COALFIRE

WHITE PAPER

Migration from MARS-E to ARC-AMPE Audit and Accountability (AU) 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 **5**
Control mapping **6**
Audit and Accountability (AU) 6
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 Audit and Accountability controls:

ARC-AMPE Control Families	
Control Family	**Number of Controls**
Access Control	51
Awareness and Training	9
Audit and Accountability (This Document)	**19**
Assessment, Authorization, and Monitoring	12
Configuration Management	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.

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 from 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.

Audit and Accountability (AU)

The set of controls in this family focus on how the Exchange shall: (1) create, protect, and retain IT system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate IT system activity; and (2) ensure that the actions of individual IT system users can be uniquely traced to those users so they can be held accountable for their actions.

MARS-E		ARC-AMPE	
Control	**Audit and Accountability Policy and Procedures**	**Control**	**Policy and Procedures**
AU-1: Audit and Accountability Policy and Procedures The organization: **a.** Develops, documents, and disseminates to applicable personnel: **1.** An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and **b.** Reviews and updates (as necessary) the current: **1.** Audit and accountability policy at least every three hundred sixty-five 365 days; and **2.** Audit and accountability procedures at least every three hundred sixty-five 365 days.		**AU-01: Policy and Procedures** **a.** Develop, document, and disseminate to organization-defined personnel and roles: **1.** Organization-level audit and accountability 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 audit and accountability policy and the associated audit and accountability controls; **b.** Designate an organization-defined official to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and **c.** Review and update the current audit and accountability: **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.	
Control	**Audit Events**	**Control**	**Event Logging**
AU-2: Audit Events The organization: **a.** Determines, based on a risk assessment and mission/business needs, that the information system is capable of auditing the following events: **1.** Server alerts and error messages;		**AU-02: Event Logging** **a.** Identify the types of events that the system is capable of logging in support of the audit function: organization-defined event types based on a risk assessment of organization defined mission/business needs; **b.** Coordinate the event logging function with other organizational entities requiring audit-related information	

MARS-E	ARC-AMPE
i. User log-on and log-off (successful or unsuccessful); ii. All system administration activities; iii. Modification of privileges and access; iv. Start up and shut down; v. Application modifications; vi. Application alerts and error messages; vii. Configuration changes; viii. Account creation, modification, or deletion; ix. File creation and deletion; x. Read access to sensitive information; xi. Modification to sensitive information; xii. Printing sensitive information; xiii. Anomalous (e.g., non-attributable) activity; xiv. Data as required for privacy monitoring privacy controls; xv. Concurrent log on from different workstations; xvi. Override of access control mechanisms; xvii. Process creation; xviii. System access, including unsuccessful and successful login attempts, to information systems containing personally identifiable information (PII); xix. Successful and unsuccessful attempts to create, read, write, modify, and/or delete extracts containing PII from a database or data repository; xx. Privileged activities or system level access to PII; xxi. Concurrent logons from different workstations; and xxii. All program initiations, e.g., executable file. **b.** Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; and **c.** Provides a rationale for why the auditable events are deemed to be adequate (relevant) to support after-the-fact investigations of security and privacy incidents; and **d.** Determines, based on current threat information and ongoing assessment of risk, which events in the following list require auditing on a continuous basis and which events require auditing in response to specific situations: **1.** User log-on and log-off (successful or unsuccessful); i. Configuration changes; ii. Application alerts and error messages; iii. All system administration activities; iv. Modification of privileges and access; v. Account creation, modification, or deletion; vi. Concurrent log on from different workstations; and vii. Override of access control mechanisms. viii. System access, including unsuccessful and successful login attempts, to information systems containing PII; ix. Successful and unsuccessful attempts to create, read, write, modify, and/or delete extracts containing PII from a database or data repository;	to guide and inform the selection criteria for events to be logged; **c.** Specify the following event types for logging within the system: organization-defined event types along with organization-defined frequency or situation for each identified event type; **d.** Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and **e.** Review and update the event types selected for logging at least every one (1) year and whenever there is a significant system modification or change in the system environment. • *Incorporates withdrawn control **AU-2(3)**.* • *Incorporates audit elements of withdrawn **App J control UL-2**.*

