COALFIRE

WHITE PAPER

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

CMS requirements for Direct Enrollment Entities

JESSICA PAYNE, CONSULTANT
IAN WALTERS, PRINCIPAL

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

Table of contents

Purpose

This white paper provides a guide for Direct Enrollment Entities (DEEs) to upgrade their Enhanced Direct Enrollment (EDE) System Security and Privacy Plans (SSPPs) 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 controls.

ARC-AMPE Control Families	
Control Family	**Number of Controls**
Access Control	46
Awareness and Training	9
Audit and Accountability	18
Assessment, Authorization, and Monitoring	12
Configuration Management (This Document)	**25**
Contingency Planning	16
Identification and Authentication	21
Incident Response	15
Maintenance	12
Media Protection	8
Physical and Environmental Protection	9
Planning	6
Program Management	5
Personnel Security	8
Personally Identifiable Information Processing and Transparency	10
Risk Assessment	8
System and Services Acquisition	18
System and Communications Protection	28
System and Information Integrity	30
Supply Chain Risk Management	4

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.

Enhanced Direct Enrollment

> *Direct Enrollment (DE) is a service that allows approved Qualified Health Plan (QHP) issuers and third-party web-brokers (online insurance sellers) to enroll consumers in Exchange coverage, with or without the assistance of an agent/broker, directly from their websites.*
>
> *The Enhanced Direct Enrollment (EDE) user experience goes well beyond the plan shopping and enrollment experience that is available via Classic DE. EDE is a service that allows approved EDE entities (e.g., QHP issuers and web-brokers approved to participate in EDE) to provide a comprehensive consumer experience including the eligibility application, Exchange enrollment, and post-enrollment year-round customer service capabilities for consumers and agents/brokers working on behalf of consumers, directly on issuer and web-broker websites. Through EDE, approved EDE Entities build and host a version of the HealthCare.gov eligibility application directly on their websites that securely integrates with a back-end suite of Federally Facilitated Exchanges (FFEs) application programing interfaces (APIs) to support application, enrollment and more.*
>
> Source: cms.gov

CMS oversight

The Centers for Medicare & Medicaid Services (CMS) exercises oversight of DEEs, 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 DEEs to undergo rigorous audit processes, including demonstrating compliance with security and privacy control requirements.
- Enforcing strict data protection measures in the DE 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 DEEs to adhere to operational policies and procedures, such as providing accurate plan information, maintaining transparent consumer interactions, and facilitating HIM enrollment without bias.
- Requiring DEEs 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 DEEs to renew their Authority to Connect (ATC) annually, providing updated documentation and evidence of continued compliance with all requirements.

Through these oversight mechanisms, CMS ensures that DEEs 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 for Direct Enrollment Entities (DEEs) Version 1.0 dated July 7th, 2025. This framework replaces the EDE 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 DEEs.
- The compliance date for DEEs is June 2026.

The minimum control baseline for ARC-AMPE DEE compliance consists of 308 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 for the mandatory baseline represents a significant increase from the EDE baseline (295 controls), and DEEs should be prepared for an increased level of effort for developing the SSPP and submitting more artifacts during audits.

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

Control mapping

The mapping of the controls found in the EDE audit baseline (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 EDE 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 EDE 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.

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td>Control</td><td>Configuration Management Policy and Procedures</td><td>Control</td><td>Policy and Procedures</td></tr>
<tr><td colspan="2">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:
a. Define configuration items at t he system and component level (e.g., hardware, software, and workstation);
b. Monitor configurations; and
c. Track and approve changes prior to implementation, including but not limited to, flaw remediation, security patches, and emergency changes (e.g., unscheduled changes such as mitigating newly discovered security vulnerabilities, system crashes, and replacement of critical hardware components).</td><td colspan="2">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.</td></tr>
<tr><td>Control</td><td>Baseline Configuration</td><td>Control</td><td>Baseline Configuration</td></tr>
<tr><td colspan="2">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.</td><td colspan="2">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.</td></tr>
</table>

EDE		ARC-AMPE	
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 information system component installations, upgrades, and updates to applicable governing standards (implemented within the 365 days specified in number 1 above); and **d.** Supporting baseline configuration documentation reflects ongoing implementation of operational configuration baseline updates, either directly or by policy **Implementation Standards** The organization reviews and updates the baseline configuration of the information system: a. Annually; b. When required due to a significant change; and c. As an integral part of information system component installations and upgrades.		**Withdrawn control**: Incorporated into **CM-02**.	
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** **1.** Following baseline configuration updates, no less than one (1) older baseline configuration must be maintained (e.g., for emergency rollback).		**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.	
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;		**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	

EDE	ARC-AMPE
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 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.	**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.
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 **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 and privacy impact analysis is recommended as part of change management.	**CM-04: Impact Analyses** Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.

