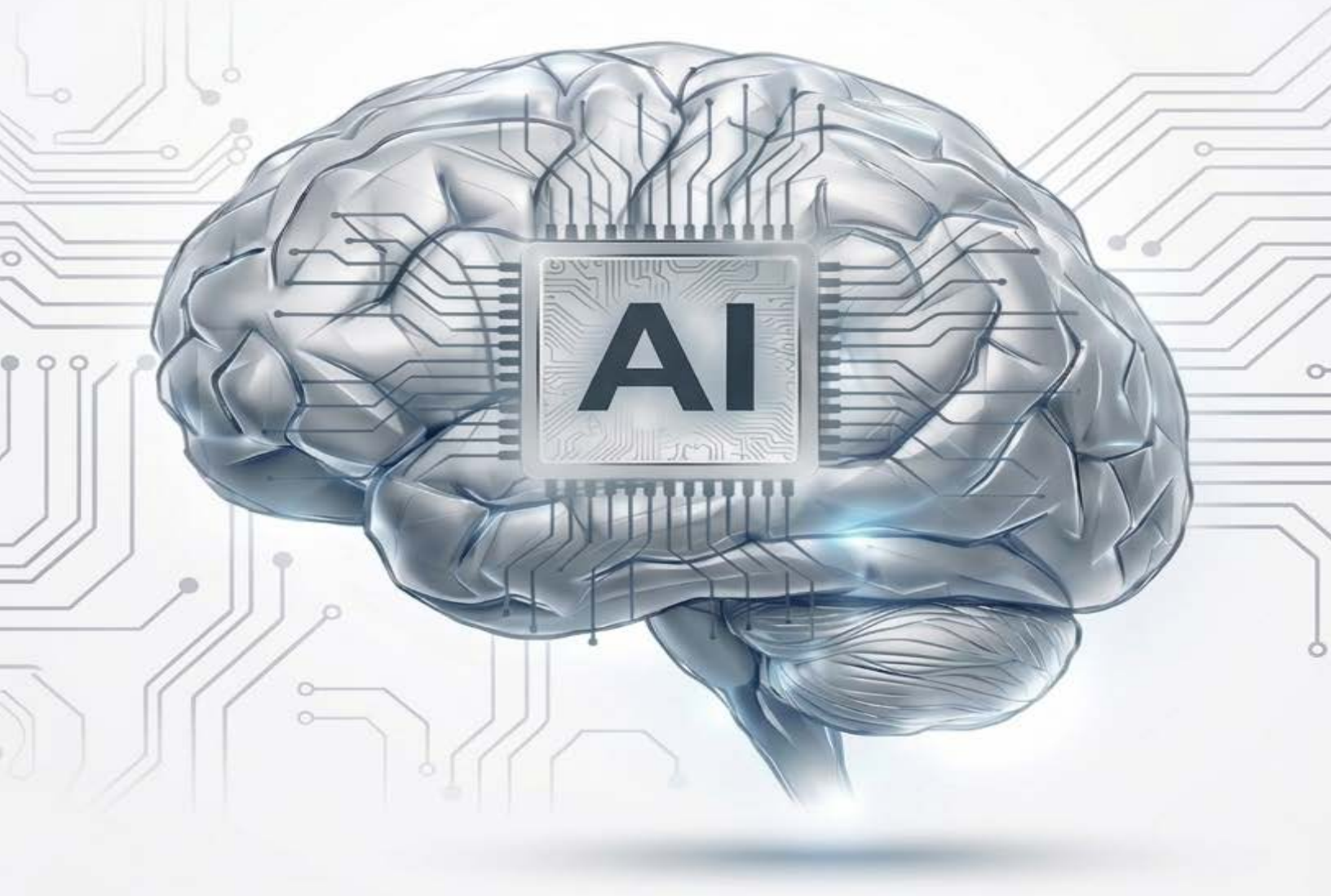
THE DECISIONS THAT COME BEFORE SCALE

An AI Lifecycle Playbook for Regulated Environments



JEROME DAVIS

Introduction

Artificial intelligence has entered regulated environments quietly. In most organizations, it did not arrive through a single strategic decision or a formal program approval. It appeared gradually, embedded in commercial software, introduced through analytics initiatives, explored by development teams, or adopted by business units seeking efficiency. By the time leadership began asking how AI should be governed, it was already in use.

This is not a failure of oversight. It is a natural consequence of how modern technology diffuses into complex organizations. AI systems do not announce themselves as governance challenges. They present as features, accelerators, or incremental improvements. Yet beneath that surface, they introduce a fundamentally different risk profile—one that does not align cleanly with the assumptions that underpin traditional software governance, security controls, or compliance processes.

Most existing governance models were designed for systems that behave predictably, execute deterministic logic, and remain largely static once deployed. AI systems do not operate this way. They are shaped by data rather than rules, influenced by human interaction, and capable of changing behavior over time. Their impact is often indirect, emerging through decision support, automation, and pattern recognition rather than explicit action. As a result, risk does not concentrate at a single point in the lifecycle. It accumulates gradually, surfaces unexpectedly, and often becomes visible only after a system is already operational.

This creates a structural problem for regulated organizations. Accountability becomes ambiguous. Approval boundaries blur. Controls that once provided confidence no longer map cleanly to how systems actually behave. Leaders are left balancing innovation against exposure without a shared language to describe what is acceptable, what requires oversight, and what constitutes a failure of governance. Technical teams move forward because the tools are available. Risk and compliance teams struggle to assess systems that do not fit existing categories. Executives sense the implications but lack a framework that translates concern into action.

The absence of a coherent AI lifecycle is not merely a documentation gap. It is an operational vulnerability. When AI systems are introduced without explicit governance, organizations inherit risk that is difficult to measure, defend, or explain. Decisions that once could be justified through design documentation or control attestations now depend on evolving data, probabilistic outputs, and human-machine interaction. In regulated environments, this creates exposure not only to compliance findings, but to reputational, legal, and operational consequences that extend beyond any single system.

This guide exists to address that reality. It does not attempt to slow adoption or impose artificial barriers to innovation. It assumes that AI will continue to be used, expanded, and integrated into core business processes. Its purpose is to provide a structured way to think about AI as a lifecycle-managed capability rather than a collection of disconnected tools. It is designed to help organizations articulate accountability, apply oversight proportionate to risk, and create continuity between strategy, implementation, and operation.

The framework presented here is intentionally pragmatic. It does not require organizations to abandon existing governance structures or adopt a rigid, one-size-fits-all model. Instead, it offers a way to integrate AI considerations into familiar decision points: how problems are defined, how data is handled, how systems are approved, how performance is monitored, and how incidents are addressed. It treats AI not as a special case that demands entirely new institutions, but as a class of systems that require clearer boundaries, earlier scrutiny, and sustained oversight.

Most importantly, this framework is written for the people who carry responsibility without always having direct control. Program leaders accountable for delivery. Executives accountable for outcomes. Risk, compliance, security, and legal professionals accountable for protecting the organization. Technical teams accountable for building systems that work in the real world. AI governance cannot belong to any one of these groups alone. It exists at their intersection, where decisions made early echo long after deployment.

What follows is not a theoretical exploration of artificial intelligence, nor a checklist designed to satisfy a single regulatory interpretation. It is an operating model intended to help organizations move forward with clarity rather than caution alone. It recognizes that uncertainty cannot be eliminated, but it can be managed deliberately. It assumes that good governance is not about preventing failure at all costs, but about ensuring that when systems evolve, the organization remains in control of their impact.

For some readers, this introduction will be enough. It may clarify why familiar governance approaches feel increasingly strained. It may articulate concerns that have been difficult to name. It may help identify who inside the organization needs to be involved in decisions that are already being made informally. If that is all it does, it has served its purpose.

For those who continue, the sections that follow provide the structure, language, and mechanisms needed to operationalize responsible AI governance. Not as an abstract ideal, but as a practical discipline aligned with how regulated organizations already function.

End Of Section

Executive Orientation

This guide establishes the organization's authoritative framework for governing Artificial Intelligence (AI) systems across their entire lifecycle. Its purpose is to provide a unified, risk-informed, and auditable approach for initiating, developing, deploying, and sustaining AI capabilities—ensuring that every AI initiative aligns with organizational strategy, complies with relevant standards, and meets stakeholder expectations for safety, security, and trustworthiness.

This guide functions as the single source of truth for AI governance and is intended for use by project teams, program managers, engineers, data professionals, and executive sponsors responsible for AI-related decision-making. It also serves as the foundational reference for emerging enterprise certification readiness under ISO/IEC 42001 and other governance frameworks.

Scope and Applicability

This governance framework applies broadly across the organization and is intended to support every category of AI system development, deployment, and operational use. It encompasses pilot projects, proofs of concept, and research efforts, as well as fully operational AI systems that support enterprise missions and customer requirements. It also governs modernization initiatives where AI capabilities are integrated into legacy systems, externally hosted or vendor-provided AI services used by the organization and internally leveraged generative AI productivity tools or agentic systems employed by staff. The framework is deliberately technology-agnostic, ensuring that it remains relevant across predictive and machine-learning models, generative AI and large language model applications, autonomous and multi-agent systems, AI-enabled decision-support capabilities, and embedded AI components within broader software platforms.

Key Standards and Source Frameworks

This governance model is grounded in a unified set of authoritative standards that collectively ensure rigor, compliance, and trust across AI system development and operations. It incorporates the CPMAI v7 methodology to structure the AI/ML lifecycle and deliverables, while ISO/IEC 42001 provides the requirements for establishing and maintaining an AI Management System, including Clauses 4–10 and Annex A controls. These are complemented by ISO/IEC 23894 for AI risk management principles and the NIST AI RMF 1.0 framework, which articulates the Govern, Map, Measure, and Manage trustworthiness functions. Security and privacy expectations are further strengthened by alignment with NIST SP 800-53 Rev 5 control families, NIST SP 1270 for bias identification and mitigation, and NIST AI 100-1 for Generative AI security. DoD-specific requirements—including CSRMC modernization principles and RAISE guidance—ensure preparedness for mission-driven and defense-aligned AI environments. Additional federal and international frameworks, such as OMB M-25-21 and the EU AI Act, inform regulatory expectations for high-risk AI systems and enterprise governance.

Policy Integration and Organizational Alignment

The AI Governance Framework is intentionally designed to integrate seamlessly with the organization's existing management systems and enterprise controls. It aligns with the Quality Management System (ISO 9001), the Information Security Management System (ISO/IEC 27001), and all related privacy, cybersecurity, and risk management policies. This alignment ensures that AI governance does not operate in isolation but instead reinforces established accountability structures, supports cross-standard control harmonization, preserves traceability and documentation integrity, and synchronizes AI governance activities with existing audit and management review cycles. By embedding AI governance within these broader organizational systems, the framework strengthens overall compliance maturity and operational coherence.

Governance Roles and Accountability Model

A successful AI governance program relies on clearly defined roles, responsibilities, and decision-making authorities. The AI Governance Lead is responsible for maintaining the governance framework, ensuring compliance, and overseeing ethical and risk-based considerations. Program Managers serve as the operational leads who drive project execution, coordinate deliverables, and ensure readiness for governance phase gates. Data Leads or Data Stewards manage data quality, provenance, and associated risks, while ML/AI Engineers conduct model development, testing, and documentation activities in alignment with governance requirements. Risk Officers and Security Analysts ensure that cybersecurity, privacy, and control obligations—including those from NIST SP 800-53—are fully addressed. The Ethics Officer guides fairness, transparency, and human oversight decisions. Ultimately, the Executive Sponsor holds final authority for risk acceptance and approvals to proceed. A detailed RACI matrix describing these relationships will be provided in Section 4.

