JANUS ASSOCIATES

EXECUTIVE SUMMARY

ARC-AMPE Compliance Roadmap:

A Practical Guide for ACA, Medicaid, and Partner Entities

Presented By JANUS Associates
September 2026

REMOVE RISK BY ADDING JANUS
JANUSASSOCIATES.COM

ARC-AMPE is the new CMS security and privacy framework that replaces MARS-E v2.2 and establishes a modern, NIST-aligned control baseline that ACA, Medicaid, and partner entities must implement by March 4, 2026, to maintain CMS connectivity and meet oversight expectations.

ARC-AMPE Volume II introduces an Excel-based System Security and Privacy Plan (SSPP) covering 402 baseline security and privacy controls derived from NIST SP 800-53 Rev. 5, significantly expanding documentation, evidence, and continuous monitoring obligations relative to prior MARS-E requirements.

I. Executive Overview: Why ARC-AMPE, Why Now

The Centers for Medicare & Medicaid Services (CMS) released the Acceptable Risk Controls for ACA, Medicaid, and Partner Entities (ARC-AMPE) as a comprehensive cybersecurity and privacy framework that supersedes MARS-E v2.2 for ACA administering entities (AEs), Medicaid agencies, exchanges, and partner entities handling ACA-related data and functions. ARC-AMPE Version 1.0 was published on March 4, 2025, with ACA Administering Entities required to achieve compliance by March 4, 2026, and Direct Enrollment Entities required by June 2026, making the one-year window a critical transition period for planning, remediation, and validation activities.

ARC-AMPE modernizes CMS expectations by aligning with NIST SP 800-53 Rev. 5 controls, integrating privacy as a core component, and emphasizing enterprise risk management and continuous monitoring over one-time compliance exercises. The framework responds to evolving cyber threats, increased regulatory and public focus on privacy, and growing dependence on cloud and third-party services, requiring stronger, more evidence-driven safeguards for personally identifiable information (PII) and protected health information (PHI) across the ACA ecosystem.

From a risk perspective, delayed or incomplete adoption of ARC-AMPE can lead to findings in CMS audits, challenges renewing Authority to Connect (ATC) or Authority to Operate (ATO), potential restrictions or disconnection from CMS-supported environments, and heightened exposure to breaches and enforcement actions by CMS and the HHS Office for Civil Rights (OCR). CMS oversight mechanisms include mandatory controls, breach reporting and corrective actions, annual ATC/ATO renewal, and rigorous evidence-based assessments, meaning that entities must not only implement controls but also demonstrate their effectiveness with defensible documentation.

JANUS Associates can serve as a strategic cybersecurity and risk management partner by helping organizations interpret ARC-AMPE requirements, map existing MARS-E and HIPAA controls to the new baseline, identify and prioritize gaps, implement technical and procedural safeguards, and build sustainable continuous monitoring and evidence-management practices that support long-term compliance and resilience. JANUS' experience with healthcare cybersecurity, NIST-based control frameworks, and CMS-driven environments enables organizations to reduce transition risk, accelerate readiness, and align security investments with business and program objectives in ACA and Medicaid operations.

II. From MARS-E to ARC-AMPE: What Changed

MARS-E v2.2 provided the prior CMS baseline for security and privacy controls in health insurance exchanges and related entities, defining minimum safeguards to protect ACA data and support compliance with federal requirements. ARC-AMPE formally replaces MARS-E v2.2 upon publication, meaning that organizations previously subject to MARS-E must now transition their security and privacy programs, documentation, and attestations to align with ARC-AMPE's expanded and updated control set.

Structurally, ARC-AMPE shifts from a primarily Word-document-based framework to an Excel-based control spreadsheet in Volume II that organizes more than 400 security and privacy controls across 20 NIST-aligned control families, including new families for privacy and supply chain risk. The minimum baseline for Administering Entities comprises 402 controls derived from NIST SP 800-53 Rev. 5, representing a significant expansion over the previous MARS-E baseline and requiring more robust implementation and documentation.

Conceptually, ARC-AMPE increases emphasis on enterprise risk management, privacy governance, and continuous monitoring, reflecting a shift from static, point-in-time compliance toward ongoing risk-informed security operations. The framework introduces the Personally Identifiable Information Processing and Transparency (PT) control family to embed privacy expectations (such as privacy program planning, consent, and data minimization) and strengthens requirements around vendor and supply chain risk management via SR controls.

For entities with significant MARS-E investments, this transition means mapping existing controls to ARC-AMPE requirements, evaluating where implementations meet, exceed, or fall short of the new baseline, and re-validating control effectiveness under updated criteria and evidence expectations. Previous artifacts, such as MARS-E-aligned SSPs, policies, and procedures, may remain useful inputs but must be revised and extended to conform to the ARC-AMPE Volume II SSPP structure and to cover the broadened set of security and privacy controls.

