including databases). **Implementation Standards** **1.** Recommend the organization perform automated reviews of the information system no less often than once every seventy-two (72) hours to identify changes in functions, ports, protocols, and/or services.		**CM-07(01): Periodic Review** **a.** Review the system upon encountering a significant risk, as incidents occur, major system/software updates, or at least every one (1) year, to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and **b.** Disable or remove functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.	
Control	**Prevent Program Execution**	**Control**	**Prevent Program Execution**
CM-7 (2): Prevent Program Execution The information system prevents program execution in accordance with policies regarding authorized software use, which include, but are not limited to, the following:		**CM-07(02): Prevent Program Execution** Prevent program execution in accordance with organizational-defined policies, rules of behavior, and rules authorizing the terms and conditions of software program usage.	

MARS-E		ARC-AMPE	
a. Software must be legally licensed; **b.** Software must be provisioned in approved configurations; and **c.** Users must be authorized for software use.			
Control	**Authorized Software/Whitelisting**	**Control**	**Authorized Software – Allow by Exception**
CM-7 (5): Authorized Software/Whitelisting The organization: **a.** Identifies defined software programs (defined in the applicable security plan) authorized to execute on the information system; **b.** Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; **c.** Receives automated updates from a trusted source; and **d.** Authorizes software whitelisting (and blacklisting) information sources include systems, appliances, devices, services, and applications (including databases). **Implementation Standards** **1.** Recommend the organization review and updates the list of authorized software programs no less often than every seventy-two (72) hours.		**CM-07(05): Authorized Software – Allow by Exception** **a.** Identify software programs authorized to execute on the system; **b.** Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and **c.** Review and update the list of authorized software programs at least quarterly or when there is a change.	
Control	**N/A**	**Control**	**Prohibiting the Use of Unauthorized Hardware**
New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE.		**CM-07(09): Prohibiting the Use of Unauthorized Hardware** **a.** Identify hardware components authorized for system use; **b.** Prohibit the use or connection of unauthorized hardware components; and **c.** Review and update the list of authorized hardware components at least every one (1) year or when there is a change.	
Control	**Information System Component Inventory**	**Control**	**System Component Inventory**
CM-8: Information System Component Inventory The organization: **a.** Develops and documents an inventory of information system components that: **1.** Accurately reflects the current information system; **2.** Includes all components within the authorization boundary of the information system; **3.** Is at the level of granularity deemed necessary for tracking and reporting; and **4.** Includes organization-defined information deemed necessary to achieve effective property accountability, which may include hardware inventory specifications (e.g., manufacturer, type, model, serial number, and physical location); software license/version information; information system/component owner and type of information system component (e.g., server, desktop, application) and for a networked component/device, the machine name and network address; and the presence of virtual machines.		**CM-08: System Component Inventory** **a.** Develop and document an inventory of system components that: **1.** Accurately reflects the system; **2.** Includes all components within the system; **3.** Does not include duplicate accounting of components or components assigned to any other system; **4.** Is at the level of granularity deemed necessary for tracking and reporting; and **5.** Includes the following information to achieve proper system component accountability: – Each component's unique identifier and/or serial number; – Type of information system component (e.g., server, desktop, and application); – Manufacturer/model information; – Operating system type and version/service pack level; – Presence of virtual machines;	

<table>
<tr><th colspan="2">MARS-E</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">b. Reviews and updates the information system component inventory at least monthly or when there is a change, or per CM 8 (1), as applicable.

Implementation Standards
1. The organization defines information deemed necessary to achieve effective property accountability.
2. The organization establishes, maintains, and updates, within every three hundred sixty-five (365) days, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII.
3. The organization fully Integrate inventory of information system components with the organizational continuous monitoring capability (CM-7).
4. For cloud environment the organization reviews and updates the information system component inventory at least monthly or when there is a change, or per CM-8 (1), as applicable; this practice is also recommended for non-cloud environment.</td><td colspan="2">– Application software version/license information;
– Physical location (e.g., building/room number);
– Logical location (e.g., Internet Protocol [IP] address, position with the information system [IS]);
– Media access control (MAC) address;
– System/component owner;
– Operational status; and
– Information system/component administrators.
b. Review and update the system component inventory at least every six (6) months.</td></tr>
<tr><td>Control</td><td>Updates During Installations/Removals</td><td>Control</td><td>Updates During Installations and Removals</td></tr>
<tr><td colspan="2">CM-8 (1): Updates During Installations/Removals
The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.</td><td colspan="2">CM-08(01): Updates During Installations and Removals
Update the inventory of system components as part of component installations, removals, and system updates.</td></tr>
<tr><td>Control</td><td>Automated Unauthorized Component Detection</td><td>Control</td><td>Automated Unauthorized Component Detection</td></tr>
<tr><td colspan="2">CM-8 (3): Automated Unauthorized Component Detection
The organization:
a. Employs automated mechanisms to scan the network no less than weekly to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
b. Takes the following actions when unauthorized components are detected:
1. Disable access to the identified component;
2. Disable the identified component’s network access;
3. Isolate the identified component; and
4. Notify the responsible actor (i.e., person/ organization-defined in security plan).