Governance Structure and Escalation Flow

The governance structure establishes a clear escalation flow to ensure that AI systems advance through their lifecycle only after meeting required controls, risk criteria, and documentation expectations. Operational issues are first addressed by the Program Manager, while compliance questions, deviations, or interpretation of governance requirements escalate to the AI Governance Lead. Any unresolved risks or decisions requiring acceptance beyond predefined thresholds are elevated to the Executive Sponsor. This structure ensures that risk-based decisions are transparent, properly authorized, and aligned with organizational priorities, reducing exposure to unmanaged or misunderstood AI-related risks.

How to Use This Guide

This guide is intended to be used as a practical reference throughout all phases of AI system planning, development, deployment, and sustainment. Project teams should rely on it during early scoping to understand mandatory deliverables, consult it during each governance phase gate to prepare required evidence, and reference it during technical development activities to ensure alignment with security, privacy, and risk expectations. It is also a foundational resource during incident response, post-deployment monitoring, and internal or external audits. Each section provides clear requirements, governance expectations, and lifecycle criteria necessary for achieving compliant and trustworthy AI implementations.

Definitions and Terminology

To promote clarity and consistency, this guide uses standardized terminology drawn from ISO/IEC 42001, the NIST AI RMF, and DoD guidance. Key terms such as AI System, Model, Training Data, Inference, Bias, Statement of Applicability, Risk Acceptance, Material Change, Continuous Compliance Validation (CCV), and AI System Resilience carry specific meanings within the context of this framework. A complete glossary of terms is provided in Appendix F to ensure uniform understanding across all teams and stakeholders.

Document Control and Ownership

Document control for this guide follows the organization’s formal management system processes. The AI Governance Lead serves as the primary document owner, with operational updates delegated to the Program Manager as needed. The guide undergoes review on an annual basis or when triggered by significant regulatory changes, emerging risks, or updates to referenced standards. All changes are version-controlled through established QMS/ISMS procedures. Major revisions require approval from the Executive Sponsor, and retention and archival practices follow ISO/IEC 42001 Clause 7.5 requirements for documented information.

End Of Section

Section 1 – Methodology Overview

1.1 Integrated Governance Methodology

The AI Governance Framework is built on the principle of harmonizing multiple industry, federal, and defense standards into a single, coherent operating model for AI system oversight. This integration ensures that AI initiatives are executed with rigor, transparency, accountability, and resilience while maintaining alignment with regulatory, security, and ethical requirements. The methodology is intentionally designed to be system-agnostic, enabling its application across a diverse set of AI technologies, deployment environments, and mission contexts.

The framework draws from CPMAI for lifecycle structure; ISO/IEC 42001 for management system requirements; the NIST AI RMF for trust, safety, and governance considerations; NIST SP 800-53 Rev 5 for security and privacy controls; and DoD CSRMC for modernization principles emphasizing automation, resilience, and mission-driven prioritization. By unifying these standards, the methodology supports both internal governance needs and external certification readiness.

1.2 CPMAI Lifecycle Alignment

The framework is anchored in the CPMAI methodology, which defines six iterative phases: Business Understanding, Data Understanding, Data Preparation, Model Development, Model Evaluation, and Operationalization. Each phase provides a predictable structure for progressing AI initiatives while embedding consistent checkpoints for governance, risk assessment, and documentation.

Within this guide, each CPMAI phase is expanded to include:

- Integrated deliverables aligned to ISO/IEC 42001 and NIST AI RMF
- Required evidence tied to NIST SP 800-53 controls
- CSRMC modernization overlays such as CCV, resilience assessments, and telemetry enablement
- Defined roles, responsibilities, and exit criteria

This alignment ensures that AI projects maintain lifecycle discipline while remaining flexible enough to accommodate iterative development, Agile workflows, and rapid experimentation.

1.3 ISO/IEC 42001 Management System Integration

ISO/IEC 42001 establishes the structure for an AI Management System (AIMS), which functions similarly to an ISMS under ISO/IEC 27001 but is tailored to the unique risks associated with AI systems. The framework incorporates Clauses 4–10 and Annex A controls to ensure that AI governance is embedded within the organization's broader management system environment.

Through this integration, the governance methodology enforces requirements for context-setting, leadership involvement, planning, operational controls, performance evaluation, and continual improvement. ISO/IEC 42001 also reinforces the need for robust documentation practices, risk assessments, monitoring of AI system behavior, and human oversight mechanisms.

1.4 NIST AI RMF Trustworthiness Integration

The NIST AI RMF provides the trustworthiness model through four core functions: Govern, Map, Measure, and Manage. These functions guide responsible AI design, development, deployment, and monitoring. Throughout this governance framework, each CPMAI phase is mapped to relevant AI RMF functions to ensure consistency with NIST best practices.

This integration strengthens:

- Accountability and governance structures (Govern)
- Context establishment and risk scoping (Map)
- Measurement of model performance, security, and fairness (Measure)
- Ongoing risk treatment and operational stability (Manage)

Together, these functions reinforce the organization's ability to design and operationalize AI systems that meet expectations for safety, robustness, transparency, and human-centric oversight.

1.5 Security and Privacy Control Integration

Because AI systems inherit and introduce security and privacy risks, the methodology embeds NIST SP 800-53 Rev 5 control considerations across every phase of the lifecycle. Controls related to access management, data protection, auditing, configuration management, resilience, supply chain integrity, and system monitoring are referenced to ensure comprehensive security integration.

The framework does not treat controls as a separate compliance exercise; instead, they are incorporated as part of the deliverables, evidence requirements, and governance checkpoints defined for each CPMAI phase. The result is a governance model that meets federal expectations for security and privacy while enabling automation and continuous assurance.

1.6 Continuous Risk Management and CSRMC Modernization

To elevate the governance framework to modern defense and enterprise standards, the methodology incorporates continuous risk management principles drawn from both NIST and DoD CSRMC. These enhancements emphasize automation, telemetry, resilience, and mission-driven prioritization.

CSRMC influences this governance methodology by introducing:

- Mission Risk Profiling (MRP) for early alignment to operational priorities
- Continuous Compliance Validation (CCV) to automate post-deployment checks
- Automated Evidence Package (AEP) generation for audit readiness
- AI System Resilience assessments to address adversarial and systemic threats
- Reciprocity and inheritance of existing security artifacts
- Telemetry-driven governance operations for AI systems

This modernization ensures that the governance framework remains resilient, measurable, and responsive to real-world operational risks.

1.7 Integration with SDLC, Agile, and DevSecOps

AI initiatives frequently operate within hybrid environments involving traditional software engineering, MLOps pipelines, and DevSecOps practices. The governance methodology is compatible with Agile and iterative development cycles and aligns with DevSecOps concepts such as automated testing, continuous monitoring, and secure deployment pipelines.

This alignment ensures that governance processes enhance rather than hinder project delivery, allowing teams to maintain velocity while meeting compliance, security, and oversight expectations.

1.8 Evidence Traceability and Audit Readiness

A core principle of this methodology is the requirement for clear evidence traceability across every phase of the AI lifecycle. Evidence captured throughout development—such as evaluation reports, resilience assessments, telemetry outputs, lineage documentation, and approval records—supports audit readiness for ISO/IEC 42001 certification, internal quality audits, customer validation, and regulatory review.

The governance methodology therefore establishes mandatory evidence categories, retention expectations, and documentation hierarchies to maintain consistency and accountability.

1.9 Visual Crosswalk and Standards Harmonization

The governance model leverages a visual crosswalk diagram that illustrates how CPMAI phases align with ISO/IEC 42001 clauses, NIST AI RMF functions, and NIST SP 800-53 control families. This diagram provides project teams and leadership with a concise reference to understand how standards intersect and where specific responsibilities reside within the lifecycle.

1.10 Alignment With DoD CSRMC

CSRMC serves as a modernization overlay to the governance methodology. Its principles—automation, mission-driven prioritization, reciprocal authorization, and resiliency—strengthen the organization's ability to manage AI risks in dynamic operational environments.

By incorporating CSRMC concepts into the lifecycle, evidence model, and sustainment strategy, the framework ensures that AI systems remain continuously validated, operationally resilient, and aligned with mission-critical requirements. This alignment positions the governance model to meet contemporary DoD expectations while enhancing enterprise assurance for all AI deployments.

End Of Section

Section 2 – CPMAI Phases

2.1 Phase I – Business Understanding

Phase I establishes the foundational alignment between organizational objectives, mission priorities, and the intended purpose of the AI system. This phase begins with a thorough exploration of the business context, operational drivers, and stakeholder expectations. The primary intent is to ensure that the AI initiative is not approached as a standalone technical project but as a strategic capability that directly supports mission outcomes, complies with governance requirements, and aligns with enterprise risk appetite.

During this phase, the team develops key governing artifacts—including the Mission Risk Profile (MRP), early versions of the Statement of Applicability (SoA), and the Critical Controls Identification Artifact. These deliverables set the tone for all subsequent phases by clarifying what risks matter most, what ethical and regulatory constraints apply, and how governance will be measured. The Program Manager and AI Governance Lead work closely to validate business goals, articulate value propositions, and ensure that all stakeholders understand both the potential benefits and associated risks of the AI system.

Exit from this phase requires formal confirmation that business objectives are feasible, mission-aligned, and governed under approved risk criteria. The MRP and preliminary critical controls must be reviewed and accepted before work progresses into data-focused activities.

2.2 Phase II – Data Understanding

Phase II focuses on developing a deep understanding of the data required to meet the business objectives established in Phase I. This includes assessing data sources, data quality, representativeness, lineage, bias risk, and any legal or ethical restrictions associated with data usage. The purpose of this phase is to ensure that the project is grounded in a realistic appraisal of data suitability and that any limitations are identified early to prevent rework or misalignment later in the lifecycle.

Key governance activities in this phase include drafting the Telemetry Configuration and Data Flow Specification, identifying initial inherited controls for the Reciprocity & Inheritance Register, and conducting privacy and bias assessments aligned with ISO/IEC 42001 and NIST SP 1270. These activities support the development of trustworthy datasets and prepare the operational groundwork for monitoring and continuous compliance later in the lifecycle.

Completion of Phase II requires validated confirmation that data is appropriate for modeling, that relevant risks have been documented, and that telemetry and inheritance considerations have been initiated. Governance leadership must approve these outcomes before data transformation begins.

2.3 Phase III – Data Preparation

Phase III transitions the project from understanding data to preparing it for use in model development. Activities in this phase include cleaning, transforming, labeling, augmenting, and versioning datasets in line with reproducibility and governance expectations. Effective data preparation is critical, as the integrity and trustworthiness of the AI system hinge on the quality and transparency of the training data.

Governance integration intensifies here through the creation of the Automated Evidence Package (AEP) for data lineage, ensuring that every transformation is recorded and traceable. Teams also validate that telemetry instrumentation is embedded in data pipelines to support drift detection and CCV activities later in the lifecycle. This phase ensures that datasets are not only technically ready but also compliant with required controls under ISO/IEC 42001, NIST SP 800-53, and CSRMC modernization expectations.

Phase III concludes when datasets meet defined quality thresholds, lineage documentation is complete, and telemetry readiness is confirmed. Governance approval is required before moving into model construction.

2.4 Phase IV – Model Development

Phase IV focuses on the creation of the AI model, integrating both technical experimentation and governance-driven safeguards. This includes selecting modeling approaches, performing iterative training, and evaluating early-stage performance. The phase also incorporates threat modeling, adversarial testing, leakage analysis, and explainability planning to ensure that the model develops within secure, transparent, and ethical boundaries.