EDE		ARC-AMPE	
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 operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.		**CM-04(01): Separate Test Environments** Analyze changes to the system in a separate test environment before implementation in an operational environment. Focus on security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.	
Control	**N/A**	**Control**	**Verification of Controls**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**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	**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 Standard 1 that reflect the most restrictive mode consistent with operational requirements;		**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	

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">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 (defined in the applicable system security plan); 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. NIST;
b. CMS;
c. Defense Information Systems Agency (DISA), Security Technical Implementation Guides (STIG);
d. Office of Management and Budget (OMB);
e. U.S. Government Configuration Baselines (USGCB),
2. The organization must use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establish own configuration settings if USGCB is not available.
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).</td><td colspan="2">system components based on explicit operational requirements; and
d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.</td></tr>
<tr><td>Control</td><td>Automated Central Management/ Application/Verification</td><td>Control</td><td>Automated Management, Application, and Verification</td></tr>
<tr><td colspan="2">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.</td><td colspan="2">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.</td></tr>
<tr><td>Control</td><td>Least Functionality</td><td>Control</td><td>Least Functionality</td></tr>
<tr><td colspan="2">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</td><td colspan="2">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</td></tr>
</table>

EDE		ARC-AMPE	
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.		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 at least quarterly to identify and eliminate unnecessary functions, ports, protocols, and/or services; **b.** Performs periodic review at least quarterly of the information system to identify changes in functions, ports, protocols, and/or services; and **c.** Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.		**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: **a.** Software must be legally licensed; **b.** Software must be provisioned in approved configurations; and **c.** Users must be authorized for software use.		**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.	
Control	**Unauthorized Software / Blacklisting**	**Control**	**N/A**
CM-7 (4): Unauthorized Software / Blacklisting The organization: **a.** Identifies defined software programs (defined in the applicable security plan) not authorized to execute on the information system; **b.** Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system;		**Withdrawn Control:** Incorporated into CM-07(05)	

EDE		ARC-AMPE	
c. Reviews and updates the list of unauthorized software programs quarterly; and **d.** Receives automated updates from a trusted source.			
Control	**N/A**	**Control**	**Authorized Software - Allow by Exception**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**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	**Information System Component Inventory**	**Control**	**System Component Inventory**
CM-8: Information System Component Inventory The organization: a. aDevelops 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: a. Each component's unique identifier and/or serial number; b. Information system of which the component is a part; c. Type of information system component (e.g., server, desktop, application); d. Manufacturer/model information; e. Operating system type and version/service pack level; f. Presence of virtual machines; g. Application software version/license information; h. Physical location (e.g., building/room number); i. Logical location (e.g., IP address, position with the information system [IS] architecture); j. Media access control (MAC) address; k. Ownership; l. Operational status; m. Primary and secondary administrators; and n. Primary user. b. Reviews and updates the information system component inventory no less than every three hundred sixty-five (365) days, or per CM 8 (1) and/or CM 8 (2), as applicable.		**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; – 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.	

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">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 personally identifiable information (PII).
3. Fully integrate inventory of information system components with the organizational continuous monitoring capability.
4. Automated asset inventory information tracking systems must:
a. Transmit updates to organization based upon organizational defined frequency;
5. Automated component tracking and management tool results must be searchable by the organization:
a. Information is provided to the organization in a format compliant with organizational defined continuous monitoring requirements;
b. Authorized component information sources include systems, platforms, appliances, devices;
c. Component information sources that do not support the exchange of information with the organization must be documented in the applicable risk assessment and security plan; and
d. Organization directed authorized component information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
6. Raw security information/results from relevant automated tools must be available in an unaltered format to the organization.</td><td colspan="2"></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:</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</td></tr>
</table>

EDE		ARC-AMPE	
6. Disable access to the identified component; **7.** Disables network access by such components/devices; **8.** Isolates the identified component; and **9.** Notifies defined personnel or roles (defined in the applicable security plan). **Implementation Standards** In a shared computing facility, the organization: 1. Employs automated mechanisms to scan continuously, using automated mechanisms with a maximum (5) five-minute delay in detection to detect the addition of unauthorized components/devices into the information system; and 2. Disables network access by such components/devices or notifies designated organizational officials.		**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.	
Control	**No Duplicate Accounting of Components**	**Control**	**N/A**
CM-8 (5): No Duplicate Accounting of Components The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.		**Withdrawn control**: Incorporated into **CM-8**.	
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. **f.** Reviews and updates (as necessary) the current configuration management plan within every year.		**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		**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.	

EDE		ARC-AMPE	
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 restrictions on the use of open source software. Open source software must: a. Be legally licensed; b. Approved by the agency information technology department; and c. Adhere to a secure configuration baseline checklist from the U.S. Government or industry		**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 organization-defined frequency. **Implementation Standard** Monitoring for user-installed software must comply with organizational defined continuous monitoring 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.	
Control	**N/A**	**Control**	**Information Location**
New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE		**CM-12: Information Location** **d.** Identify and document the location of organization-defined information and the specific system components on which the information is processed and stored; **e.** Identify and document the users who have access to the system and system components where the information is processed and stored; and **f.** Document changes to the location (i.e., system or system components) where the information is processed and stored.	
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

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**.

WP_ACA CMS Controls Migration (Configuration Management (CM))_07142025