COALFIRE

WHITE PAPER

Migration from MARS-E to ARC-AMPE Contingency Planning (CP) controls

CMS requirements for Administering Entities

JESSICA PAYNE, CONSULTANT
IAN WALTERS, PRINCIPAL

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

Table of contents

Purpose **2**
Background **3**
Affordable Care Act 3
CMS oversight 3
ARC-AMPE 3
Control mapping **4**
Contingency Planning (CP) 4
References **11**
Legal disclaimer **12**

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 Contingency Planning 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 (This Document)	**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.

Contingency Planning (CP)

The set of controls in this family focus on how the Exchange shall establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for Exchange IT systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

MARS-E		ARC-AMPE	
Control	**Contingency Planning Policy and Procedures**	**Control**	**Policy and Procedures**
CP-1: Contingency Planning Policy and Procedures The organization: **a.** Develops, documents, and disseminates to applicable personnel: **1.** A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. **b.** Reviews and updates (as necessary) the current: **1.** Contingency planning policy within every three hundred sixty-five (365) days or as necessitated by significant change. **2.** Contingency planning procedures within every three hundred sixty-five (365) days or as necessitated by significant.		**CP-01: Policy and Procedures** **a.** Develop, document, and disseminate to applicable personnel and roles: **1.** Organization-level contingency planning 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 contingency planning policy and the associated contingency planning controls; **b.** Designate an organization-defined official to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and **c.** Review and update the current contingency planning: **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	**Contingency Plan**	**Control**	**Contingency Plan**
CP-2: Contingency Plan The organization: **a.** Develops a contingency plan for the information system in accordance with NIST SP 800-34 that:		**CP-02: Contingency Plan** **a.** Develop a contingency plan for the system that: **1.** Identifies essential missions and business functions and associated contingency requirements;	

MARS-E	ARC-AMPE
1. Identifies essential organizational missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, and assigns these to specific individuals with contact information; 4. Addresses maintaining essential organizational missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by designated officials within the organization. **b.** Distributes copies of the contingency plan to the Information System Security Officer, Business Owner, Contingency Plan Coordinator, CMS, and other stakeholders identified within the contingency plan; **c.** Coordinates contingency planning activities with incident-handling activities; **d.** Reviews the contingency plan for the information system within every three hundred sixty-five (365) days; **e.** Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; **f.** Communicates contingency plan changes to key contingency personnel and organizational elements identified in this section; and **g.** Protects the contingency plan from unauthorized disclosure and modification. **Implementation Standards** 1. The system must be continuously monitored and assessed to ensure that it is operating as intended and that changes do not have an adverse effect on system performance. 2. The organization must verify that the provisioned implementation that is assessed and/or monitored meets users' needs and is an approved system configuration. 3. The organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to whom the organization will distribute the CP and communicate any changes.	2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, and assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure; 5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; 6. Addresses the sharing of contingency information; and 7. Is reviewed and approved by organization-defined personnel or roles (e.g., Contingency Plan Coordinator [CPC) and business owners); **b.** Distribute copies of the contingency plan to organization-defined key contingency personnel or roles; **c.** Coordinate contingency planning activities with incident handling activities; **d.** Review the contingency plan for the system within at least one (1) year; **e.** Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; **f.** Communicate contingency plan changes to organization-defined key contingency personnel or roles; **g.** Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and **h.** Protect the contingency plan from unauthorized disclosure and modification.
Control | **Coordinate with Related Plans**	**Control** | **Coordinate with Related Plans**
CP-2 (1): Coordinate with Related Plans The organization coordinates contingency plan development with organizational elements responsible for related plans.	**CP-02(01): Coordinate with Related Plans** Coordinate contingency plan development with organizational elements responsible for related plans.
Control | **Capacity Planning**	**Control** | **N/A**
CP-2 (2): Capacity Planning The organization conducts capacity planning to ensure the necessary capacity for information processing,	**Withdrawn Control**: No longer required for the minimum baseline but should still be considered a best practice.