The governance model introduces two critical CSRMC-aligned artifacts at this stage: the initial Cyber Resilience Posture Report (CRPR) and the Automated Control Validation Ruleset (ACVR). These artifacts help formalize model-level risk assessments, adversarial robustness considerations, and automated validation criteria. Throughout this phase, evidence is captured for compliance with NIST SP 800-53 controls related to testing, configuration management, and supply chain integrity.

Progression to the evaluation phase requires that model performance, security, and resilience criteria are met and that governance stakeholders approve the CRPR and ACVR.

2.5 Phase V – Model Evaluation

Phase V provides an independent and comprehensive evaluation of the model's readiness for deployment. Evaluation activities focus on verifying fairness, robustness, transparency, privacy protections, and mission alignment. This phase confirms whether the model meets operational requirements and if residual risks are within acceptable bounds.

A key modernization requirement in this phase is completing a pre-deployment Continuous Compliance Validation (CCV) cycle, which uses telemetry and automated checks to validate compliance against defined technical and governance thresholds. The Cyber Resilience Posture Report is updated based on evaluation findings, and all evidence is consolidated into the AEP for audit readiness.

Exit from this phase requires governance approval of the updated CRPR, acceptance of residual risk by the Executive Sponsor, and a formal Go/No-Go decision.

2.6 Phase VI – Operationalization

Phase VI transitions the AI system from development to managed operational use. The focus shifts to monitoring, resilience, incident response, CCV execution, and model lifecycle management. This phase requires ongoing governance oversight to ensure that the system remains trustworthy, secure, compliant, and aligned with mission needs.

Key activities include activating continuous telemetry, generating operational AEPs, executing CCV cycles, monitoring drift and dependency risks, and ensuring that human oversight is functioning as intended. This phase integrates seamlessly with the organization's operational governance routines, including incident management, change control, and periodic management reviews.

Completion of this phase requires demonstrating stable operations, validated resilience posture, active telemetry feeds, and standing CCV cycles. Governance leadership must confirm these outcomes before the system enters long-term sustainment and continuous improvement cycles.

End Of Section

Section 3 – Cross-Cutting Controls & Governance

3.1 Overview of Cross-Cutting Governance Functions

Cross-cutting governance functions provide continuous oversight across all phases of the AI system lifecycle. These functions ensure that risk management, documentation, oversight, and compliance activities are not limited to discrete milestones but are embedded into day-to-day operations. The purpose of this section is to define the enterprise-level governance activities that operate in parallel with the CPMAI phases and enable consistent, transparent, and auditable management of AI systems. These cross-cutting functions form the backbone of an effective AI Management System (AIMS) and prepare the organization for ISO/IEC 42001, NIST AI RMF, and DoD CSRMC compliance.

3.2 Continuous Risk Management

Risk management is a perpetual activity woven through every phase of AI development and operational use. The organization maintains a unified AI Risk Register that captures technical, ethical, operational, cybersecurity, and mission-driven risks. These risks evolve as the system progresses, requiring consistent updates informed by telemetry, evaluation results, and stakeholder feedback. Continuous risk management ensures that residual risks remain within tolerance, informs decision-making, and strengthens readiness for external assessment or certification.

This process is reinforced by CSRMC modernization concepts, most notably the Mission Risk Profile (MRP), which identifies high-priority mission impacts early, and Continuous Compliance Validation (CCV), which automatically evaluates risk posture during deployment. Together, these capabilities enable ongoing alignment with mission requirements and operational resilience.

3.3 Change Management and Material Change Evaluation

AI systems degrade, drift, and evolve over time. To maintain governance integrity, the organization implements a structured change management process that evaluates all modifications—including data changes, model retraining, shifts in dependencies, or updates to deployment infrastructure. Any proposed change must be reviewed for its impact on risk posture, compliance obligations, human oversight requirements, and operational performance.

A material change evaluation determines whether a modification requires partial or full reenactment of earlier lifecycle phases, such as renewed testing, updated bias assessments, or reissued approvals. This evaluation is consistent with ISO/IEC 42001 Clause 8 requirements and integrates CSRMC principles to ensure resilience and mission-aligned risk assessment.

3.4 Decision Accountability and Executive Oversight for AI Systems

AI governance extends beyond the existence of controls, documentation, or technical safeguards. It requires demonstrable accountability for the decisions that introduce, authorize, and sustain AI-enabled capabilities within the enterprise. Because AI systems can influence outcomes in non-deterministic and evolving ways, governance must ensure that decision authority remains visible, revisitable, and actively exercised over time.

Within this framework, accountability is established by explicitly linking AI system artifacts to the decisions they support. Business justification documents, risk assessments, Statements of Applicability, approval records, and operational review outputs are treated not merely as compliance evidence, but as decision records that capture the rationale, assumptions, and risk acceptance judgments made at each point in the lifecycle. These artifacts collectively demonstrate why an AI system was approved, under what conditions it was deemed acceptable, and which leaders were responsible for those determinations.

Executive oversight is maintained through structured review mechanisms that evaluate whether the conditions under which prior decisions were made continue to hold. As AI systems evolve through retraining, data changes, dependency updates, or expanded use, governance reviews reassess alignment with original intent, risk tolerance, and mission objectives. This ensures that accountability does not expire at deployment but persists throughout operational use.

The governance model therefore requires that leadership roles identified in Section 4 remain engaged not only at initial approval gates, but during material change evaluations, periodic performance reviews, and continuous compliance validation cycles. These interactions provide traceable evidence that AI-related decisions are actively owned, monitored, and reaffirmed, rather than passively inherited as systems mature.

By framing governance artifacts as decision accountability instruments, the organization demonstrates that AI systems are not operating on autopilot. Instead, they remain under explicit human authority, with clear ownership for outcomes, risk acceptance, and corrective action. This approach satisfies external accountability expectations, including those articulated by oversight bodies such as the U.S. Government Accountability Office, while remaining fully aligned with ISO/IEC 42001 management system principles.

3.5 Statement of Applicability (SoA) Management

The Statement of Applicability functions as the authoritative record of the controls and requirements that apply to a given AI system. The SoA is first drafted during Phase I and progressively updated across the lifecycle as risks evolve, new controls become relevant, or exemptions are justified. Managing the SoA ensures traceability between the AI system and the underlying governance framework, supporting audits, internal reviews, and certification preparation.

The SoA also links ISO/IEC 42001 controls, NIST AI RMF functions, NIST SP 800-53 Rev 5 controls, and CSRMC modernization criteria, providing a single consolidated view of the system's governance footprint.

3.6 Document and Record Control

Effective document and record control ensures that all governance documentation remains accurate, current, and accessible. This includes lifecycle artifacts, evidence logs, telemetry outputs, risk assessments, approval forms, and operational reports. Document control practices follow ISO/IEC 42001 Clause 7.5 requirements, defining how documents are created, stored, protected, versioned, and archived.

Maintaining robust document control supports transparency, enhances audit readiness, and reduces the risk of inconsistent or outdated artifacts influencing decision-making. Document retention schedules are aligned with both internal QMS/ISMS practices and contractual or regulatory requirements.

3.7 Competence and Awareness

The organization ensures that individuals working with AI systems possess the necessary skills, training, and awareness to perform their duties responsibly. Competence programs include role-based training in AI safety, data management, privacy, security, ethics, and operational monitoring. Individuals must demonstrate proficiency in relevant governance requirements and understand how their responsibilities influence system trustworthiness.

Awareness efforts support cultural adoption by equipping stakeholders with knowledge of AI risks, governance principles, and reporting mechanisms, consistent with ISO/IEC 42001 Clauses 7.2 and 7.3.

3.8 Human Oversight and Authority Model

Human oversight is an essential safeguard for ensuring that AI systems operate within acceptable bounds and remain aligned with ethical and mission expectations. The authority model defines who has oversight responsibilities, how escalations occur, and what thresholds require intervention. Oversight includes monitoring decision-making behavior, reviewing anomalies, validating model explanations, approving risk acceptance, and ensuring that fallback mechanisms are effective.

This human-centered governance requirement aligns with ISO/IEC 42001 Annex A controls and NIST AI RMF expectations for transparency and accountability.

3.9 Supplier and Third-Party Management

AI systems frequently rely on external vendors, cloud providers, data suppliers, and toolchains. The organization maintains a structured third-party management process that evaluates supplier trustworthiness, contractual obligations, security posture, and alignment with AI governance requirements. Supplier assessments include reviewing control inheritance opportunities, validating evidence provided by vendors, and monitoring ongoing compliance.

Where applicable, CSRMC reciprocity and inheritance concepts are used to reuse validated controls, reducing redundancy while maintaining assurance.

3.10 Corrective and Preventive Actions

Corrective and preventive action (CAPA) processes address gaps, deviations, incidents, or audit findings that arise during the AI system lifecycle. Corrective actions resolve detected issues, while preventive actions identify and mitigate potential problems before they impact system trustworthiness. The CAPA process follows ISO/IEC 42001 Clause 10.2 and ensures that governance improvements are data-driven and sustainable.

Each CAPA entry is tracked, assigned, and verified for completion, strengthening both compliance and operational integrity.

3.11 Internal Audits and Continual Improvement

Internal audits provide objective evaluations of the AI governance framework, checking conformance with ISO/IEC 42001, NIST AI RMF, NIST SP 800-53, and CSRMC modernization obligations. Audits assess documentation, evidence quality, system behavior, and adherence to governance requirements.

Continual improvement activities arise from audit findings, performance measurements, incident reviews, and user feedback. The organization maintains a structured improvement cycle aligned with ISO/IEC 42001 Clause 10.3 to ensure that governance practices evolve alongside technological advances, regulatory changes, and operational experience.

3.12 AI Risk Taxonomy

An enterprise AI Risk Taxonomy provides a standardized structure for identifying, classifying, and managing risks across all AI initiatives. This taxonomy enables consistent risk reporting, clearer communication among stakeholders, and alignment with ISO/IEC 42001, NIST AI RMF, and CSRMC. The taxonomy categorizes risks into technical, ethical, operational, cybersecurity, privacy, regulatory, and mission-driven domains. Each category includes representative risk types—for example, model bias, data drift, adversarial vulnerability, hallucination, system instability, supply chain exposure, and mission degradation. By maintaining a shared taxonomy, the organization ensures that all teams evaluate risks using consistent language and criteria, strengthening cross-functional governance and enabling more accurate aggregation of enterprise risk.

AI Risk Taxonomy Table

Risk Domain	Description	Representative Risks
Technical	Risks arising from model behavior, performance, and reliability	Model drift, data drift, hallucinations, overfitting, instability
Ethical	Risks related to fairness, transparency, and responsible outcomes	Bias, unfair impact, lack of explainability
Operational	Risks impacting business continuity and operational performance	System downtime, dependency failures, resource saturation
Cybersecurity	Risks associated with adversarial threats or security vulnerabilities	Adversarial attacks, poisoning, model extraction, unauthorized access
Privacy	Risks related to data protection and privacy violations	Leakage, reidentification, improper data handling
Regulatory	Risks tied to compliance with laws, standards, or policies	EU AI Act noncompliance, audit failures, contractual violations
Mission-Driven	Risks affecting mission success or critical organizational functions	Mission degradation, misalignment with mission intent, performance shortfall

3.13 Governance Cadence

The governance cadence defines the structured rhythm of oversight activities required to maintain continuous compliance, transparency, and operational assurance. This cadence spans planning sessions, phase-gate reviews, risk register updates, CCV cycles, telemetry evaluations, audit preparations, and executive reviews. It ensures that governance does not occur sporadically but is woven into the organization's operational tempo.

