COALFIRE

WHITE PAPER

Migration from EDE to ARC-AMPE System and Services Acquisition (SA) controls

CMS requirements for Direct Enrollment Entities

JESSICA PAYNE, CONSULTANT
IAN WALTERS, PRINCIPAL

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

Table of contents

Purpose

This white paper provides a guide for Direct Enrollment Entities (DEEs) to upgrade their Enhanced Direct Enrollment (EDE) System Security and Privacy Plans (SSPPs) to the Acceptable Risk Controls for ACA, Medicaid, and Provider Entities (ARC-AMPE).

Due to the substantial number of controls, and to facilitate ease of use, this white paper is one of a series of 20 which divides the ARC-AMPE by control family. This white paper addresses the System and Services Acquisition controls.

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

Background

Affordable Care Act

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

Enhanced Direct Enrollment

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

CMS oversight

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

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

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

ARC-AMPE

CMS published the ARC-AMPE for Direct Enrollment Entities (DEEs) Version 1.0 dated July 7th, 2025. This framework replaces the EDE security and privacy guidelines:

- ARC-AMPE Volume 1 contains high-level guidance, and Volume 2 has the minimum-level security and privacy controls.
- ARC-AMPE Volume 2 is the new format for the SSPP for DEEs.
- The compliance date for DEEs is June 2026.

The minimum control baseline for ARC-AMPE DEE compliance consists of 308 controls which have been derived from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, “Security and Privacy Controls for Information Systems and Organizations.”

The number of controls required for the mandatory baseline represents a significant increase from the EDE baseline (295 controls), and DEEs should be prepared for an increased level of effort for developing the SSPP and submitting more artifacts during audits.

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

Control mapping

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

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

System and Services Acquisition (SA)

The set of controls in this family focus on how the Exchange shall: (1) allocate sufficient resources to adequately protect Exchange IT systems; (2) employ system development life cycle processes that incorporate IS considerations; (3) employ software usage and installation restrictions; and (4) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

EDE		ARC-AMPE	
Control	**System and Services Acquisition Policy and Procedures**	**Control**	**Policy and Procedures**
SA-1: System and Services Acquisition Policy and Procedures The organization: **a.** Develops, documents, and disseminates to applicable personnel: **1.** A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **2.** Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and **b.** Reviews and updates (as necessary) the current: **1.** System and services acquisition policy within every three (3) years; and **2.** System and services acquisition procedures within every three (3) years.		**SA-01: Policy and Procedures** a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition 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 system and services acquisition policy and the associated system and services acquisition controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and c. Review and update the current system and services acquisition: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	
Control	**Allocation of Resources**	**Control**	**Allocation of Resources**
SA-2: Allocation of Resources The organization: **a.** Determines information security requirements for the information system or information system service in mission/business process planning; **b.** Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; 1. As part of the capital planning and investment control process, the organization must determine, document, and allocate resources required to protect the privacy and confidentiality of personally identifiable information (PII) in the information system.		**SA-02: Allocation of Resources** **a.** Determine the high-level information security and privacy requirements for the system or system service in mission and business planning; **b.** Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and **c.** Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.	

