COALFIRE

WHITE PAPER

Migration from MARS-E to ARC-AMPE Program Management (PM) controls

CMS requirements for Administering Entities

IAN WALTERS, PRINCIPAL
JESSICA PAYNE, CONSULTANT

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**
Program Management (PM) 4
References **13**
Legal disclaimer **14**

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 Program Management 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	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 (This Document)	**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.

Program Management (PM)

The set of controls in this family complement the security controls in the foregoing 19 security control families by focusing on the organization-wide information security requirements that are essential for managing information security programs.

MARS-E		ARC-AMPE	
Control	**Information Security Program Plan**	**Control**	**Information Security Program Plan**
PM-1: Information Security Program Plan The organization: **a.** Develops and disseminates an organization-wide information security program plan that: **1.** Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; **2.** Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; **3.** Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, and cyber-physical); and **4.** Is approved by a senior official with responsibility and accountability for the risk incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; **b.** Reviews the organization-wide information security program plan within every three hundred sixty-five (365) days; **c.** Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and **d.** Protects the information security program plan from unauthorized disclosure and modification		**PM-01: Information Security Program Plan** **a.** Develop and disseminate an organization-wide information security program plan that: **1.** Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; **2.** Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; **3.** Reflects the coordination among organizational entities responsible for information security; and **4.** Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; **b.** Review and update the organization-wide information security program plan at least every one (1) year and following organization-defined events; and **c.** Protect the information security program plan from unauthorized disclosure and modification.	

MARS-E		ARC-AMPE	
Control	**Senior Information Security Officer**	**Control**	**Information Security Program Leadership Role**
PM-2: Senior Information Security Officer The organization appoints a senior information security officer with the responsibility and resources to coordinate, develop, implement, and maintain an organization-wide information security program.		**PM-02: Information Security Program Leadership Role** Appoint a Senior Information Security Officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	
Control	**Information Security Resources**	**Control**	**Information Security and Privacy Resources**
PM-3: Information Security Resources The organization: **a.** Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; **b.** Employs a business case to record the resources required; and **c.** Ensures that information security resources are available for expenditure as planned.		**PM-03: Information Security and Privacy Resources** **a.** Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; **b.** Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards; and **c.** Make the planned information security and privacy resources available for expenditure.	
Control	**Plan of Action and Milestones Process**	**Control**	**Plan of Action and Milestones Process**
PM-4: Plan of Action and Milestones Process The organization: **a.** Implements a process to ensure that plans of action and milestones (POA&M) for the security program and associated organizational information systems: **1.** Are developed and maintained; **2.** Document the remedial information security actions to adequately respond to risks to organizational operations and assets, individuals, other organizations, and the Nation; and **3.** Are reported in accordance with organizational and CMS reporting requirements; **b.** Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.		**PM-04: Plan of Action and Milestones Process** **a.** Implement a process to ensure that Plans of Action and Milestones (POA&M) for the information security, privacy, and supply chain risk management programs and associated organizational systems: **1.** Are developed and maintained; **2.** Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and **3.** Are reported in accordance with established reporting requirements. **b.** Review POA&Ms for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	
Control	**Information System Inventory**	**Control**	**System Inventory**
PM-5: Information System Inventory The organization develops and maintains an inventory of its information systems.		**PM-05: System Inventory** Develop and update an inventory of the organizational systems at least every one (1) year or when there is a significant change to the inventory.	
Control	**N/A**	**Control**	**Inventory of Personally Identifiable Information**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**PM-05(01): Inventory of Personally Identifiable Information** Establish, maintain, and update an inventory of all systems, applications, and projects that process Personally Identifiable Information (PII) continuously or when there is a significant change to the systems, applications, and projects that process PII.	

MARS-E		ARC-AMPE	
Control	**Information Security Measures of Performance**	**Control**	**Measures of Performance**
PM-6: Information Security Measures of Performance The organization develops, monitors, and reports on the results of information security measures of performance to evaluate the effectiveness of IT security and privacy policies, procedures, and controls. The measures and metrics must provide information on measures of implementation, efficiency, effectiveness, and impact.		**PM-06: Measures of Performance** Develop, monitor, and report on the results of information security and privacy measures of performance.	
Control	**Enterprise Architecture**	**Control**	**Enterprise Architecture**
PM-7: Enterprise Architecture The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.		**PM-07: Enterprise Architecture** Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.	
Control	**Critical Infrastructure Plan**	**Control**	**Critical Infrastructure Plan**
PM-8: Critical Infrastructure Plan The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan		**PM-08: Critical Infrastructure Plan** Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	
Control	**Risk Management Strategy**	**Control**	**Risk Management Strategy**
PM-9: Risk Management Strategy The organization: **a.** Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; **b.** Implements the risk management strategy consistently across the organization; and **c.** Reviews and updates the risk management strategy at least every three hundred sixty-five (365) days or as required, to address organizational changes. The risk management strategy must include a process to evaluate and address privacy risks for individuals and information (data) such as risk to individual, risk to the system, risk to the organization, and risk to the enterprise. In addition to business risks that arise out of privacy violations, such as reputation or liability risks, organizational policies should also focus on minimizing the risk of harm to individuals.		**PM-09: Risk Management Strategy** **a.** Develop a comprehensive strategy to manage: **1.** Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and **2.** Privacy risk to individuals resulting from the authorized processing of Personally Identifiable Information (PII); **b.** Implement the risk management strategy consistently across the organization; and **c.** Review and update the risk management strategy at least every one (1) year or as required, to address organizational changes.	
Control	**Security Authorization Process**	**Control**	**Authorization Process**
PM-10: Security Authorization Process The organization: **a.** Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes;		**PM-10: Authorization Process** **a.** Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes; **b.** Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and	