The cadence includes recurring meetings at the operational, governance, and executive levels. Operational reviews address system performance, anomalies, and day-to-day risks. Governance reviews focus on documentation, risk posture, evidence updates, and adherence to standards. Executive reviews evaluate strategic alignment, risk acceptance decisions, and compliance with mission or contractual expectations. This structured cadence strengthens predictability, enforces accountability, and ensures that AI systems maintain a validated and trustworthy posture throughout their lifecycle.

Governance Cadence Table

Cadence Level	Frequency	Primary Activities	Participants
Operational Review	Weekly	Telemetry checks, drift analysis, anomaly review, issue escalation	Program Manager, Data Lead, ML Engineers
Governance Review	Bi-Weekly / Monthly	Risk register updates, SoA updates, documentation review, CCV preparation	AI Governance Lead, Security, Risk Officer
Executive Review	Quarterly	Risk acceptance, strategic alignment, performance evaluation, major approvals	Executive Sponsor, Leadership Stakeholders
Audit & Compliance Cycle	Annual or Triggered	Internal audits, external assessments, certification prep	Governance Lead, Internal Audit, Compliance Teams

3.14 CSRMC-Aligned Continuous Risk Management

Continuous risk management under CSRMC introduces modernization capabilities that enhance the organization's ability to monitor, assess, and validate AI systems in real time. This approach combines mission prioritization, automation, resilience analysis, and telemetry to form a dynamic and adaptive risk governance model.

Under this approach, Mission Risk Profiling (MRP) ensures that risks are evaluated through the lens of mission impact. Automated Evidence Packages (AEPs) maintain a current, traceable record of system behavior, controls, and assessments. Continuous Compliance Validation (CCV) uses automated rulesets to evaluate compliance posture during development and deployment, ensuring that AI systems remain aligned with operational, security, and ethical requirements. Telemetry streams enable real-time visibility into system behavior and support anomaly detection, resilience checks, and proactive mitigation. Collectively, these capabilities ensure that the AI governance program evolves from static, documentation-heavy processes to a continuously validated, operationally resilient governance model aligned with DoD modernization priorities.

CSRMC Continuous Risk Management Table

CSRMC Element	Description	Purpose	Lifecycle Touchpoints	Responsible Roles	Evidence Produced
Mission Risk Profile (MRP)	Identifies mission-critical impacts and operational priorities	Ensure mission-aligned risk evaluation	Phase I, Updates in II–VI	AI Governance Lead, Program Manager	Mission Risk Profile Document
Critical Controls Identification	Maps risks to prioritized security and resilience controls	Focus governance on mission-essential safeguards	Phase I–II	Governance Lead, Security Officer	Critical Controls Artifact
Telemetry Configuration & Data Flow Specification	Defines telemetry sources, visibility requirements, and monitoring strategy	Enable real-time oversight and CCV monitoring	Phase II–III	Data Lead, MLOps, Security	Telemetry Specification Document
Reciprocity & Inheritance Register	Tracks inherited controls and reused security artifacts	Reduce redundancy and reuse validated assessments	Phase II, Updates in III–VI	Governance Lead, Security Officer	Reciprocity & Inheritance Register
Cyber Resilience Posture Report (CRPR)	Summarizes resilience posture, adversarial readiness, and dependency risks	Document resilience against adversarial and systemic threats	Phase IV–V, Updates in VI	ML Engineers, Security, Governance Lead	CRPR Report
Automated Evidence Package (AEP)	Consolidated evidence bundle updated continuously	Maintain audit-ready, real-time system documentation	Phase III–VI	Governance Lead, Data Lead, MLOps	AEP Bundle (logs, reports, validations)
Continuous Compliance Validation (CCV)	Automated execution of compliance checks	Continuously validate conformance to defined controls	Phase V–VI	MLOps, Security, Governance Lead	CCV Reports
Automated Control Validation Ruleset (ACVR)	Machine-readable rules driving CCV cycles	Define automated validation criteria for risk and compliance	Phase IV–V	Governance Lead, Security Officer	ACVR Ruleset

CSRMC Element	Description	Purpose	Lifecycle Touchpoints	Responsible Roles	Evidence Produced
Deviation, Exception, & Risk Acceptance Tracking	Logs deviations and risk acceptance decisions	Ensure transparency and proper authorization of elevated risk	Phase I–VI	Governance Lead, Exec Sponsor	Risk Acceptance Register
AI System Resilience Measures	Tracks resilience mechanisms, fallback paths, and dependency strength	Strengthen operational survivability under adverse conditions	Phase IV–VI	ML Engineers, Security, Governance Lead	Resilience Measures Documentation

End Of Section

Section 4 – Roles and RACI Matrix

4.1 Overview

This section establishes the organizational roles, responsibilities, and accountability structure necessary to operate a comprehensive and certifiable AI Governance Framework. Clearly defined responsibilities are essential to ensuring that AI initiatives remain aligned with enterprise strategy, mission objectives, regulatory obligations, and ethical expectations. This section directly supports ISO/IEC 42001 Clause 5 (Leadership) and Clauses 7.2–7.3 (Competence and Awareness), integrates NIST AI RMF Govern functions, and aligns with the mission-focused decision authority model emphasized in the DoD CSRMC. By formalizing governance ownership through detailed role descriptions and a structured RACI model, the organization ensures clarity, strengthens program discipline, and enables consistent audit readiness throughout the AI lifecycle.

4.2 Role Descriptions

The following roles represent governance functions rather than job titles. They may be combined or distributed depending on the size, maturity, and structure of the organization.

Executive Sponsor

The Executive Sponsor maintains ultimate accountability for the AI system. This role ensures that the initiative aligns with enterprise strategy and mission needs, approves risk acceptance decisions, validates compliance with policies and regulations, and authorizes major governance actions. The Executive Sponsor also ensures resources and cross-organizational support are available to sustain the AI Governance Framework.

AI Governance Lead

The AI Governance Lead oversees the AI Governance Framework and ensures continuous alignment to ISO/IEC 42001, NIST AI RMF, and CSRMC modernization expectations. Responsibilities include maintaining governance policies, coordinating compliance reviews, managing lifecycle evidence, overseeing ethical and responsible AI practices, and driving consistency across AI initiatives. This role ensures that governance requirements are embedded throughout the lifecycle.

Program Manager

The Program Manager directs day-to-day execution of AI projects, ensuring that deliverables, evidence, documentation, and risk management requirements are fulfilled. This role coordinates cross-functional teams, manages phase gate readiness, oversees schedules and dependencies, and ensures that development and operational activities remain aligned with mission and business objectives.

Data Lead / Data Steward

The Data Lead ensures the quality, provenance, suitability, and governance posture of data across the AI lifecycle. Responsibilities include managing data inventories, conducting profiling, maintaining lineage, supporting bias and privacy assessments, and contributing to telemetry configuration for monitoring and CCV. The Data Lead is accountable for ensuring that data-driven risks are documented and mitigated.

ML/AI Engineer

The ML/AI Engineer develops, trains, evaluates, and documents the AI model. Responsibilities include experiment tracking, performance evaluation, explainability development, adversarial robustness analysis, and support for resilience posture assessments. This role contributes to the Automated Evidence Package (AEP), Cyber Resilience Posture Report (CRPR), and telemetry design.

MLOps / Platform Engineer

The MLOps Engineer owns the deployment, monitoring, and operational lifecycle of AI systems. Responsibilities include managing automated pipelines, ensuring secure model deployment, configuring telemetry, activating CCV cycles, and ensuring consistent operational performance. This role is central to continuous compliance and resilience activities.

Security Officer / Cyber Analyst

The Security Officer ensures integration of cybersecurity, privacy, and resilience controls within AI systems. Responsibilities include conducting adversarial threat modeling, validating telemetry integrity, implementing NIST SP 800-53 Rev 5 controls, and supporting CCV and resilience assessments. This role ensures alignment with enterprise cybersecurity architecture.

Risk Officer

The Risk Officer manages enterprise AI risks across development and deployment. Responsibilities include maintaining the AI Risk Register, monitoring residual risk, coordinating risk acceptance decisions, and ensuring alignment with mission-driven MRP requirements. The Risk Officer ensures proper escalation when governance thresholds are exceeded.

Privacy Officer / Data Protection Lead

The Privacy Officer enforces privacy and data protection requirements across the AI lifecycle. Responsibilities include validating compliance with privacy regulations, conducting data protection impact assessments, supporting minimization and retention controls, and ensuring that privacy risks are documented and mitigated.

Ethics Officer

The Ethics Officer ensures that AI systems adhere to principles of fairness, transparency, accountability, and human oversight. Responsibilities include assessing ethical risks, validating explainability, reviewing bias mitigation strategies, and ensuring alignment with responsible AI practices and ISO/IEC 42001 Annex A controls.

Internal Audit

Internal Audit independently evaluates the AI Governance Framework and its implementation. Responsibilities include verifying adherence to ISO/IEC 42001, NIST AI RMF, NIST SP 800-53, and CSRMC criteria, reviewing evidence quality, and assessing internal control effectiveness. This role supports certification readiness and external audit preparation.

Supplier/Vendor Manager

The Supplier/Vendor Manager oversees AI-relevant external suppliers, including platforms, data providers, and toolchains. Responsibilities include validating supplier controls, managing inherited control documentation, assessing supply chain risks, and coordinating ongoing compliance monitoring.

4.3 RACI Matrix Overview

The RACI matrix clarifies ownership of lifecycle tasks, governance responsibilities, and evidence requirements. It ensures that all participants understand when they are responsible, accountable, consulted, or informed for each activity. This structure eliminates ambiguity, strengthens coordination, and supports auditability by establishing consistent governance behaviors across AI initiatives. The RACI model also reinforces CSRMC-aligned decision authority and mission-focused escalation.

4.4 Delegation and Escalation Model

The delegation and escalation model establishes clear thresholds for decision-making authority across operational, governance, and executive domains. Routine project decisions remain delegated to the Program Manager and technical leads. Governance decisions, deviations, exceptions, or material changes escalate to the AI Governance Lead. Any acceptance of elevated or mission-impacting risk requires Executive Sponsor approval. This escalation structure supports rapid decision-making while preserving accountability and alignment with CSRMC mission-focused risk governance.

4.5 Competency Requirements and Training Alignment

Competence and awareness form the foundation for a trustworthy and compliant AI governance program. Each role must maintain appropriate training in AI safety, data governance, cybersecurity, privacy, risk management, and ethical principles. ISO/IEC 42001 Clause 7.2 requires evidence of competency for all individuals performing tasks that influence AI system trustworthiness. Clause 7.3 further requires awareness of AI risks, governance policies, and reporting expectations. Ongoing

education ensures that the organization adapts to emerging technologies, regulatory changes, and evolving operational risks.

4.6 Full Detailed RACI Matrix

A full detailed RACI matrix, containing role assignments for every CPMAI task, cross-cutting governance requirement, CSRMC modernization element, and evidence ownership area, is provided in Appendix A. This matrix is designed for operational teams, auditors, and governance reviewers who require comprehensive visibility into control ownership, lifecycle accountability, and compliance responsibilities.

End Of Section

Section 5 – Evidence and Documentation Index

5.1 Overview

This section defines the full set of evidence, documentation, and record-keeping expectations required to support an auditable, certifiable, and operationally trustworthy AI Governance Framework. Evidence serves as the backbone of ISO/IEC 42001 conformity, NIST AI RMF alignment, CSRMC modernization readiness, and NIST SP 800-53 control validation. By establishing clear evidence requirements for each phase of the AI lifecycle and for all cross-cutting governance functions, this section ensures that AI systems remain transparent, traceable, and continuously accountable.