MARS-E		ARC-AMPE	
x. Privileged activities or system level access to PII; xi. Concurrent logons from different workstations; and xii. All program initiations, e.g., executable file. xiii. Verify that proper logging is enabled to audit administrator activities. **e.** For Cloud Environment, the organization defines the events to be audited. The events to be audited are accepted and approved by the Authorizing Official.			
Control	**Reviews and Updates**	**Control**	**N/A**
AU-2 (3): Reviews and Updates The organization reviews and updates the list of auditable events no less often than every three hundred sixty-five (365) days and whenever there is a significant system modification. **Implementation Standards** The organization reviews and updates the list of auditable events as per the frequency defined in this control or whenever there is a change in the threat environment. The System Owner reviews and approves the list of auditable events.		**Withdrawn Control**: Incorporated into **AU-02**.	
Control	**Content of Audit Records**	**Control**	**Content of Audit Records**
AU-3: Content of Audit Records The information system generates audit records containing information that specifies: **a.** Date and time of the event; **b.** Component of the information system (e.g., software component, hardware component) where the event occurred; **c.** Type of event; **d.** User/subject identity; **e.** Outcome (success or failure) of the event; **f.** Execution of privileged functions; and **g.** Command line (for process creation events). **Implementation Standards** Record disclosures of sensitive information, including protected health and financial information. Log information type, date, time, receiving party, and releasing party. Verify within every ninety (90) days for each extract that the data is erased, or its use is still required.		**AU-03: Content of Audit Records** Ensure that audit records contain information that establishes the following: **a.** What type of event occurred; **b.** When the event occurred; **c.** Where the event occurred; **d.** Source of the event; **e.** Outcome of the event; and **f.** Identity of any individuals, subjects, or objects/entities associated with the event.	
Control	**Additional Audit Information**	**Control**	**Additional Audit Information**
AU-3 (1): Additional Audit Information **a.** The information system provides the capability to include more detailed information in the audit records for audit events that capture: **1.** Filename accessed; **2.** Program or command used to initiate the event; and **3.** Source and destination addresses.		**AC-03(01): Additional Audit Information** Generate audit records containing the following additional information and event details explicitly needed for audit requirements: **a.** Session, connection, transaction, or activity duration; **b.** For client-server transactions, the number of bytes received and bytes sent; **c.** Additional informational messages to diagnose or identify the event;	

<table>
<tr><th colspan="2">MARS-E</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">Implementation Standards
Required for Cloud Environment; recommended for non-cloud environment:
1. The information system generated audit records include:
a. More detailed session, connection, transaction, or activity duration information;
b. For client-server transactions, the number of bytes received and bytes sent;
c. Additional informational messages to diagnose or identify the event; and
d. Characteristics that describe or identify the object or resource being acted upon in the audit records for audit events identified by type, location, or subject.
2. The organization defines audit record types. The audit record types are approved and accepted by the System Owner.</td><td colspan="2">d. Characteristics that describe or identify the object or resource being acted upon;
e. Individual identities of group account users; and
f. Full-text of privileged commands.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Limit Personally Identifiable Information Elements</td></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.</td><td colspan="2">AU-03(03): Limit Personally Identifiable Information Elements
Limit Personally Identifiable Information (PII) contained in audit records to the defined elements identified in the privacy risk assessment: system-defined elements in the Privacy Impact Assessment (PIA).</td></tr>
<tr><td>Control</td><td>Audit Storage Capacity</td><td>Control</td><td>Audit Log Storage Capacity</td></tr>
<tr><td colspan="2">AU-4: Audit Storage Capacity
The organization allocates audit record storage capacity and configures auditing to reduce the likelihood that storage capacity will be exceeded.

Implementation Standards
Capacity must be sufficient to handle auditing records during peak performance times (e.g., open enrollment).</td><td colspan="2">AU-04: Audit Log Storage Capacity
Allocate audit log storage capacity to accommodate, at a minimum, storage capacity of ninety (90) days and any other organization-defined audit log retention requirements.</td></tr>
<tr><td>Control</td><td>Response to Audit Processing Failures</td><td>Control</td><td>Response to Audit Logging Processing Failures</td></tr>
<tr><td colspan="2">AU-5: Response to Audit Processing Failures
The information system:
a. Alerts defined personnel or roles (defined in the applicable system security plan) in the event of an audit processing failure; and
b. Takes the actions defined in Implementation Standard 1 in response to an audit failure or audit storage capacity issue.