MARS-E		ARC-AMPE	
telecommunications, and environmental support during contingency operations.			
Control	**Resume Essential Missions/Business Functions**	**Control**	**Resume Missions and Business Functions**
CP-2 (3): Resume Essential Missions/Business Functions The organization plans for the resumption of essential missions and business functions within the approved Maximum Tolerable Downtime (MTD), determined by the business owner, for the business functions.		**CP-02(03): Resume Missions and Business Functions** Plan for the resumption of essential mission and business functions within the Business Owner-approved Maximum Tolerable Downtime (MTD) of contingency plan activation.	
Control	**Identify Critical Assets**	**Control**	**Identify Critical Assets**
CP-2 (8): Identify Critical Assets The organization identifies critical information system assets supporting essential missions and business functions.		**CP-02(08): Identify Critical Assets** Identify critical system assets supporting essential mission and business functions.	
Control	**Contingency Training**	**Control**	**Contingency Training**
CP-3: Contingency Training The organization provides contingency training to operational and support personnel (including managers and information system users) consistent with assigned roles and responsibilities: **a.** Within ninety (90) days of assuming a contingency role or responsibility; **b.** When required by information system changes; and **c.** Within every three hundred sixty-five (365) days thereafter.		**CP-03: Contingency Training** **a.** Provide contingency training to system users consistent with assigned roles and responsibilities: **1.** Within thirty (30) days of assuming a contingency role or responsibility; **2.** When required by system changes; and **3.** Every one (1) year thereafter; and **b.** Review and update contingency training content at least every one (1) year and following organization-defined events.	
Control	**Contingency Plan Testing**	**Control**	**Contingency Plan Testing**
CP-4: Contingency Plan Testing The organization: **a.** Tests the contingency plan for the information system within every three hundred sixty-five (365) days using functional exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan; **b.** Reviews the contingency plan test results; and **c.** Initiates corrective actions, if needed **Implementation Standards** **1.** The organization must produce an after-action report to improve existing processes, procedures, and policies. **2.** Contingency plan test results will be made available to the business owner.		**CP-04: Contingency Plan Testing** **a.** Test the contingency plan for the system at least within every one (1) year using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: the most current NIST SP 800-34, NIST SP 800-84, and any organization-defined functional tests or exercises; **b.** Review the contingency plan test results; and **c.** Initiate corrective actions, if needed.	
Control	**Coordinate with Related Plans**	**Control**	**Coordinate with Related Plans**
CP-4 (1): Coordinate with Related Plans The organization coordinates contingency plan testing with organizational elements responsible for related plans.		**CP-04(01): Coordinate with Related Plans** Coordinate contingency plan testing with organizational elements responsible for related plans.	

MARS-E		ARC-AMPE	
Control	**Alternate Storage Site**	**Control**	**Alternate Storage Site**
CP-6: Alternate Storage Site The organization: **a.** Establishes an alternate storage site as well as the necessary agreements to permit the storage and retrieval of information system backup information; and **b.** Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.		**CP-06: Alternate Storage Site** **a.** Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and **b.** Ensure that the alternate storage site provides controls equivalent to that of the primary site.	
Control	**Separation from Primary Site**	**Control**	**Separation from Primary Site**
CP-6 (1): Separation from Primary Site The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.		**CP-06(01): Separation from Primary Site** Identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.	
Control	**Accessibility**	**Control**	**Accessibility**
CP-6 (3): Accessibility The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		**CP-06(03): Accessibility** Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.	
Control	**Alternate Processing Site**	**Control**	**Alternate Processing Site**
CP-7: Alternate Processing Site The organization: **a.** Establishes an alternate processing site as well as the necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions within the time period specified in Implementation Standard 1 when the primary processing capabilities are unavailable; **b.** Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and **c.** Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site. **Implementation Standards** **1.** Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of essential missions and business functions within a resumption time period consistent with the recovery time objectives defined by the business owner in the contingency plan. **2.** In a cloud environment, the service provider defines a resumption time period consistent with the recovery time objectives and business impact analysis. The resumption time period is approved by the business owner.		**CP-07: Alternate Processing Site** **a.** Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of organization-defined system operations for essential missions and business functions within an allowable outage time consistent with recovery time and recovery point objectives (specified by the applicable system contingency plan or Continuity of Operations Plan (COOP) for the business function(s) supported by the system, when the primary processing capabilities are unavailable; **b.** Make available at the alternate processing site the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and **c.** Provide controls at the alternate processing site that are equivalent to those at the primary site.	
Control	**Separation from Primary Site**	**Control**	**Separation from Primary Site**

MARS-E		ARC-AMPE	
CP-7 (1): Separation from Primary Site The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.		**CP-07(01): Separation from Primary Site** Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.	
Control	**Accessibility**	**Control**	**Accessibility**
CP-7 (2): Accessibility The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		**CP-07(2): Accessibility** Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.	
Control	**Priority of Service**	**Control**	**Priority of Service**
CP-7 (3): Priority of Service The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organizational availability requirements (including recovery time objectives).		**CP-07(03): Priority of Service** Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).	
Control	**Telecommunications Services**	**Control**	**Telecommunications Services**
CP-8: Telecommunications Services The organization establishes alternate telecommunications services as well as the necessary agreements to permit the resumption of information system operations for essential organizational missions and business functions within the resumption time period specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. **Implementation Standards** **1.** Ensure alternate telecommunications Service Level Agreements (SLA) are in place to permit resumption of system Recovery Time Objectives (RTO) and business function Maximum Tolerable Downtimes (MTD). **2.** The system owner defines a resumption time consistent with the RTOs and business impact analysis. The time is approved and accepted by the business owner.		**CP-08: Telecommunications Services** Establish alternate telecommunications services, including necessary agreements to permit the resumption of organization-defined system operations for essential missions and business functions within the resumption time specified by System Recovery Time Objectives (RTO) and business functions Maximum Tolerable Downtime (MTD) as specified in the applicable system contingency plan, Information System Contingency Plan (ISCP), Business Impact Analysis (BIA), or Continuity of Operations Plan (COOP) when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	
Control	**Priority of Service Provisions**	**Control**	**Priority of Service Provisions**
CP-8 (1): Priority of Service Provisions The organization: **a.** Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and **b.** Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.		**CP-08(01): Priority of Service Provisions** **a.** Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives [RTO]); and **b.** Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.	