The Evidence and Documentation Index also provides clarity to project teams, auditors, and leadership on where documentation resides, who owns it, how it is maintained, and how it demonstrates compliance with internal and external requirements. This structured approach transforms governance from a reactive activity into a proactive, continuous, and automated discipline.

5.2 Evidence Philosophy and Documentation Requirements

Evidence in an AI governance context is not limited to static documents produced at milestones. Instead, it encompasses a spectrum of artifacts—including automated outputs, telemetry streams, logs, assessments, meeting records, phase-gate approvals, and compliance validations—that collectively represent the system's trustworthiness. Evidence must be:

- Accurate: Reflecting actual system behavior, decisions, and risks.
- Traceable: Clearly linked to lifecycle phases, governance requirements, and controls.
- Versioned: Maintained according to ISO/IEC 42001 Clause 7.5 documentation controls.
- Reusable: Leveraging reciprocity and inheritance where appropriate to reduce redundancy.
- Automated where possible: Supporting CSRMC's Automated Evidence Package (AEP) vision to reduce manual burden.

This philosophy ensures that evidence is both meaningful and manageable, supporting operational assurance and certification readiness.

5.3 Evidence Categories

Evidence requirements span multiple categories, each serving a specific governance purpose. These categories are applicable across all AI initiatives and map directly to lifecycle phases, ISO/IEC 42001 controls, NIST AI RMF functions, NIST SP 800-53 controls, and CSRMC modernization elements.

Governance and Policy Evidence

This category includes documents demonstrating alignment with organizational policies, governance structure, ethical frameworks, leadership oversight, and internal controls.

Risk and Security Evidence

Evidence supporting continuous risk management, including risk registers, threat assessments, resilience documentation, adversarial testing, security controls, and mission risk profiling.

Data Governance Evidence

Artifacts documenting data suitability, quality, lineage, privacy compliance, profiling results, and data pipeline integrity.

Model Development Evidence

Documentation of model experiments, performance metrics, explainability analysis, bias assessments, and robustness evaluations.

Operational and Monitoring Evidence

Telemetry, logs, CCV reports, incident response records, and operational performance measures demonstrating that deployed systems remain trustworthy.

Gate Approvals and Decision Records

Formal records capturing governance decisions, risk acceptance, deviations, exceptions, and executive approvals.

5.4 Comprehensive Evidence Index

The following table outlines the major evidence artifacts required across the AI lifecycle. It provides a consolidated view of where evidence is produced, who owns it, and what governance functions it supports.

Evidence and Documentation Index Table

Artifact	Description	Lifecycle Phase	Primary Owner	Governance Alignment
AI Governance Scope Statement	Defines system purpose, scope, boundaries, and constraints.	Phase I	AI Governance Lead	ISO/IEC 42001 Clause 4, NIST AI RMF Govern
Mission Risk Profile (MRP)	Establishes mission-driven risk baseline and prioritization.	Phase I	Risk Officer	CSRMC MRP, NIST SP 800-53 RA, AI RMF Map
Statement of Applicability (SoA)	Documents applicable controls and justification.	Phases I–VI	AI Governance Lead	ISO/IEC 42001 Annex A, NIST SP 800-53
Stakeholder Register	Identifies stakeholders, roles, decision authorities.	Phase I	Program Manager	ISO/IEC 42001 Clause 4
Data Inventory	Catalog of datasets, sources, provenance, access controls.	Phase II	Data Lead	ISO/IEC 42001 Clause 8, AI RMF Map
Data Profiling Report	Summarizes data quality, distribution, bias indicators, anomalies.	Phase II	Data Lead	ISO/IEC 23894, NIST SP 1270
Privacy & Ethics Assessment	Evaluates privacy impact, fairness, transparency, and ethical risks.	Phase II	Privacy Officer & Ethics Officer	ISO/IEC 42001 Clause 8, AI RMF Map
Telemetry Configuration Specification	Defines visibility, observability, monitoring signals, and data flows.	Phase II	MLOps Engineer	CSRMC Visibility (TEL)
Data Preparation Logs	Records of cleaning, transformation, feature engineering, and labeling steps.	Phase III	Data Lead	ISO/IEC 42001 Clause 8
Automated Evidence Package (AEP) – Data	Machine-generated evidence of data lineage, integrity, and quality.	Phase III	Governance Lead / MLOps	CSRMC Automation (AEP)
Model Experiment Logs	Versioned documentation of experiments, parameters, and results.	Phase IV	ML Engineer	AI RMF Measure, NIST SP 800-53 SA
Threat Model	Adversarial and misuse risk assessment for model and system.	Phase IV	Security Officer	CSRMC Survivability (RES), NIST SP 800-53 SI/SR
Cyber Resilience Posture Report (CRPR)	Evaluates model/system resilience, robustness, and survivability.	Phase IV–V	Security Officer & ML Engineer	CSRMC Survivability (RES)
Automated Control Validation Ruleset (ACVR)	Rules defining automated CCV tests and compliance logic.	Phase IV–V	AI Governance Lead	CSRMC Automation (CCV)
Evaluation Report	Comprehensive evaluation results including fairness, robustness, and performance.	Phase V	ML Engineer	NIST AI RMF Measure
Go/No-Go Decision Record	Executed formal authorization or rejection for deployment.	Phase V	Executive Sponsor	ISO/IEC 42001 Clause 9
CCV Results	Automated evidence of compliance and control effectiveness.	Phase VI	MLOps Engineer	CSRMC CCV, ISO/IEC 42001 Clause 9
Operational Telemetry Logs	Real-time drift monitoring, anomalies, and operational indicators.	Phase VI	MLOps Engineer	ISO/IEC 42001 Clause 9, AI RMF Manage
Incident Response Report	Documentation of detected incidents, mitigations, lessons learned.	Phase VI	Security Officer	ISO/IEC 42001 Clause 10, NIST SP 800-61
Management Review Record	Executive-level oversight summary, decisions, and improvement actions.	All Phases	Executive Sponsor	ISO/IEC 42001 Clause 9

5.5 Evidence Repository Structure

All evidence must be stored in a structured, access-controlled repository integrated with the organization's QMS, ISMS, and AIMS. The repository must enforce version control, retention policies, and audit logging in alignment with ISO/IEC 42001 Clause 7.5.

A recommended structure includes:

- Root Directory: AI Governance Repository
- Phase I – Business Understanding
- Phase II – Data Understanding
- Phase III – Data Preparation
- Phase IV – Model Development
- Phase V – Model Evaluation
- Phase VI – Operationalization
- Cross-Cutting Governance (Risk, Compliance, Telemetry, Audit)
- Management Reviews
- Incident Response Records
- Appendices and Reference Materials

5.6 Evidence Retention and Archival

Evidence retention follows the requirements of ISO/IEC 42001, ISO/IEC 27001, contractual obligations, and regulatory mandates. Retention durations must be documented, consistently applied, and reviewed during management evaluations. Archival procedures must ensure long-term integrity, readability, and accessibility, particularly for AI systems supporting mission-critical or regulated use cases.

5.7 Audit Readiness and Traceability

Audit preparedness is strengthened through continuous documentation, automated evidence generation, and structured record-keeping. Traceability across lifecycle artifacts ensures that auditors can easily validate:

- System purpose and scope
- Control applicability and justification
- Risk posture evolution
- Data integrity and model development practices
- Operational performance and resilience
- Governance decision rationale

By maintaining a complete and accurate evidence index, the organization supports internal audits, ISO/IEC 42001 certification audits, customer assessments, and regulatory inquiries with minimal disruption.

End Of Section

Section 6 – Maturity and Rollout Model

6.1 Overview

This section defines the organization's approach to adopting, scaling, and institutionalizing the AI Governance Framework. While earlier sections describe the structure and processes required for compliant and trustworthy AI operations, the maturity and rollout model focuses on how these capabilities are introduced, operationalized, and continuously improved across the enterprise. The goal is to ensure that AI governance becomes an embedded, sustainable organizational function rather than a one-time initiative. This section aligns with ISO/IEC 42001 Clauses 9 and 10 (performance evaluation and improvement), NIST AI RMF's Govern function, and CSRMC's emphasis on modernization and resilience.

6.2 AI Governance Maturity Model

The maturity model provides a structured view of the organization's progression toward full governance capability. Each stage represents a meaningful advancement in processes, controls, cultural adoption, and operational readiness.

Stage 1 – Foundational Awareness

At this stage, the organization recognizes the need for AI governance but lacks formal processes, controls, and accountability structures. AI experimentation may exist, but oversight, documentation, and risk management are inconsistent. The primary goal is to establish basic awareness of AI risks, responsibilities, and governance expectations.

Stage 2 – Structured Governance

The organization formalizes governance roles, documentation expectations, lifecycle processes, and risk management procedures. Evidence generation becomes consistent, and oversight mechanisms are introduced. Initial alignment with ISO/IEC 42001 and NIST AI RMF begins, and projects are required to pass through basic governance checks.

Stage 3 – Integrated Management System

AI governance becomes fully integrated with enterprise systems such as QMS, ISMS, risk management, and cybersecurity. Automated evidence generation is introduced, and CSRMC-aligned monitoring begins. Governance becomes consistent across programs, and cross-functional roles support lifecycle oversight and operational readiness.

Stage 4 – Continuous Assurance and Optimization

The organization achieves continuous monitoring and CCV automation, with telemetry-driven governance and resilience assessments fully operational. Governance functions are optimized through automation, mission-driven risk prioritization, and maturity in evidence generation. The organization is positioned for ISO/IEC 42001 certification or demonstrates equivalent conformance. AI systems operate with continuous accountability and enterprise-level resilience.

6.3 CSRMC-Influenced Tier 4 – Enterprise Continuous Assurance

Tier 4 incorporates CSRMC modernization concepts to transform governance from periodic review to continuous, mission-aligned assurance. Capabilities include automated validation of controls, telemetry-based monitoring, continuous risk posture assessment, resilience reviews, and mission impact tracking.

Organizations operating at this tier:

- Continuously validate compliance through CCV cycles
- Maintain fully automated AEPs
- Monitor drift, anomalies, adversarial activity, and resilience posture in real time
- Use mission risk criteria and operational telemetry to guide governance decisions
- Maintain readiness for internal audits, ISO/IEC 42001 certification, and regulatory assessments

This tier represents the enterprise-level operational state required for mission-critical or regulated AI deployments.

6.4 The 180-Day Rollout Plan

This rollout plan establishes the initial operational capability (IOC) of the AI Governance Framework. The intent is to stand up the essential infrastructure, processes, roles, and controls within 180 days before transitioning into the full sustainment cycle.

Days 1–30: Governance Stand-Up and Orientation

- Appoint governance roles (Governance Lead, Risk Officer, Data Lead, Privacy Officer, Security Officer, etc.)
- Establish the AI Governance Repository and documentation control processes
- Publish foundational governance policies, lifecycle guidance, and phase-gate requirements
- Conduct stakeholder onboarding and leadership briefings
- Identify early pilot projects for governance process validation

Key Milestones: By Day 30, the organization has a functioning governance structure, initial training is complete, and foundational artifacts are in place to support pilot activation.

Days 31–90: Infrastructure, Templates, and Initial Controls

- Develop governance templates (SoA, MRP, Telemetry Specification, CRPR, AEP structure)
- Implement evidence management workflows and repository structure
- Define telemetry and data governance requirements
- Deliver functional training to governance roles
- Begin aligning pilot projects with governance expectations

Key Milestones: By Day 90, governance infrastructure and templates are operational, telemetry requirements are documented, and pilot projects are formally onboarded into governance processes.