Implementation Standards
1. The information system takes the following action in response to an audit failure or audit storage capacity issue:
a. Shut down the information system or halt processing immediately; and</td><td colspan="2">AU-05: Response to Audit Logging Processing Failures
a. Alert organization-defined personnel or roles within near real-time in the event of an audit logging process failure; and
b. Take the following additional actions:
• Shut down the system or halt processing immediately; or
• Shut down systems that do not support automatic shutdown within one (1) hour of the audit processing failure.</td></tr>
</table>

MARS-E		ARC-AMPE	
b. Systems that do not support automatic shutdown must be shut down within 24 hours of the audit processing failure.			
Control	**Audit Review, Analysis, and Reporting**	**Control**	**Audit Record Review, Analysis, and Reporting**
AU-6: Audit Review, Analysis, and Reporting The organization: **a.** Reviews and analyzes information system audit records no less often than weekly for indications of inappropriate or unusual activity as defined within the Implementation Standards; **b.** Reports findings to defined personnel or roles (defined in the applicable system security plan); and **c.** For Cloud Environment, the Authorizing Official shall document and accept the coordination between service provider and organization. In multi-tenant environments, the capability and means for providing review, analysis, and reporting to the organization for data pertaining to consumer shall be documented. **Implementation Standards** **1.** Review system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, and firewall), applications, performance, and system resource utilization to determine anomalies no less often than once within a twenty-four (24)-hour period and on demand. Generate alert notification for technical personnel review and assessment. **2.** Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies no less often than once within a twenty-four (24)-hour period and on demand. Generate alerts for technical personnel review and assessment. **3.** Investigate suspicious activity or suspected violations on the information system, and report findings to appropriate officials and take appropriate action. **4.** Use automated utilities to review audit records at least once every seventy-two (72) hours for unusual, unexpected, or suspicious behavior. **5.** Inspect administrator groups on demand but no less often than once every fourteen (14) days to ensure unauthorized administrator, system, and privileged application accounts have not been created. **6.** Perform manual reviews of system audit records randomly on demand but no less often than once every thirty (30) days.		**AU-06: Audit Record Review, Analysis, and Reporting** **a.** Review and analyze system audit records no less often than weekly (every seven [7] days) for indications of organization-defined inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity; **b.** Report findings to organization-defined personnel or roles; and **c.** Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.	
Control	**Process Integration**	**Control**	**Automated Process Integration**
AU-6(1): Process Integration The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. **Implementation Standards**		**AU-06(01): Automated Process Integration** Integrate audit record review, analysis, and reporting processes using automated mechanisms to the fullest extent possible.	

MARS-E		ARC-AMPE	
Audit record sources include systems, appliances, devices, services, and applications (including databases).			
Control	**Correlate Audit Repositories**	**Control**	**Correlate Audit Record Repositories**
AU-6 (3): Correlate Audit Repositories The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. **Implementation Standards** Repository sources include systems, appliances, devices, services, and applications (including databases).		**AU-06(03): Correlate Audit Record Repositories** Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.	
Control	**Audit Reduction and Report Generation**	**Control**	**Audit Record Reduction and Report Generation**
AU-7: Audit Reduction and Report Generation The information system provides an audit reduction and report generation capability that: **a.** Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and **b.** Does not alter the original content or time marking of audit records.		**AU-07: Audit Record Reduction and Report Generation** Provide and implement an audit record reduction and report generation capability that: **a.** Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and **b.** Does not alter the original content or time ordering of audit records.	
Control	**Automatic Processing**	**Control**	**Automatic Processing**
AU-7 (1): Automatic Processing The information system provides the capability to process audit records for events of interest based on selectable event criteria.		**AU-07(01): Automatic Processing** Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: organization-defined selectable event criteria and fields within audit records.	
Control	**Time Stamps**	**Control**	**Time Stamps**
AU-8: Time Stamps The information system: **a.** Uses internal system clocks to generate time stamps for audit records; and **b.** Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and are accurate to within one hundred (100) milliseconds.		**AU-08: Time Stamps** **a.** Use internal system clocks to generate time stamps for audit records; and **b.** Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and are accurate to within one hundred (100) milliseconds.	
Control	**Synchronization with Authoritative Time Source**	**Control**	**N/A**
AU-8 (1): Synchronization with Authoritative Time Source The information system: **a.** Compares the internal information system clocks no less often than daily and at system boot with one or more of the following federally maintained NTP stratum-1 servers: **1.** NIST Internet Time Servers (http://tf.nist.gov/tf-cgi/servers.cgi)		**Withdrawn Control**: Incorporated into **SC-45(1)**.	