EDE	ARC-AMPE
c. Includes information security requirements in mission/business case planning, and **d.** Establishes a discrete line item in programming and budgeting documentation for the implementation and management of information systems security.	
Control **System Development Life Cycle**	**Control** **System Development Life Cycle**
SA-3: System Development Life Cycle The organization: **a.** Manages the information system using the formally defined and documented system development life cycle (SDLC) process that incorporates information security considerations; **b.** Defines and documents information security roles and responsibilities throughout the system development life cycle; **c.** Identifies individuals having information system security roles and responsibilities; and **d.** Integrates the organizational information security risk management process into system development life cycle activities.	**SA-03: System Development Life Cycle** **a.** Acquire, develop, and manage the system using a formally defined and documented system development life cycle (SDLC) process that incorporates information security and privacy considerations; **b.** Define and document information security and privacy roles and responsibilities throughout the SLDC; **c.** Identify individuals having information security and privacy roles and responsibilities; and **d.** Integrate the organizational information security and privacy risk management process into SLDC activities.
Control **Acquisition Process**	**Control** **Acquisition Process**
SA-4: Acquisition Process The organization: a. Includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: 1. Security functional requirements; 2. Security strength requirements; 3. Security assurance requirements; 4. Security-related documentation requirements; 5. Requirements for protecting security-related documentation; 6. Description of the information system development, implementation and production environments or their equivalents; 7. Acceptance criteria b. When acquiring information systems, components, or services used to store, process, or transmit personally identifiable information (PII), ensure the following, in consultation with the privacy office, are included in the acquisition contract: 1. List of security and privacy controls necessary to ensure protection of PII and, if appropriate, enforce applicable privacy requirements. 2. Privacy requirements set forth in Appendix J of NIST SP 800-53, Rev. 4, including privacy training and awareness, and rules of behavior.	**SA-04: Acquisition Process** Include the following requirements, descriptions, and criteria, explicitly or by reference, using organization-defined standardized contract language in the acquisition contract for the system, system component, or system service: **a.** Security and privacy functional requirements; **b.** Strength of mechanism requirements; **c.** Security and privacy assurance requirements; **d.** Controls needed to satisfy the security and privacy requirements. **e.** Security and privacy documentation requirements; **f.** Requirements for protecting security and privacy documentation; **g.** Description of the system development environment and environment in which the system is intended to operate; **h.** Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and **i.** Acceptance criteria.

EDE		ARC-AMPE	
3. Privacy functional requirements, i.e., functional requirements specific to privacy. 4. Privacy Act of 1974 and any other organization-specific privacy clauses.			
Control	**Functional Properties of Security Controls**	**Control**	**Functional Properties of Controls**
SA-4 (1): Functional Properties of Security Controls The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.		**SA-04(01): Functional Properties of Controls** Require the developer of the system, system component, or system service to provide a description of the functional properties of the security and privacy controls to be implemented.	
Control	**Design/Implementation Information for Security Controls**	**Control**	**Design and Implementation Information for Security Controls**
SA-4 (2): Design/Implementation Information for Security Controls The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed, which shall include: **a.** Security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces, **b.** Source code and hardware schematics; and **c.** High-level design documentation at sufficient detail to prove the security control implementation.		**SA-04(02): Design and Implementation Information for Security Controls** Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes security-relevant external system interfaces, high-level design documentation, and source code or hardware schematics at organization-defined level of detail to prove the control implementation.	
Control	**Continuous Monitoring Plan**	**Control**	**N/A**
SA-4 (8): Continuous Monitoring Plan The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that is commensurate with Continuous Diagnostics and Mitigation, ongoing authorization, requirements.		**Withdrawn control**: No longer required for the minimum baseline but should still be considered best practice.	
Control	**Functions/Ports/Protocols/Services in Use**	**Control**	**Functions, Ports, Protocols, and Services in Use**
SA-4 (9): Functions/Ports/Protocols/Services in Use The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle the functions, ports, protocols, and services intended for organizational use.		**SA-04(09): Functions, Ports, Protocols, and Services in Use** Require the developer of the information system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.	
Control	**Information System Documentation**	**Control**	**System Documentation**
SA-5: Information System Documentation The organization: **a.** Obtains administrator documentation for the information system, system component, or information system service that describes:		**SA-05: System Documentation** **a.** Obtain or develop administrator documentation for the system, system component, or system service that describes: **1.** Secure configuration, installation, and operation of the system, component, or service;	