Days 91–150: Pilot Activation and Governance Enforcement

- Conduct Phase Gate reviews for early pilot AI projects
- Capture evidence required for AEP population and lifecycle validation
- Produce the initial Cyber Resilience Posture Report (CRPR)
- Run early CCV trials and activate partial telemetry streams
- Refine governance processes based on pilot feedback

Key Milestones: By Day 150, CCV and telemetry operate in trial mode, governance processes have been validated with real systems, and evidence structures (AEP and CRPR) are proven functional.

Days 151–180: Demonstrated Governance Capability

- Produce the first fully populated AEP for a pilot system
- Conduct a formal governance review and leadership evaluation
- Update governance processes, templates, and training based on lessons learned
- Finalize the long-term roadmap for automation, resilience, and certification readiness

Key Milestones: By Day 180, governance roles, repositories, telemetry requirements, initial CCV, and resilience assessments are fully operational, enabling immediate transition into the sustainment cycle.

This period concludes with measurable improvements in governance maturity, evidence quality, and operational discipline.

6.5 Governance Metrics Dashboard

A governance metrics dashboard provides leadership with continuous visibility into governance performance, system trustworthiness, and operational risk posture. Metrics evolve based on maturity level, system criticality, and regulatory expectations.

Representative metrics include:

- Bias Rate: Measures fairness and disparity across protected attributes
- Drift Rate: Tracks data or model drift across operational cycles
- Control Effectiveness: Evaluates success of implemented controls and CCV checks
- Training Completion Rates: Indicates workforce readiness and competency
- Resilience Score: Summarizes adversarial robustness and dependency strength
- Telemetry Coverage: Shows monitoring completeness across pipelines and components

Dashboards support informed decision-making, early risk detection, and continuous improvement.

End Of Section

Section 7 – Governance Operations & Sustainment

7.1 Overview

This section defines how the organization sustains AI governance once the framework is operational. It establishes the ongoing cadence, workflows, and continuous improvement mechanisms necessary to maintain trustworthiness, compliance, and readiness for internal or external assessments. These sustainment practices ensure that AI systems remain aligned with mission needs, that risks are continuously evaluated and mitigated, and that governance activities operate as a stable, repeatable function across the enterprise. Through structured reviews, continuous monitoring, regular updates to governance artifacts, and CSRMC-aligned assurance activities, the organization evolves from initial implementation into a mature, continuously validated AI governance environment.

7.2 Governance Meeting Cadence

A structured governance cadence ensures consistent oversight, timely decision-making, and sustained alignment across all AI initiatives. The cadence follows a tiered structure that differentiates between operational reviews, governance reviews, and executive oversight. Operational meetings occur more frequently and focus on day-to-day system behavior, telemetry signals, incident trends, and CCV outputs. Governance reviews evaluate documentation completeness, risk posture, SoA updates, and evidence readiness. Executive reviews assess strategic alignment, approve risk acceptance requests, and evaluate program maturity progress. This multi-tiered cadence creates predictability and ensures that no AI system progresses or operates without continuous and disciplined oversight.

7.3 Continuous Monitoring Workflow

Continuous monitoring is the backbone of AI system sustainment. This workflow integrates telemetry streams, automated evidence updates, CCV cycles, resilience tests, and real-time analytics to ensure that the system remains trustworthy, stable, and aligned with mission and business requirements. Monitoring covers key dimensions including model drift, data drift, bias emergence, performance degradation, security anomalies, and dependency risks. Telemetry pipelines feed into governance dashboards for real-time visibility, while automated alerts trigger risk escalation pathways defined in the governance model. The workflow ensures that monitoring is not a one-time activity, but a continuous operational function integrated into MLOps and governance processes.

7.4 Framework Maintenance

The AI Governance Framework must evolve alongside organizational needs, regulatory changes, emerging threats, and technological advancements. Framework maintenance includes updating policies, templates, RACI assignments, phase-gate criteria, SoA content, and risk evaluation procedures. Maintenance also requires periodic review of external standards—ISO/IEC 42001, NIST AI RMF, NIST SP 800-53, CSRMC, EU AI Act—and incorporation of new requirements. The AI Governance Lead serves as the custodian of the framework and ensures that maintenance is performed consistently and documented according to ISO/IEC 42001 Clause 10.

7.5 Annual Management Review

An annual management review provides executive leadership with a comprehensive assessment of AI governance effectiveness. This review evaluates: governance performance against objectives, risk trends, audit findings, training completion, model performance stability, incidents, operational telemetry summaries, and improvement opportunities. Leaders assess whether governance resources remain sufficient, whether controls remain effective, and whether organizational priorities require adjustments to governance strategy. The review is documented and archived as part of the organization's compliance record and satisfies ISO/IEC 42001 Clause 9.3.

7.6 Awareness & Training

Ongoing awareness and training ensure that all stakeholders understand their responsibilities, governance expectations, and emerging AI risks. Training programs include mandatory onboarding for governance roles, recurring refresher sessions, targeted technical training for ML/MLOps teams, and awareness campaigns addressing ethical risks, security threats, and operational considerations. Training compliance is monitored as part of governance metrics and is included in annual management reviews. This reinforces the "competence and awareness" requirements of ISO/IEC 42001 Clauses 7.2 and 7.3.

7.7 Exception Handling

Exception handling establishes a formal process for documenting, reviewing, approving, and tracking deviations from governance requirements. Exceptions may include control waivers, unmitigated risks, incomplete evidence, or temporary operational workarounds. Each exception must be supported by a justification, evaluated for mission impact, reviewed by the AI Governance Lead, and approved by the Executive Sponsor if residual risk exceeds predefined thresholds. All exceptions are logged in the Risk Acceptance Register and reviewed during audits and management reviews.

7.8 CSRMC-Based Sustainment Activities

CSRMC modernization principles significantly enhance sustainment operations by introducing mission-driven, automated, and resilience-oriented risk governance. Sustainment includes continuous activation of CCV cycles, permanent telemetry-driven monitoring, ongoing updates to the Automated Evidence Package (AEP), routine updates to the Cyber Resilience Posture Report (CRPR), and periodic reassessment of mission-critical dependencies. These activities ensure that the AI system maintains continuous authorization posture, operational resilience, and a validated security baseline. CSRMC sustainment represents a shift from periodic review to real-time assurance.

7.9 Example 12-Month Implementation Roadmap

This roadmap illustrates a representative sustainment cycle once the AI Governance Framework is operational. It provides leadership with a clear view of how governance activities cycle throughout the year to maintain certification readiness, operational stability, and continuous improvement.

Months 1–3: Launch

During the launch phase, governance processes are activated across ongoing AI initiatives. CCV cycles begin, telemetry dashboards become operational, and teams complete required governance training. Early audits validate foundational compliance.

Months 4–6: Stabilize

Governance processes stabilize as documentation, evidence, and monitoring outputs become consistent. The Risk Register, SoA, and AEP undergo refinement based on real-world activity. Leadership receives the first quarterly risk and governance performance briefing.

Months 7–9: Integrate

Cross-functional integration deepens as governance, security, MLOps, data teams, and executive leadership align around continuous assurance principles. Internal audits are conducted, resilience measures are validated, and process improvements are applied.

Months 10–12: Certify

The organization demonstrates sustained governance maturity, consistency in evidence generation, and adherence to ISO/IEC 42001 and CSRMC expectations. Leadership validates readiness for external audits or customer assessments. A full management review closes the cycle, and lessons learned inform the next year’s roadmap.

End Of Section

The Decisions That Come Before Scale

For many organizations, artificial intelligence still feels distant. It appears as a feature toggle, a pilot project, or a conversation that keeps getting deferred in favor of more immediate priorities. There may be no formal AI program, no dedicated team, and no sense that anything urgent is happening at all.

That perception is understandable. Most organizations are not building large models or running advanced automation. What they are doing—often without realizing it—is standing at the point where decisions about AI will soon become unavoidable. The systems being evaluated today, the vendors being selected, and the use cases being explored will shape how AI enters the organization long before it feels widespread.

This is the moment that matters most.

The earliest choices about where AI is used, how it is framed, and who is responsible for it quietly establish patterns that persist. A pilot conducted without clear ownership becomes a precedent. A capability introduced as “just a tool” becomes embedded in workflows. A system adopted for convenience begins influencing decisions in ways that were never explicitly reviewed.

Legacy risk does not require scale to exist. It begins when systems are introduced without a shared understanding of their role, their limits, or their long-term implications. By the time AI feels ubiquitous, those early assumptions are already difficult to unwind.

Lifecycle ownership is not something that becomes necessary once AI is everywhere. It is what allows organizations to adopt AI deliberately, without drifting into complexity they did not choose. Treating AI as something that will eventually need governance often means governance arrives too late—after systems are already depended on, trusted implicitly, or woven into critical processes.

The purpose of a lifecycle approach is not to slow experimentation or demand certainty where none exists. It is to ensure that even small, early uses of AI remain visible, accountable, and revisitable. When systems are introduced with the expectation that they will be assessed, adjusted, and, if necessary, retired, organizations retain the ability to steer rather than react.

For leaders and practitioners encountering AI now—at the edges rather than the core—this is an opportunity rather than a burden. It is a chance to establish clarity before complexity, and ownership before scale. Decisions made at this stage are easier to explain, easier to correct, and far less costly than those made after reliance has set in.

The legacy of AI within an organization is not determined by how advanced the technology becomes, but by how intentionally it is introduced. Systems that begin with clear purpose and defined accountability tend to evolve in manageable ways. Systems that begin informally tend to accumulate risk quietly, until they demand attention under pressure.

This framework exists for those who are early enough to choose differently.

AI will not arrive all at once. It will appear gradually, through opportunities that seem reasonable in isolation. Whether those moments add up to a capability the organization controls—or one it must later disentangle—depends on the discipline applied from the start.

The question is not whether AI will become part of the organization's future. It is whether that future is shaped deliberately, or inherited without design.

End Of Section

Appendix A – Full RACI Matrix

This RACI Matrix has been rebuilt to align directly with the intent of Section 4 of the guide—meaning it supports ISO/IEC 42001 Clause 5 (Leadership), Clauses 7.2–7.3 (Competence & Awareness), NIST AI RMF Govern functions, and the mission-focused decision authority expectations of the DoD CSRMC.

Role Groupings

The following roles correspond directly to Section 4 role descriptions. These are governance functions, not job titles, and can be combined or scaled depending on organizational size.

- Executive Sponsor (ES) – Ultimate authority for mission alignment and risk acceptance.
- AI Governance Lead (GL) – Oversees governance framework and system-wide lifecycle conformance.
- Program Manager (PgM) – Manages lifecycle execution, timelines, deliverables, and cross-functional coordination.
- Data Lead (DL) – Ensures data suitability, provenance, quality, and governance compliance.
- ML/AI Engineer (MLE) – Develops, documents, and evaluates models.
- MLOps / Platform Engineer (MLOps) – Owns deployment, monitoring, telemetry, automation, and CCV.
- Security Officer (SecO) – Ensures cybersecurity, privacy, and adversarial resilience controls.
- Risk Officer (RO) – Manages risk register, residual risk evaluations, and MRP alignment.
- Privacy Officer (PO) – Ensures compliance with privacy requirements and PIAs.
- Ethics Officer (EO) – Oversees fairness, transparency, explainability, and responsible AI.
- Compliance Officer (CO) – Ensures adherence to ISO/IEC 42001, NIST AI RMF, and audit readiness.
- Internal Audit (IA) – Independently validates governance effectiveness.
- Supplier/Vendor Manager (SVM) – Oversees external AI suppliers and inherited controls.