III. Inside the ARC-AMPE Framework

ARC-AMPE is published in multiple components, with two primary volumes guiding scope, governance, and detailed control implementation. Volume I provides high-level guidance on program intent, applicability across ACA Administering Entities and partner entities, governance expectations, and overall security and privacy principles, framing how organizations should interpret and apply the framework across systems and contracts. Volume II provides the Excel-based System Security and Privacy Plan (SSPP) template and the mandatory baseline controls for ACA Administering Entities, closely tied to NIST SP 800-53 Rev. 5 and designed to standardize documentation for CMS review.

The Volume II spreadsheet includes an index and multiple tabs that define the mandatory baseline, tailoring and scoping decisions, control family listings, and data entry fields for describing control implementation details. Each control maps to a NIST SP 800-53 Rev. 5 identifier, is assigned a control priority, and includes data fields where entities must document the implementation approach, responsible roles, implementation status, review frequency, and references to supporting evidence or artifacts. The tailoring functionality allows entities to adjust implementation details to reflect system characteristics and risk while preserving or enhancing the baseline requirements; tailoring cannot weaken the CMS-defined security posture.

ARC-AMPE operates within a broader CMS and HHS policy ecosystem that includes the CMS Acceptable Risk Safeguards (ARS), Information Security and Privacy Policy (IS2P2), and HIPAA Security, Privacy, and Breach Notification Rules. By integrating NIST SP 800-53 Rev. 5 controls and privacy concepts, ARC-AMPE helps entities align ACA-specific expectations with organization-wide security and privacy programs, supporting consistent protection of PHI and PII, facilitating HIPAA compliance, and streamlining responses to CMS oversight and audits.

IV. NIST SP 800-53 Rev. 5 and Integrated Risk Management

NIST Special Publication 800-53 Revision 5 provides a catalog of security and privacy controls for information systems and organizations, covering traditional families such as Access Control (AC), Audit and Accountability (AU), Configuration Management (CM), Incident Response (IR), and System and Communications Protection (SC), among others. ARC-AMPE's mandatory baseline of 402 controls is drawn from these NIST SP 800-53 Rev. 5 families, and incorporates additional privacy and supply chain controls, ensuring that ACA and Medicaid entities align their security posture with current federal best practices.

The NIST Risk Management Framework (RMF), detailed in NIST SP 800-37, provides the lifecycle for integrating these controls into enterprise and system-level risk management, including categorizing systems, selecting controls, implementing controls, assessing control effectiveness, authorizing systems, and performing continuous monitoring. ARC-AMPE applies these concepts by requiring entities to manage cybersecurity and privacy not only at the system level but also through an integrated enterprise risk management (ERM) approach, including updating risk registers, incorporating emerging threats, and involving senior leadership in risk decisions.

This alignment supports a shift from checklist-driven compliance toward risk-informed decision-making, enabling organizations to prioritize high-impact controls, allocate resources where they reduce risk most, and demonstrate that protective measures are commensurate with the sensitivity of PII and PHI and with mission criticality. Well-implemented ARC-AMPE programs can thus strengthen both regulatory posture and operational resilience, reducing the likelihood and impact of cyber incidents while satisfying CMS oversight expectations.

V. Governance, Roles, and Responsibilities

ARC-AMPE expects that ACA Administering Entities, Medicaid agencies, and partner entities establish clear governance structures with defined roles and accountability for security and privacy. Effective governance typically includes executive sponsors who provide strategic direction and resources; Chief Information Security Officers (CISOs) or comparable security leaders; privacy officers responsible for data protection and compliance with privacy regulations; and business owners accountable for ACA and Medicaid systems and data.

Within the SSPP, entities are expected to identify the responsible organization and key designated contacts, assign security and privacy responsibility for each control or control family, and ensure that roles such as system owners, information system security officers, and privacy coordinators are documented and traceable. ARC-AMPE's control structure, particularly in program management (PM), planning (PL), and privacy (PT) families, reinforces expectations for governance artifacts such as security plans, privacy program plans, policy approvals, and leadership-level risk acceptance records.

Cross-functional governance is essential to effective ARC-AMPE implementation and involves IT, security, privacy, legal, compliance, procurement, and program leadership in structured committees or working groups that oversee control implementation, monitor risks, coordinate remediation, and manage communications with CMS. For multi-vendor environments, governance should extend to third-party management, including contract clauses that align vendors with ARC-AMPE controls, regular performance and security reviews, and coordinated incident response processes.

VI. Building Your ARC-AMPE Compliance Roadmap

Given that the fixed compliance deadline of March 4, 2026, has already passed for ACA Administering Entities, organizations should adopt a phased roadmap that sequences discovery, remediation, implementation, and validation activities over the remaining months. A practical structure should follow four phases: discovery and gap analysis, remediation planning, implementation and validation, and finalization and submission.