EDE	ARC-AMPE
1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; **b.** Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; **c.** Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent. **d.** Protects documentation as required, in accordance with the risk management strategy; and **e.** Distributes documentation to defined personnel or roles (defined in the applicable system security and privacy plan [SSPP]).	2. Effective use and maintenance of security and privacy functions and mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative or privileged functions; **b.** Obtain or develop user documentation for the system, system component, or system service that describes: 1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and 3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals; **c.** Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take organization-defined actions in response; and **d.** Distribute documentation to organization-defined personnel or roles.
Control **Security Engineering**	**Control** **Security and Privacy Engineering Principles**
SA-8: Security Engineering The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	**SA-08: Security and Privacy Engineering Principles** Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: organization-defined systems security and privacy engineering principles.
Control **External Information System Services**	**Control** **External System Services**
SA-9: External Information System Services The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities regarding external information system services in a SLA or similar agreement; and c. Employs defined processes, methods, and techniques (defined in the applicable System Security and Privacy Plan [SSPP]) to monitor security control compliance by external service providers on an ongoing basis. **Implementation Standards**	**SA-09: External System Services** **a.** Require that providers of external system services comply with organizational security and privacy requirements and employ the organization-defined controls; **b.** Define and document organizational oversight and user roles and responsibilities regarding external system services; and **c.** Employ defined processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: organization-defined processes, methods, and techniques.

<table>
<tr><th colspan="2">EDE</th><th colspan="2">ARC-AMPE</th></tr>
<tr><td colspan="2">1. The service contract or agreement must include language requiring the provider to be subject to U.S. Federal laws and regulations protecting PII.
2. The service contract or agreement must include language requiring adherence to the security and privacy policies and standards set by the organization consistent with 45 CFR 155.260(b), define security and privacy roles and responsibilities.
3. The organization must notify CMS at least 45 days prior to transmitting data into an external information service environment.</td><td colspan="2"></td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Processing, Storage, and Service Location</td></tr>
<tr><td colspan="2">Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.</td><td colspan="2">SA-09(05): Processing, Storage, and Service Location
Restrict the location of information processing, information or data, and system services to organization-defined locations based on organization-defined requirements or conditions.</td></tr>
<tr><td>Control</td><td>N/A</td><td>Control</td><td>Processing and Storage Location - U.S. Jurisdiction</td></tr>
<tr><td colspan="2">New NIST SP 800-53 Rev. 5 Control and applicable to ARC-AMPE</td><td colspan="2">SA-09(08): Processing and Storage Location - U.S. Jurisdiction
Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.</td></tr>
<tr><td>Control</td><td>Developer Configuration Management</td><td>Control</td><td>Developer Configuration Management</td></tr>
<tr><td colspan="2">SA-10: Developer Configuration Management
The organization requires the developer of the information system, system component, or information system service to:
a. Perform configuration management during system, component, or service development, implementation, and operation;
b. Document, manage, and control the integrity of changes to organization-defined configuration items under configuration management;
c. Implement only organization-approved changes to the system, component, or service;
d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
e. Track security flaws and flaw resolution within the system, component, or service and report findings to defined organization-defined personnel or roles (defined in the applicable system security and privacy plan [SSPP]).</td><td colspan="2">SA-10: Developer Configuration Management
Require the developer of the system, system component, or system service to:
a. Perform configuration management during system, component, or service design, development, implementation, operation, and disposal;
b. Document, manage, and control the integrity of changes to organization-defined configuration items under configuration management.
c. Implement only organization-approved changes to the system, component, or service;
d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and
e. Track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel or roles.</td></tr>
</table>