CPMAI Lifecycle RACI Matrix

Each table maps lifecycle responsibilities to the appropriate governance functions, making responsibilities transparent and auditable.

Phase I – Business Understanding

Activity	ES	GL	PgM	DL	MLE	MLOps	SecO	RO	PO	EO	CO	IA	SVM
Define business problem & mission alignment	A	C	R	C	I	I	I	C	I	C	I	I	I
Establish governance boundaries & scope	A	R	R	C	I	I	C	C	I	C	C	I	I
Identify stakeholders & decision authorities	A	R	R	I	I	I	I	C	I	C	C	I	I
Initial risk assessment & MRP impact	I	C	R	C	C	I	C	A	I	C	C	I	I
Develop Responsible AI objectives	A	R	R	C	I	I	C	C	C	A	C	I	I
Initial Statement of Applicability (SoA v1)	I	A	C	I	I	I	C	R	I	C	C	I	I
Business case, value hypothesis & success metrics	A	C	R	C	C	I	I	C	I	C	C	I	I

Phase II – Data Understanding

Activity	ES	GL	PgM	DL	MLE	MLOps	SecO	RO	PO	EO	CO	IA	SVM
Data source identification & inventory	I	C	R	A	C	I	C	I	C	I	I	I	R
Data profiling & quality assessment	I	C	C	A	R	I	C	I	I	C	I	I	I
Bias & representativeness assessment	I	C	C	C	A	I	C	I	I	R	I	I	I
Privacy & data protection review	I	C	C	C	I	I	C	I	A	I	C	I	I
Security review of data access & lineage	I	I	C	R	I	I	A	C	I	I	I	I	C
Update risk register (data risks)	I	C	R	C	C	I	C	A	C	C	C	I	I
Update SoA (data controls)	I	C	C	I	I	I	C	R	C	C	A	I	I

Phase III – Data Preparation

Activity	ES	GL	PgM	DL	MLE	MLOps	SecO	RO	PO	EO	CO	IA	SVM
Data cleaning, transformation, & labeling	I	I	C	A	R	C	C	I	C	C	I	I	I
Data privacy enhancements (minimization, de-ID)	I	C	C	A	C	I	R	C	A	C	I	I	I
Data versioning & lineage tracking	I	I	C	A	C	R	C	I	I	I	I	I	I
Update risk register (data prep risks)	I	C	R	C	C	I	C	A	C	C	C	I	I
Update SoA	I	C	C	I	I	I	C	R	C	C	A	I	I
Data pipeline specification & documentation	I	C	R	A	C	C	C	C	C	C	I	I	I

Phase IV – Model Development

Activity	ES	GL	PgM	DL	MLE	MLOps	SecO	RO	PO	EO	CO	IA	SVM
Model design & selection	I	C	C	C	A	C	I	C	I	C	I	I	I
Threat modeling & adversarial analysis	I	C	C	I	R	C	A	C	I	C	I	I	I
Robustness, stress & adversarial testing	I	I	C	I	A	R	R	C	I	I	I	I	I
Explainability & transparency design	I	C	C	I	A	I	I	C	I	A	I	I	I
Model experiments, logs & lineage	I	C	C	I	A	R	C	I	I	I	I	I	I
Update risk register (model risks)	I	C	R	C	C	I	C	A	C	C	C	I	I
Update SoA	I	C	C	I	I	I	C	R	C	C	A	I	I
Draft Model Card	I	C	C	I	A	I	C	C	C	A	C	I	I

Phase V – Model Evaluation

Activity	ES	GL	PgM	DL	MLE	MLOps	SecO	RO	PO	EO	CO	IA	SVM
Define independent evaluation criteria	I	A	R	C	C	I	C	C	C	C	C	I	I
Conduct independent evaluation	I	C	C	I	R	I	C	C	I	C	C	A	I
Robustness, fairness & reliability evaluation	I	I	C	I	A	I	C	C	I	R	I	I	I
Residual risk documentation & acceptance	A	C	R	I	I	I	C	A	C	C	C	I	I
Update Model Card (Release Candidate)	I	C	C	I	A	I	C	C	C	A	I	I	I
Evaluation Report	I	C	R	I	A	I	C	C	I	C	C	I	I
Go/No-Go decision	A	R	R	I	C	I	C	C	I	C	C	I	I

Phase VI – Operationalization

Activity	ES	GL	PgM	DL	MLE	MLOps	SecO	RO	PO	EO	CO	IA	SVM
Deployment readiness validation	I	A	R	C	C	C	C	C	I	I	C	I	I
Monitoring & telemetry activation	I	I	C	I	I	A	C	I	I	I	I	I	I
CCV automation configuration	I	I	C	I	I	A	C	C	I	I	C	I	I
AEP automation configuration	I	I	C	I	I	A	I	I	I	I	C	I	I
Operational risk updates	I	C	R	I	I	C	C	A	C	C	C	I	I
Resilience & failover testing	I	I	C	I	I	A	R	C	I	I	I	I	I
Update Model Card (Release Version)	I	C	C	I	A	I	C	C	C	A	I	I	I
Post-deployment review	I	A	R	C	C	C	C	C	C	C	C	I	I
Continuous governance reporting	I	A	R	I	I	C	C	C	I	I	C	I	I

End Of Section

Appendix B – Phase Gate Review Templates

Introduction

Appendix A provides the complete set of Phase Gate Review Templates used to ensure disciplined, traceable, and auditable progression through each CPMAI lifecycle phase. These gates are a core part of the AI Governance Framework, serving as formal control points where project teams must demonstrate readiness to proceed and leadership must validate compliance, completeness, and alignment with organizational governance standards.

Each gate consolidates the required deliverables, evidence, and decision criteria for its respective phase, supporting:

- Quality assurance by preventing incomplete or non-compliant work from advancing
- Risk management by identifying issues early and enforcing corrective actions
- Governance accountability through documented leadership review and sign-off
- Certification alignment with ISO/IEC 42001, NIST AI RMF, DoD CSRMC, and related frameworks
- Audit readiness via structured, repeatable evidence capture

Every Gate Review Template includes the following standardized sections:

- Project and Phase Information – Metadata for traceability across the lifecycle.
- Purpose of the Gate – Defines what the gate is validating.
- Required Deliverables & Evidence Checklist – Phase-specific mandatory artifacts.
- Acceptance Criteria – Minimum requirements for approval.
- Findings & Required Corrective Actions – Issues, gaps, and assignments.
- Residual Risks / Deviations Accepted – Documented exceptions or outstanding risks.
- Decision & Leadership Sign-Off – Approval, conditional approval, or rejection.
- Archival Instructions – Repository location and evidence indexing requirements

The following pages provide one Gate Review Template for each CPMAI lifecycle phase, plus a Gate Register Summary Sheet for tracking approvals across the entire AI project or program.

Gate 1 – Business Understanding Review

The following template is used to validate that all Business Understanding phase activities have been completed in accordance with organizational governance, risk, and compliance expectations.

Section	Details
Project & Phase Information	Project Name: Project ID: Date of Review: Phase: CPMAI Phase I – Business Understanding Review Type: Initial / Follow-up / Final
Purpose of the Gate	To confirm that the project's business objectives, mission alignment, stakeholders, governance requirements, risk criteria, and success measures are fully defined and documented. This gate ensures the project is positioned for compliant, mission-aligned execution before entering Phase II.
Required Deliverables & Evidence Checklist	▫ Business Case / Value Proposition ▫ Governance Scope Statement ▫ Stakeholder Register ▫ AI Use Case Definition (including assumptions & constraints) ▫ Mission Alignment Summary (if applicable) ▫ Initial Risk Criteria & Risk Appetite ▫ Initial Statement of Applicability (SoA v1) ▫ Ethical & Responsible AI Considerations ▫ Success Metrics (KPIs / mission outcomes) ▫ Phase I Documentation Archive Completed
Acceptance Criteria	• Business need and mission alignment are clearly defined. • Stakeholders are documented with roles and decision authority. • Governance scope aligns with organizational AI governance policies. • Risk criteria are defined and approved. • Initial SoA (v1) completed and stored in repository. • Success metrics are measurable and traceable. • No open critical gaps preventing transition into data-focused work.
Findings & Required Corrective Actions	Finding 1: Corrective Action: Finding 2: Corrective Action: Finding 3: Corrective Action:
Residual Risks / Deviations Accepted	Risk / Deviation: Justification for Acceptance: Approved By:
Decision & Leadership Sign-Off	Decision: Approved / Conditionally Approved / Not Approved Reviewer Name & Title: Signature / Digital Approval: Date:
Archival Instructions	All Gate 1 materials shall be stored in the AI Governance Repository using the following structure: /Governance/Phase_Gates/Gate1_BusinessUnderstanding/<ProjectName>/<YYYY-MM-DD>/

Gate 2 – Data Understanding Review

The following template is used to validate that all Data Understanding phase activities have been completed in accordance with organizational governance, data management requirements, and AI system assurance expectations.

Section	Details
Project & Phase Information	Project Name: Project ID: Date of Review: Phase: CPMAI Phase II – Data Understanding Review Type: Initial / Follow-up / Final
Purpose of the Gate	To confirm that all data sources, data characteristics, data risks, privacy constraints, and legal/ethical considerations have been thoroughly analyzed and documented. This gate ensures that the project team fully understands the data landscape before entering Phase III data preparation activities.
Required Deliverables & Evidence Checklist	▫ Data Inventory & Source Register ▫ Data Profiling Report ▫ Data Quality Assessment ▫ Data Sensitivity & Privacy Analysis (PII, PHI, CUI, etc.) ▫ Data Provenance & Lineage Summary ▫ Data Access & Ownership Documentation ▫ Dataset Representativeness & Bias Scan (initial) ▫ Data Governance Constraints & Compliance Requirements ▫ Dataset Acceptance & Readiness Checklist ▫ Phase II Documentation Archive Completed
Acceptance Criteria	• All data sources required for the AI use case are identified and cataloged. • Data provenance, lineage, and transformations are documented. • Privacy and sensitivity assessments (including CUI/PII/PHI if applicable) are completed. • Data quality issues and gaps are documented with planned remediation actions. • Initial bias and representativeness risks have been evaluated. • Data owners, stewards, and access roles are clearly defined. • No critical data uncertainties exist that would prevent preparation or transformation work.
Findings & Required Corrective Actions	Finding 1: Corrective Action: Finding 2: Corrective Action: Finding 3: Corrective Action:
Residual Risks / Deviations Accepted	Risk / Deviation: Justification for Acceptance: Approved By:
Decision & Leadership Sign-Off	Decision: Approved / Conditionally Approved / Not Approved Reviewer Name & Title: Signature / Digital Approval: Date:
Archival Instructions	All Gate 2 materials shall be stored in the AI Governance Repository using the following structure: /Governance/Phase_Gates/Gate2_DataUnderstanding/<ProjectName>/<YYYY-MM-DD>/

Gate 3 – Data Preparation Review

The following template is used to validate that all Data Preparation phase activities have been completed in alignment with organizational governance, data engineering standards, data protection requirements, and AI assurance expectations.