Phase 1: Discovery and Gap Analysis

In this phase, entities should inventory ACA/Medicaid systems, interfaces, and data flows in scope for ARC-AMPE, confirm ARC-AMPE applicability, and map existing MARS-E and HIPAA controls to the ARC-AMPE baseline to identify overlaps and deficiencies. Organizations should also review the Volume II SSPP template, evaluate the completeness and quality of existing SSP or SSPP documentation, and perform an initial self-assessment or independent readiness review against the 402-control baseline.

Phase 2: Remediation Planning

Based on the gap analysis, entities should prioritize control deficiencies according to risk and CMS expectations, define remediation projects (e.g., MFA deployment, logging enhancements, vendor risk assessments), secure necessary resources, and update policies and procedures to reflect ARC-AMPE terminology and requirements. Create or update a detailed Plan of Action and Milestones (POA&M) to track remediation tasks, owners, target dates, and dependencies in alignment with NIST RMF practices.

Phase 3: Implementation and Validation

During this phase, organizations execute prioritized technical changes and process improvements, update SSPP entries to reflect implemented controls, and collect supporting evidence such as configuration baselines, training records, logs, and test results. Internal reviews, such as control testing, tabletop exercises, or independent assessments, should validate that controls operate as described and that documentation is accurate, traceable, and consistent with ARC-AMPE Volume II expectations.

Phase 4: Finalization and Submission

In the final phase, entities should finalize the SSPP spreadsheet, ensuring that all applicable mandatory baseline controls are addressed, tailoring decisions are justified, and references to evidence repositories are complete. Organizations should confirm that their documentation and artifacts are ready for CMS review, that governance bodies have endorsed the SSPP and associated risk decisions, and that ongoing continuous monitoring plans are in place.

Throughout each phase, JANUS can assist by conducting readiness and gap assessments, facilitating MARS-E-to-ARC-AMPE mapping, advising on remediation priorities and control design, developing or refining SSPP content, and performing pre-assessment validations that simulate CMS scrutiny. This partnership approach enables ACA and Medicaid entities to compress timelines without sacrificing control quality or audit readiness, aligning technical workstreams with governance, risk, and compliance objectives.

VII. Modern SSPP and Documentation Expectations

ARC-AMPE's Volume II SSPP template introduces more rigorous and structured documentation expectations than prior MARS-E-based Word templates, requiring a higher degree of specificity and evidence linkage. For each baseline control, entities must document the implementation approach, responsible roles or teams, control status, review frequency, and references to supporting artifacts such as policies, procedures, configurations, and logs, all within the Excel-based format.

Documentation must address technical and procedural dimensions, including configuration baselines for key platforms, user behavior rules, security and privacy training records, logging and monitoring practices, and privacy-specific processes such as consent management, data minimization, and breach notification. ARC-AMPE's privacy and supply chain control families add specific expectations around PII processing transparency, privacy program planning, and vendor oversight, all of which must be reflected in the SSPP narrative and evidence references.

High-quality SSPP documentation improves the efficiency of CMS assessments by reducing follow-up questions, clarifying control scope and ownership, and enabling auditors to validate compliance through well-organized evidence. Investing effort up front in accurate, complete, and consistent SSPP entries also supports ongoing audit readiness by establishing a reusable documentation foundation for annual ATC/ATO renewal, internal audits, and third-party assessments.

VIII. Continuous Monitoring, Audit Readiness, and Evidence Management

ARC-AMPE places strong emphasis on continuous monitoring to ensure that implemented controls remain effective over time and adapt to changing threats and system changes. Continuous monitoring activities generally include regular vulnerability scanning and remediation, log review and correlation, configuration compliance checks, incident response exercises, periodic user access reviews, and updates to risk assessments and POA&Ms.

To support audit readiness, organizations should design systematic evidence-collection processes and repositories that capture and retain proof of control performance, such as security assessment reports, scan results, access review records, training completion logs, incident tickets, and change management records. Evidence management practices should define retention periods, ownership, access controls, and indexing or tagging to align artifacts with specific ARC-AMPE controls and SSPP references, enabling efficient responses to CMS or third-party audit requests.

JANUS services such as vulnerability management, penetration testing, configuration reviews, and continuous risk assessments can be integrated into an organization's continuous monitoring strategy to provide independent validation and expert guidance. By aligning testing cycles, reporting formats, and remediation tracking with ARC-AMPE and NIST RMF expectations, JANUS can help entities demonstrate sustained compliance, quickly surface emerging risks, and maintain a strong security posture between formal audits.