EDE		ARC-AMPE	
Control	**Developer Security Testing and Evaluation**	**Control**	**Developer Testing and Evaluation**
SA-11: Developer Security Testing and Evaluation The organization requires the developer of the information system, system component, or information system service to: **a.** Create and implement a security assessment plan in accordance with, but not limited to, current organization procedures; **b.** Perform unit; integration; system; regression testing/evaluation in accordance with organizational defined system development life cycle; **c.** Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; **d.** Implement a verifiable flaw remediation process; and **e.** Correct flaws identified during security testing/evaluation. **f.** Conduct tests that: **1.** Minimize to the use of PII to the maximum extent practicable; **2.** Use actual PII only if a formal memorandum of agreement (MOA), memorandum of understanding (MOU), or data exchange agreement has been established between the data owner of the PII and the entity developing/testing the information system including how loss, theft, or compromise (i.e., breach) of PII is to be handled; **3.** Use de-identified or anonymized PII to the maximum extent practicable; and **4.** Coordinate use of PII with the organization's privacy office before conducting any testing. **Implementation Standards** **1.** If the security control assessment results are used in support of the security authorization process for the information system, ensure that no security relevant modifications of the information systems have been made after the assessment and after selective verification of the results. **2.** Use hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment. **3.** All systems supporting development and pre-production testing are connected to an isolated network separated from production systems. Network traffic into and out of the development and pre-production testing environment is only permitted to facilitate system testing and is restricted by source and destination access control lists as well as ports and protocols.		**SA-11: Developer Testing and Evaluation** Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to: **a.** Develop and implement a plan for ongoing security and privacy control assessments; **b.** Perform unit, integration, system, and regression testing/evaluation in accordance with the organizational-defined frequency at organization-defined depth and coverage; **c.** Produce evidence of the execution of the assessment plan and the results of the testing and evaluation; **d.** Implement a verifiable flaw remediation process; and **e.** Correct flaws identified during testing and evaluation.	
Control	**Development Process, Standards, and Tools**	**Control**	**Development Process, Standards, and Tools**
SA-15: Development Process, Standards, and Tools The organization: a. Requires the developer of the information system, system component, or information system service to follow a documented development process that: 1. Explicitly addresses security requirements;		**SA-15: Development Process, Standards, and Tools** **a.** Require the developer of the system, system component, or system service to follow a documented development process that: **1.** Explicitly addresses security and privacy requirements;	

EDE		ARC-AMPE	
2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Reviews the development process, standards, tools, and tool options/configurations at least every three (3) years to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy all applicable System Acquisition (SA) and Configuration Management (CM) security controls		**2.** Identifies the standards and tools used in the development process; **3.** Documents the specific tool options and tool configurations used in the development process; and **4.** Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and **b.** Review the development process, standards, tools, tool options, and tool configurations at least every one (1) year or as needed to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy organization-defined security and privacy requirements.	
Control	**N/A**	**Control**	**Minimize Personally Identifiable Information**
Existing NIST SP 800-53 Rev.4 control and new to ARC-AMPE.		**SA-15(12): Minimize Personally Identifiable Information** Require the developer of the system or system component to minimize the use of Personally Identifiable Information (PII) in development and test environments.	
Control	**Developer Security Architecture and Design**	**Control**	**Developer Security Architecture and Design**
SA-17: Developer Security Architecture and Design The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: a. Is consistent with and supportive of the organization's security architecture (see PL-8), which is established within and is an integrated part of the organization's enterprise architecture; and b. Accurately and completely describes the required security functionality and the allocation of security controls among physical and logical components; and c. Accurately and completely describes the privacy requirements and the allocation of security and privacy controls among physical and logical components d. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.		**SA-17: Developer Security Architecture and Design** Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that: **a.** Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture; **b.** Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and **c.** Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.	
Control	**Unsupported System Components**	**Control**	**Unsupported System Components**
SA-22: Unsupported System Components The organization: **a.** Replaces information system components as soon as possible after discovery that support for the components is no longer available from the developer, vendor, or manufacturer; and		**SA-22: Unsupported System Components** **a.** Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or **b.** Provide the following option(s) for alternative sources for continued support for unsupported components: provide justification and document the approval for the continued	

EDE	ARC-AMPE
b. Where immediate replacement is not possible, provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.	use of unsupported system components required to satisfy mission/business needs.

References

NIST SP 800-53 Revision 5.1.1

NIST SP 800-53 Revision 4

CMS Standards

Legal disclaimer

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.

WP_ACA CMS Controls Migration (System and Services Acquisition (SA)) 07142025