<table>
<tr><th colspan="2">MARS-E</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">2. U.S. Naval Observatory Stratum-1 NTP Servers (http://tycho.usno.navy.mil/ntp.html); and
3. CMS-designated internal NTP time servers providing an NTP Stratum-2 service to the foregoing servers; and
b. Synchronizes the internal clocks to the authoritative time source when the time difference is greater than one hundred (100) milliseconds.

Implementation Standards
For Cloud Environment:
1. The information system synchronizes internal information system clocks at least hourly with: http://tf.nist.gov/tf-cgi/servers.cgi
2. The organization selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server.
3. The organization synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.</td><td colspan="2"></td></tr>
<tr><td>Control</td><td>Protection of Audit Information</td><td>Control</td><td>Protection of Audit Information</td></tr>
<tr><td colspan="2">AU-9: Protection of Audit Information
The information system protects audit information and audit tools from unauthorized access, modification, and deletion.</td><td colspan="2">AU-09: Protection of Audit Information
a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and
b. Alert organization-defined personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.</td></tr>
<tr><td>Control</td><td>Audit Backup on Separate Physical Systems / Components</td><td>Control</td><td>N/A</td></tr>
<tr><td colspan="2">AU-9 (2): Audit Backup on Separate Physical Systems / Components (For Cloud Environment and Recommended for Non-Cloud Environments)
The information system backs up audit records no less often than weekly onto a physically different system or system component than the system or component being audited.</td><td colspan="2">Withdrawn Control: No longer required for the minimum baseline but should still be considered a best practice.</td></tr>
<tr><td>Control</td><td>Access by Subset of Privileged Users</td><td>Control</td><td>Access by Subset of Privileged Users</td></tr>
<tr><td colspan="2">AU-9 (4): Access by Subset of Privileged Users
The organization authorizes access to management of audit functionality to only those individuals or roles who are not subject to audit by that system and defines this access in the applicable security plan.</td><td colspan="2">AU-09(04): Access by Subset of Privileged Users
Authorize access to management of audit logging functionality to only an organization-defined subset of privileged users or roles.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Non-Repudiation</td></tr>
<tr><td colspan="2">Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.</td><td colspan="2">AU-10: Non-Repudiation
Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed organization-defined actions to be covered by non-repudiation.</td></tr>
<tr><td>Control</td><td>Audit Record Retention</td><td>Control</td><td>Audit Record Retention</td></tr>
</table>

MARS-E	ARC-AMPE
AU-11: Audit Record Retention The organization retains audit records online for at least ninety (90) days and archives old records for ten (10) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. **Implementation Standards** **1.** When subject to a legal investigation (e.g., Insider Threat), audit records must be maintained until released by the investigating authority. **2.** Audit record retention must comply with National Archives and Records Administration (NARA) or other authoritative mandate durations. **3.** Audit inspection reports, including a record of corrective actions, are retained by the organization for a minimum of three (3) years from the date the inspection was completed. **4.** The organization retains audit records online for at least ninety (90) days and further preserves audit records offline for a period that is in accordance with NARA requirements.	**AU-11: Audit Record Retention** Retain audit records for ninety (90) days and archive old records for ten (10) years consistent with records retention policy to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.
Control **N/A**	**Control** **Long-Term Retrieval Capability**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.	**AU-11(01): Long-Term Retrieval Capability** Employ organization-defined measures to ensure that long-term audit records generated by the system can be retrieved.
Control **Audit Generation**	**Control** **Audit Record Generation**
AU-12: Audit Generation The information system: **a.** Provides audit record generation capability for all auditable events defined in AU-2 and associated implementation standards including requirements of 5 U.S.C §552a(c), Accounting of Certain Disclosures. **1.** All successful and unsuccessful authorization attempts; **2.** All changes to logical access control authorities (e.g., rights and permissions); **3.** All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations, and audit record generation services; **4.** The audit trail that must capture the enabling or disabling of audit report generation services; and **5.** The audit trail must capture command line changes, batch file changes, and queries made to the system (e.g., operating system, application, and database). **b.** Allows defined personnel or roles (defined in the applicable security plan) to select which auditable events are to be audited by specific components of the information system; and **c.** Generates audit records for the list of events defined in AU-2 with the content defined in AU-3.	**AU-12: Audit Record Generation** **a.** Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on all systems and network components where audit capability is deployed/available; **b.** Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system; and **c.** c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

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

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.

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.

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 (Audit and Accountability (AU))_03102025