IX. How JANUS Supports ARC-AMPE Compliance

JANUS, MARS-E, and now ARC-AMPE specialists can map its cybersecurity consulting and risk management services directly to the ARC-AMPE lifecycle, from initial readiness through ongoing continuous monitoring. Readiness assessments and control gap analyses can be structured against the ARC-AMPE 402-control baseline and NIST SP 800-53 Rev. 5 families, providing a prioritized view of technical and procedural gaps, including privacy and supply chain requirements.

Control mapping and SSPP development services can translate existing MARS-E-aligned controls, HIPAA safeguards, and enterprise security practices into ARC-AMPE-conformant documentation, including detailed implementation descriptions, role assignments, and evidence references consistent with Volume II spreadsheet expectations. Technical remediation guidance, combined with penetration testing, vulnerability management, and configuration reviews, supports closing high-risk findings and ensures implemented controls are both effective and defensible under CMS scrutiny.

Illustratively, a Medicaid agency with fragmented MARS-E artifacts and limited centralized documentation could work with JANUS to conduct an ARC-AMPE readiness assessment, rationalize overlapping policies, map system-level controls to the new baseline, and stand up a consolidated SSPP and evidence repository in a matter of months. Similarly, a partner entity supporting ACA eligibility and enrollment operations could leverage JANUS to integrate privacy and supply chain controls into its vendor management and DevSecOps pipelines, closing gaps that might otherwise delay ATC/ATO renewal or expose the organization to audit findings.

X. Checklists, Templates, and Next Steps

The following checklists and worksheet examples provide practical starting points; adapt them to each organization's environment and use them alongside official CMS ARC-AMPE templates and guidance.

ARC-AMPE readiness checklist

- ☐ Governance structure defined (executive sponsor, security lead, privacy officer, business owners identified for ACA/Medicaid systems).
- ☐ ARC-AMPE applicability confirmed for all ACA, Medicaid, and partner systems (including cloud and third-party services).
- ☐ System inventory and data flows documented for in-scope systems; integrations with CMS environments.
- ☐ Official ARC-AMPE Volume II SSPP Excel template obtained and adopted as the primary documentation vehicle.
- ☐ Existing MARS-E, HIPAA, and enterprise controls mapped to ARC-AMPE baseline controls, with initial gap analysis completed.
- ☐ Centralized evidence repository identified or established (e.g., GRC tool or secured document management system) and aligned with control structure.

Milestones checklist

1. **Step 1:** ARC-AMPE gap assessment completed, with documented control gaps and risk ratings.
2. **Step 2:** Remediation and POA&M approved by governance body, with owners and timelines defined.
3. **Step 3:** High-priority technical remediations and key policy updates implemented; SSPP content substantially complete.
4. **Step 4:** SSPP finalized and validated; evidence repository populated for all mandatory baseline controls; continuous monitoring plan documented and approved.

Example SSPP worksheet fields (aligned with ARC-AMPE Volume II)

For each ARC-AMPE control in the Volume II spreadsheet, organizations should be prepared to complete fields such as:

- ☐ Control identifier and name (e.g., AC-2 Account Management, PT-2 Privacy Impact Assessment).
- ☐ Applicability and tailoring rationale (e.g., applicable to all production environments; tailored to specific data types while meeting CMS minimums).
- ☐ Implementation description (how the control is implemented, including technologies, processes, and organizational practices).
- ☐ Responsible role or team (e.g., Information Security, Privacy Office, System Owner, Vendor).
- ☐ Review frequency and monitoring mechanisms (e.g., quarterly access reviews, daily log monitoring, annual risk assessment).
- ☐ Evidence references (e.g., policy IDs, procedure documents, system screenshots, scan reports, training logs) and locations in the evidence repository.

These worksheet structures should mirror the official ARC-AMPE Volume II template while remaining flexible enough to integrate into each organization's governance, risk, and compliance tooling and documentation processes.

NEXT STEPS

Organizations that have not yet begun or are mid-stream in their ARC-AMPE transition should immediately confirm applicability, secure access to the CMS Volume II SSPP template from CMS and initiate or update their ARC-AMPE gap assessment, focusing on high-impact control families such as access control, incident response, logging and monitoring, privacy, and supply chain risk. From there, entities should formalize their roadmap, align governance and resources, and establish sustainable continuous monitoring and evidence-management practices to maintain compliance beyond the deadline.

JANUS stands ready to partner with ACA Administering Entities, Medicaid agencies, exchanges, and partner organizations to conduct ARC-AMPE readiness consultations, design tailored roadmaps and provide accelerated assessments and implementation support so that compliance obligations are met on time and in a way that strengthens overall cybersecurity and risk management posture.

GSA Contract Holder
Contract # 00XYZA00B000C

JANUS Associates
1200 High Ridge Road
Stamford, CT 06905
Tel: 203.251.0200
Email: info@janusassociates.com
Website: janusassociates.com

CELEBRATING JANUS 37+ YEARS PROTECTING client data since 1988

certified WBENC WOMEN'S BUSINESS ENTERPRISE