MARS-E	ARC-AMPE
b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and **c.** Fully integrates the security authorization processes into an organization-wide risk management program. The organization's Authorizing Official: **a.** Grants/denies the Authorization to Operate (ATO) based on the evaluation of security risks; **b.** Manages the established Authority to Connect (ATC) process; **c.** If the organization maintains a system-to-system connection with CMS through an executed Interconnection Security Agreement with CMS, CMS grants/denies the "Authority to Connect"; and **d.** Grants/denies the authorization to establish system-to-system connections with other external entities. The organization's security authorization process must ensure privacy safeguards and privacy documentation requirements, such as privacy impact assessments (PIA), have been appropriately addressed prior to any security authorization.	**c.** Integrate the authorization processes into an organization-wide risk management program.
Control **Mission/Business Process Definition**	**Control** **Mission and Business Process Definition**
PM-11: Mission/Business Process Definition The organization: **a.** Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and **b.** Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained. When defining mission/business processes for information security and identifying resulting risks, the organization must address the privacy risks stemming from those processes.	**PM-11: Mission and Business Process Definition** **a.** Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and **b.** Determine information protection and Personally Identifiable Information (PII) processing needs arising from the defined mission and business processes; and **c.** Review and revise the mission and business processes at least every three (3) years or when significant changes to mission and business occur.
Control **Insider Threat Program**	**Control** **Insider Threat Program**
PM-12: Insider Threat Program The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team. When defining the requirements for and designing an organization's insider threat program, the insider threat team must engage the participation of, and obtain concurrence from the organization's Privacy Officer prior to implementation. For existing insider threat programs, conduct a review of the program with the organization's Privacy Officer to ensure program meets applicable privacy requirements	**PM-12: Insider Threat Program** Implement an insider threat program that includes a cross-discipline insider threat incident handling team.
Control **Information Security Workforce**	**Control** **Security and Privacy Workforce**
PM-13: Information Security Workforce The organization establishes an information security workforce development and improvement program.	**PM-13: Security and Privacy Workforce** Establish a security and privacy workforce development and improvement program.

MARS-E		ARC-AMPE	
Control	**Testing, Training, and Monitoring**	**Control**	**Testing, Training, and Monitoring**
PM-14: Testing, Training, and Monitoring The organization: **a.** Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: **1.** Are developed and maintained; **2.** Continue to be executed in a timely manner; and **b.** Reviews testing, training, and monitoring plans for consistency with the organizational privacy risk management strategy and organization-wide priorities for risk response actions.		**PM-14: Testing, Training, and Monitoring** **a.** Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems: **1.** Are developed and maintained; and **2.** Continue to be executed; and **b.** Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	
Control	**Contacts with Security Groups and Associations**	**Control**	**Security and Privacy Groups and Associations**
PM-15: Contacts with Security Groups and Associations The organization establishes and institutionalizes contact with selected groups and associations within the security community: **a.** To facilitate ongoing security education and training for organizational personnel; **b.** To maintain currency with recommended security practices, techniques, and technologies; and **c.** To share current security-related information including threats, vulnerabilities, and incidents.		**PM-15: Security and Privacy Groups and Associations** Establish and institutionalize contact with selected groups and associations within the security and privacy communities: **a.** To facilitate ongoing security and privacy education and training for organizational personnel; **b.** To maintain currency with recommended security and privacy practices, techniques, and technologies; and **c.** To share current security and privacy information, including threats, vulnerabilities, and incidents.	
Control	**Threat Awareness Program**	**Control**	**Threat Awareness Program**
PM-16: Threat Awareness Program The organization implements a threat awareness program that includes a cross-organization information-sharing capability.		**PM-16: Threat Awareness Program** Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.	
Control	**N/A**	**Control**	**Privacy Program Plan**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**PM-18: Privacy Program Plan** **a.** Develop and disseminate an organization-wide privacy program plan that provides an overview of the organization's privacy program, and: **1.** Includes a description of the structure of the privacy program and the resources dedicated to the privacy program; **2.** Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements; **3.** Includes the role of the senior official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities; **4.** Describes management commitment, compliance, and the strategic goals and objectives of the privacy program; **5.** Reflects coordination among organizational entities responsible for the different aspects of privacy; and	