Implementation Standards
In a cloud environment, the Service Provider:
1. Employs automated mechanisms to scan continuously, using automated mechanisms with a maximum (5) five-minute delay in detection to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
2. Disables network access by such components/devices or notifies designated organizational officials.</td><td colspan="2">CM-08(03): Automated Unauthorized Component Detection
a. Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms continuously, using automated mechanisms with a maximum five (5) minute delay in detection; and
b. Take the following actions when unauthorized components and/or provisioned configurations are detected:
– Disable network access by such components;
– Isolate the component; and
– Notify responsible personnel or role.</td></tr>
<tr><td>Control</td><td>No Duplicate Accounting of Components</td><td>Control</td><td>N/A</td></tr>
<tr><td colspan="2">CM-8 (5): No Duplicate Accounting of Components</td><td colspan="2">Withdrawn control: Incorporated into CM-8.</td></tr>
</table>

MARS-E		ARC-AMPE	
The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.			
Control	**Configuration Management Plan**	**Control**	**Configuration Management Plan**
CM-9: Configuration Management Plan The organization develops, documents, and implements a configuration management plan for the information system that: **a.** Addresses roles, responsibilities, and configuration management processes and procedures; **b.** Establishes a process for identifying and managing configuration items throughout the system development life cycle; **c.** Defines the configuration items for the information system; **d.** Places the configuration items under configuration management; and **e.** Protects the configuration management plan from unauthorized disclosure and modification.		**CM-09: Configuration Management Plan** Develop, document, and implement a configuration management plan for the system that: **a.** Addresses roles, responsibilities, and configuration management processes and procedures; **b.** Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; **c.** Defines the configuration items for the system and places the configuration items under configuration management; **d.** Is reviewed and approved by organization-defined personnel or roles (e.g., Business Owner and System Owner); and **e.** Protects the configuration management plan from unauthorized disclosure and modification.	
Control	**Software Usage Restrictions**	**Control**	**Software Usage Restrictions**
CM-10: Software Usage Restrictions The organization: **a.** Uses software and associated documentation in accordance with contract agreements and copyright laws; **b.** Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and **c.** Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.		**CM-10: Software Usage Restrictions** **a.** Use software and associated documentation in accordance with contract agreements and copyright laws; **b.** Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and **c.** Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	
Control	**Open Source Software**	**Control**	**N/A**
CM-10 (1): Open Source Software The organization establishes the organization-defined restrictions on the use of open source software.		**Withdrawn control**: No longer required for the minimum baseline but should still be considered best practice.	
Control	**User-Installed Software**	**Control**	**User-Installed Software**
CM-11: User-Installed Software The organization: **a.** Establishes organization-defined policies governing the installation of software by users; **b.** Enforces software installation policies through organization-defined methods; and **c.** Monitors policy compliance at least monthly. **Implementation Standards** **1.** Monitoring for user-installed software must comply with information security continuous monitoring (ISCM) requirements.		**CM-11: User-Installed Software** **a.** Establish organization-defined policies governing the installation of software by users; **b.** Enforce software installation policies through the organization-defined applicable System Security and Privacy Plan (SSPP); and **c.** Monitor policy compliance continuously.	

MARS-E		ARC-AMPE	
Control	**N/A**	**Control**	**Information Location**
New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE.		**CM-12: Information Location** **a.** Identify and document the location of organization-defined information and the specific system components on which the information is processed and stored; **b.** Identify and document the users who have access to the system and system components where the information is processed and stored; and **c.** Document changes to the location (i.e., system or system components) where the information is processed and stored.	
Control	**N/A**	**Control**	**Automated Tools to Support Information Location**
New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE.		**CM-12(01): Automated Tools to Support Information Location** Use automated tools to identify organization-defined information by information type on system components to ensure controls are in place to protect organizational information and individual privacy.	
Control	**N/A**	**Control**	**Data Action Mapping**
New NIST SP 800-53 Rev. 5 control and applicable to ARC-AMPE.		**CM-13: Data Action Mapping** Develop and document a map of system data actions.	

References

NIST SP 800-53 Revision 5.1.1

NIST SP 800-53 Revision 4

CMS Standards

Legal disclaimer

This white paper is provided by Coalfire Systems, Inc. or its subsidiaries (“Coalfire”) for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided “as-is” with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

About the authors

Ian Walters, Principal

Ian is a seasoned cybersecurity professional with a wealth of experience across a spectrum of frameworks and standards, including NIST SP 800-53, HIPAA, ISO 27001, ISO 20000, and ISO 9001.

With a meticulous eye for detail and a strategic mindset, Ian excels in developing tailored solutions to ensure compliance and mitigate risks within complex organizational environments. His expertise extends to leading audits and risk assessments, as well as providing advisory for driving continuous improvement initiatives to enhance cybersecurity posture and operational resilience.

Jessica Payne, Consultant

Jessica joined Coalfire in 2024 with five prior years of cybersecurity consulting experience. She supports our clients as a Consultant for the GRC Healthcare team where she specializes in cybersecurity risk management, cybersecurity program advisory, and compliance for the healthcare industry.

Her extensive experience in cybersecurity consulting allows her to provide customized solutions and guidance on industry best practices, greatly improving client security postures and ensuring compliance with regulatory standards. She is dedicated to ongoing improvement and to staying abreast of the latest cybersecurity trends and technologies to offer innovative solutions to her clients.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

Copyright © 2025 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward-looking statements are not predictions and are subject to change without notice. Coalfire is not responsible for any errors or omissions.

WP_ACA CMS Controls Migration (Configuration Management (CM))_03262025