<table>
<tr><th colspan="2">MARS-E</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td>Control</td><td>Single Points of Failure</td><td>Control</td><td>Single Points of Failure</td></tr>
<tr><td colspan="2">CP-8 (2): Single Points of Failure
The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.</td><td colspan="2">CP-08(02): Single Points of Failure
Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.</td></tr>
<tr><td>Control</td><td>Information System Backup</td><td>Control</td><td>System Backup</td></tr>
<tr><td colspan="2">CP-9: Information System Backup
The organization:
a. Conducts backups of user-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1;
b. Conducts backups of system-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1;
c. Conducts backups of information system documentation, including security-related documentation, other forms of data, and paper records, within the frequency defined in the applicable security plan, consistent with recovery time and recovery point objectives; and
d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Implementation Standards
1. Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. Backups to include user-level and system-level information (including system state information). Maintain three (3) generations of backups, at least one (1) of which is available online (a full backup as well as all related incremental or differential backups). Off-site and on-site backups must be logged with name, date, time, and action.
2. Backups must comply with CMS requirements for protecting data at rest. (See SC-28)
3. Ensure that a current, retrievable copy of PII is available before movement of servers.
4. Use the encryption methodology specified in SC-13 to encrypt PII in backups at the storage location.
5. Establish procedures that create a retrievable, exact copy of the PHI before any movement of information system equipment.
6. For cloud environments, the system owner shall determine what elements of the cloud environment require the Information System Backup control.
7. For cloud environments, the system owner determines how Information System Backup will be verified and the appropriate periodicity of the check.</td><td colspan="2">CP-09: System Backup
a. Conduct backups of user-level information contained in organization-defined system components consistent with:
1. Daily Incremental backups and weekly full backups;
2. Maintaining three (3) generations of backups, at least one (1) of which is available online (a full backup and all related incremental backups);
b. Conduct backups of system-level information contained in the system consistent with:
1. Daily incremental backups and weekly full backups;
2. Maintaining three (3) generations of backups, at least one (1) of which is available online (a full backup and all related incremental backups);
c. Conduct backups of system documentation, including security- and privacy-related documentation consistent with:
1. Daily incremental backups and weekly full backups;
2. Maintaining three (3) generations of backups, at least one (1) of which is available online (a full backup and all related incremental backups); and
d. Protect the confidentiality, integrity, and availability of backup information.</td></tr>
<tr><td>Control</td><td>Testing for Reliability/Integrity</td><td>Control</td><td>Testing for Reliability and Integrity</td></tr>
<tr><td colspan="2">CP-9(1): Testing for Reliability/Integrity
The organization tests backup information following each backup, at least every six months, to verify media reliability and information integrity.</td><td colspan="2">CP-09(01): Testing for Reliability and Integrity
Test backup information at least every six (6) months to verify media reliability and information integrity.</td></tr>
</table>

MARS-E		ARC-AMPE	
Control	**Separate Storage for Critical Information**	**Control**	**N/A**
CP-9 (3): Separate Storage for Critical Information The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.		**Withdrawn Control**: No longer required for the minimum baseline but should still be considered a best practice.	
Control	**N/A**	**Control**	**Cryptographic Protection**
New NIST SP 800-53 Rev.5 Control and applicable to ARC-AMPE.		**CP-09(08): Cryptographic Protection** Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all backup files.	
Control	**Information System Recovery and Reconstitution**	**Control**	**System Recovery and Reconstitution**
CP-10: Information System Recovery and Reconstitution The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner. **Implementation Standards** **1.** Secure information system recovery and reconstitution includes, but is not limited to: **a.** Reset all system parameters (either default or organization-established); **b.** Reinstall patches; **c.** Reestablish configuration settings; **d.** Reinstall application and system software; and **e.** Fully test the system.		**CP-10: System Recovery and Reconstitution** Provide for the recovery and reconstitution of the system to a known state within organization-defined time period specified in the contingency plan, or COOP after a disruption, compromise, or failure.	
Control	**Transaction Recovery**	**Control**	**Transaction Recovery**
CP-10 (2): Transaction Recovery The information system implements transaction recovery for transaction-based systems.		**CP-10(02): Transaction Recovery** Implement transaction recovery for systems that are transaction based.	

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 (Contingency Planning (CP))_03102025