MARS-E		ARC-AMPE	
		6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and **b.** Update the plan at least every one (1) year and address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.	
Control	**N/A**	**Control**	**Privacy Program Leadership Role**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**PM-19: Privacy Program Leadership Role** Appoint a senior official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement applicable privacy requirements and manage privacy risks through the organization-wide privacy program.	
Control	**N/A**	**Control**	**Dissemination of Privacy Program Information**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**PM-20: Dissemination of Privacy Program Information** Maintain a resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that: **a.** Ensures that the public has access to information about organizational privacy activities and can communicate with its senior official for privacy; **b.** Ensures that organizational privacy practices and reports are publicly available; and **c.** Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.	
Control	**N/A**	**Control**	**Privacy Policies on Websites, Applications, and Digital Services**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**PM-20(01): Privacy Policies on Websites, Applications, and Digital Services** Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services that: **a.** Are written in plain language and organized in a way that is easy to understand and navigate; **b.** Provide information needed by the public to make an informed decision about whether and how to interact with the organization; and **c.** Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.	

MARS-E		ARC-AMPE	
Control	**N/A**	**Control**	**Accounting of Disclosures**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**PM-21: Accounting of Disclosures** **a.** Develop and maintain an accurate accounting of disclosures of Personally Identifiable Information (PII), including: **1.** Date, nature, and purpose of each disclosure; and **2.** Name and address, or other contact information of the individual or organization to which the disclosure was made; **b.** Retain the accounting of disclosures for the length of the time the PII is maintained or five (5) years after the disclosure is made, whichever is longer; and **c.** Make the accounting of disclosures available to the individual to whom the PII relates upon request.	
Control	**N/A**	**Control**	**Personally Identifiable Information Quality Management**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**PM-22: Personally Identifiable Information Quality Management** Develop and document organization-wide policies and procedures for: **a.** Reviewing for the accuracy, relevance, timeliness, and completeness of Personally Identifiable Information (PII) across the information life cycle; **b.** Correcting or deleting inaccurate or outdated PII; **c.** Disseminating notice of corrected or deleted PII to individuals or other appropriate entities; and **d.** Appeals of adverse decisions on correction or deletion requests.	
Control	**N/A**	**Control**	**Minimization of PII Used in Testing, Training, and Research**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**PM-25: Minimization of PII Used in Testing, Training, and Research** **a.** Develop, document, and implement policies and procedures that address the use of Personally Identifiable Information (PII) for internal testing, training, and research; **b.** Limit or minimize the amount of PII used for internal testing, training, and research purposes; **c.** Authorize the use of PII when such information is required for internal testing, training, and research; and **d.** Review and update policies and procedures at least every one (1) year.	
Control	**N/A**	**Control**	**Complaint Management**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**PM-26: Complaint Management** Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational security and privacy practices that includes: **a.** Mechanisms that are easy to use and readily accessible by the public; **b.** All information necessary for successfully filing complaints;	

MARS-E		ARC-AMPE	
		c. Tracking mechanisms to ensure all complaints received are reviewed and addressed within thirty (30) working days from timestamp of submission, unless unusual or exceptional circumstances preclude completing action by that time; **d.** Acknowledgement of receipt of complaints, concerns, or questions from individuals within ten (10) working days from timestamp of submission; and **e.** Response to complaints, concerns, or questions from individuals within thirty (30) working days from timestamp of submission, unless unusual or exceptional circumstances preclude completing action by that time.	
Control	**N/A**	**Control**	**Risk Framing**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE		**PM-28: Risk Framing** **a.** Identify and document: **1.** Assumptions affecting risk assessments, risk responses, and risk monitoring; **2.** Constraints affecting risk assessments, risk responses, and risk monitoring; **3.** Priorities and trade-offs considered by the organization for managing risk; and **4.** Organizational risk tolerance; **b.** Distribute the results of risk framing activities to organization-defined personnel who have responsibilities for risk management; and **c.** Review and update risk framing considerations at least every one (1) year or when a significant change occurs.	
Control	**N/A**	**Control**	**Risk Management Program Leadership Roles**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**PM-29: Risk Management Program Leadership Roles** **a.** Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and **b.** Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.	
Control	**N/A**	**Control**	**Continuous Monitoring Strategy**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**PM-31: Continuous Monitoring Strategy** Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include: **a.** Establishing organization-wide metrics to be monitored as defined by the organization; **b.** Establishing organization-defined frequencies for monitoring and organization-defined frequencies for assessment of control effectiveness; **c.** Ongoing monitoring of organizationally defined metrics in accordance with the continuous monitoring strategy; **d.** Correlation and analysis of information generated by control assessments and monitoring; **e.** Response actions to address results of the analysis of control assessment and monitoring information; and	

MARS-E	ARC-AMPE
	f. Reporting the security and privacy status of organizational systems to organization-defined personnel or roles at least every thirty (30) days.

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 (Program Management)_0310/2025