Section	Details
Project & Phase Information	Project Name: Project ID: Date of Review: Phase: CPMAI Phase III – Data Preparation Review Type: Initial / Follow-up / Final
Purpose of the Gate	To confirm that datasets have been properly prepared, transformed, cleaned, documented, protected, and versioned for use in AI model development. This gate ensures data readiness, compliance with data governance requirements, and the integrity and reproducibility of all dataset preparation activities.
Required Deliverables & Evidence Checklist	▫ Data Cleaning & Transformation Summary ▫ Dataset Versioning & Lineage Records ▫ Data Labeling Guidelines (if applicable) ▫ Data Pipeline Specification ▫ Data Quality Validation Reports ▫ Privacy-Preserving Transformation Documentation ▫ Access Control & Dataset Security Validation ▫ Dataset Reproducibility Verification ▫ Dataset Acceptance for Model Development (signed) ▫ Phase III Documentation Archive Completed
Acceptance Criteria	• All datasets required for model development are fully cleaned, transformed, and validated. • Data lineage and versioning metadata are complete and traceable. • Data labeling processes adhere to documented standards. • Dataset quality meets acceptance thresholds defined in Phase II. • Privacy-preserving methods (masking, minimization, etc.) are correctly applied and documented. • Dataset access is properly controlled and logged. • Data pipelines are stable, documented, and reproducible. • No unresolved data issues exist that would compromise model development.
Findings & Required Corrective Actions	Finding 1: Corrective Action: Finding 2: Corrective Action: Finding 3: Corrective Action:
Residual Risks / Deviations Accepted	Risk / Deviation: Justification for Acceptance: Approved By:
Decision & Leadership Sign-Off	Decision: Approved / Conditionally Approved / Not Approved Reviewer Name & Title: Signature / Digital Approval: Date:
Archival Instructions	All Gate 3 materials shall be stored in the AI Governance Repository using the following structure: /Governance/Phase_Gates/Gate3_DataPreparation/<ProjectName>/<YYYY-MM-DD>/

Gate 4 – Model Development Review

The following template is used to validate that all Model Development phase activities have been completed in accordance with organizational governance, secure engineering practices, AI assurance requirements, and documentation standards.

Section	Details
Project & Phase Information	Project Name: Project ID: Date of Review: Phase: CPMAI Phase IV – Model Development Review Type: Initial / Follow-up / Final
Purpose of the Gate	To confirm that model development activities—including feature engineering, training, experimentation, documentation, robustness testing, fairness analysis, security review, and explainability development—have been thoroughly executed and recorded. This gate verifies that the model meets established development standards and is ready to proceed to formal evaluation.
Required Deliverables & Evidence Checklist	▫ Model Development Plan ▫ Feature Engineering Summary ▫ Experimentation Logs & Versioning Records ▫ Model Architecture & Configuration Documentation ▫ Training Dataset Version Reference ▫ Model Performance Benchmark Results ▫ Bias, Fairness & Representativeness Assessment ▫ Robustness & Security Testing Results ▫ Explainability & Transparency Documentation (XAI Plan) ▫ Human Oversight Requirements & Design Integration ▫ Updated Model Card (Draft) ▫ Phase IV Documentation Archive Completed
Acceptance Criteria	• Model development followed documented and approved processes. • Experimentation is fully logged, reproducible, and version-controlled. • Model achieves performance criteria defined in Phase I. • Fairness, representativeness, and bias risks have been analyzed and mitigated. • Robustness and security testing demonstrate resilience against adversarial, edge, and failure scenarios. • Explainability and transparency requirements are met and documented. • Human oversight requirements are integrated and validated. • Model Card draft is complete and accurate. • No development issues remain that would block independent evaluation.
Findings & Required Corrective Actions	Finding 1: Corrective Action: Finding 2: Corrective Action: Finding 3: Corrective Action:
Residual Risks / Deviations Accepted	Risk / Deviation: Justification for Acceptance: Approved By:
Decision & Leadership Sign-Off	Decision: Approved / Conditionally Approved / Not Approved Reviewer Name & Title: Signature / Digital Approval: Date:
Archival Instructions	All Gate 4 materials shall be stored in the AI Governance Repository using the following structure: /Governance/Phase_Gates/Gate4_ModelDevelopment/<ProjectName>/<YYYY-MM-DD>/

Gate 5 – Model Evaluation Review

The following template is used to validate that all Model Evaluation phase activities have been completed in accordance with organizational governance, AI assurance requirements, independent evaluation standards, risk documentation expectations, and deployment readiness criteria.

Section	Details
Project & Phase Information	Project Name: Project ID: Date of Review: Phase: CPMAI Phase V – Model Evaluation Review Type: Initial / Follow-up / Final
Purpose of the Gate	To confirm that the model has been independently evaluated for performance, fairness, robustness, explainability, uncertainty, safety, and mission or business readiness. This gate ensures that risks, limitations, and dependencies are fully understood, documented, and acceptable prior to deployment.
Required Deliverables & Evidence Checklist	▫ Formal Evaluation Plan (approved) ▫ Independent Evaluation Report ▫ Final Performance Validation Results ▫ Bias, Fairness & Representativeness Evaluation ▫ Robustness, Stress, & Adversarial Testing Results ▫ Explainability & Transparency Validation (XAI Outputs) ▫ Residual Risk Assessment & Updated Risk Register Entries ▫ Updated Model Card (Final or Release Candidate) ▫ Uncertainty & Limitations Documentation ▫ Go/No-Go Recommendation Memo ▫ Phase V Documentation Archive Completed
Acceptance Criteria	• Independent evaluation is complete and properly documented. • Model meets or exceeds performance thresholds defined in Phase I. • Bias, fairness, and representativeness testing confirm acceptable risk posture. • Robustness and adversarial testing show no unresolved critical vulnerabilities. • Explainability requirements are met for all intended users and stakeholders. • Residual risks are documented with clear justification for acceptance. • Model Card is complete, accurate, and ready for operational review. • Go/No-Go recommendation is well-supported by evidence. • No critical issues remain that would prevent operational deployment.
Findings & Required Corrective Actions	Finding 1: Corrective Action: Finding 2: Corrective Action: Finding 3: Corrective Action:
Residual Risks / Deviations Accepted	Risk / Deviation: Justification for Acceptance: Approved By:
Decision & Leadership Sign-Off	Decision: Approved / Conditionally Approved / Not Approved Reviewer Name & Title: Signature / Digital Approval: Date:
Archival Instructions	All Gate 5 materials shall be stored in the AI Governance Repository using the following structure: /Governance/Phase_Gates/Gate5_ModelEvaluation/<ProjectName>/<YYYY-MM-DD>/

Gate 6 – Operationalization Review

The following template is used to validate that all Operationalization phase activities have been completed in alignment with organizational governance, monitoring and telemetry requirements, AI assurance expectations, CSRMC-aligned continuous validation practices, and long-term lifecycle oversight.

Section	Details
Project & Phase Information	Project Name: Project ID: Date of Review: Phase: CPMAI Phase VI – Operationalization Review Type: Initial / Follow-up / Final
Purpose of the Gate	To confirm that all operational readiness activities—including deployment preparation, monitoring activation, drift detection setup, incident response readiness, CCV integration, governance documentation, resilience validation, and lifecycle management processes—are complete. This gate ensures that the AI system is safe, secure, reliable, continuously monitored, and fully prepared for production deployment and sustainment.
Required Deliverables & Evidence Checklist	▫ Deployment Readiness Checklist ▫ AI System Runbook (Operations, Escalation, Failover) ▫ AI Monitoring & Drift Management Plan ▫ Telemetry Specification & Dashboard Activation Proof ▫ Continuous Compliance Validation (CCV) Configuration ▫ Cyber Resilience Posture Report (CRPR) ▫ Incident Response Plan (AI-Specific) ▫ Operational Access & Role Authorization Review ▫ Material Change Evaluation Procedure (activated) ▫ Model Card (Release Version) ▫ Post-Deployment Review Schedule ▫ Phase VI Documentation Archive Completed
Acceptance Criteria	• Deployment configuration and operational controls are complete and validated. • Monitoring, telemetry, and drift detection mechanisms are active and functional. • CCV cycles are configured and scheduled with validated evidence sources. • Incident response procedures are documented, tested, and aligned with enterprise requirements. • Resilience and failover behaviors meet mission or business continuity thresholds. • Role-based access and operational authority are fully established. • Release Model Card is complete and archived. • Post-deployment review cadence is defined and approved. • No open operational risks exist that would prevent safe deployment.
Findings & Required Corrective Actions	Finding 1: Corrective Action: Finding 2: Corrective Action: Finding 3: Corrective Action:
Residual Risks / Deviations Accepted	Risk / Deviation: Justification for Acceptance: Approved By:
Decision & Leadership Sign-Off	Decision: Approved / Conditionally Approved / Not Approved Reviewer Name & Title: Signature / Digital Approval: Date:
Archival Instructions	All Gate 6 materials shall be stored in the AI Governance Repository using the following structure: /Governance/Phase_Gates/Gate6_Operationalization/<ProjectName>/<YYYY-MM-DD>/

Gate Register Summary Sheet

The Gate Register provides a consolidated log of all Phase Gate reviews conducted across the AI project lifecycle. It offers leadership and auditors a single reference point for verifying approvals, dates, corrective actions, and repository locations.

Gate	Phase	Date Reviewed	Decision	Reviewer(s)	Corrective Actions Required	Completion Date	Repository Location
Gate 1	Business Understanding		Approved / Conditional / Not Approved				/Governance/Phase_Gates/Gate1_BusinessUnderstanding/
Gate 2	Data Understanding		Approved / Conditional / Not Approved				/Governance/Phase_Gates/Gate2_DataUnderstanding/
Gate 3	Data Preparation		Approved / Conditional / Not Approved				/Governance/Phase_Gates/Gate3_DataPreparation/
Gate 4	Model Development		Approved / Conditional / Not Approved				/Governance/Phase_Gates/Gate4_ModelDevelopment/
Gate 5	Model Evaluation		Approved / Conditional / Not Approved				/Governance/Phase_Gates/Gate5_ModelEvaluation/
Gate 6	Operationalization		Approved / Conditional / Not Approved				/Governance/Phase_Gates/Gate6_Operationalization/

End of Section

Appendix C – Crosswalk Matrices

This appendix consolidates all crosswalks necessary to demonstrate how the AI Governance Framework aligns with leading standards and federal modernization constructs. These matrices support audit readiness, traceability, control inheritance, and certification preparation by showing how lifecycle tasks map to required governance domains.

The following crosswalks will be included in this appendix:

- Visual Crosswalk Chart
- CSRMC Modernization Elements Reference
- CPMAI → ISO/IEC 42001
- CPMAI → NIST AI RMF
- ISO/IEC 42001 → NIST AI RMF
- CPMAI → NIST 800-53 Rev 5
- CPMAI → CSRMC
- ISO/IEC 42001 → CSRMC
- NIST AI RMF → CSRMC
- 800-53 Critical Controls → CSRMC
- ISO/IEC 42001 Clause Reference Index summarizing clause purpose and section linkage

Visual Crosswalk Chart

The chart below provides a single consolidated visualization showing how all major frameworks align across the AI lifecycle and governance requirements. This serves as the master reference for how CPMAI, ISO/IEC 42001, NIST AI RMF, NIST SP 800-53, and CSRMC interlock.

Lifecycle / Governance Area	CPMAI	ISO/IEC 42001	NIST AI RMF	NIST SP 800-53 (Key Controls)	CSRMC Modernization Elements
Mission & Business Alignment	Phase I – Business Understanding	Clause 4 (Context), Clause 5 (Leadership)	Govern	PM family, PL family, RA-1–RA-3	Mission-Driven Risk (MRP)
Risk Planning & Policy Formation	Phase I	Clause 6 (Planning), Annex A.4	Govern	RA, PL, PM	MRP, Survivability / Resilience
Data Requirements & Sensitivity Analysis	Phase II – Data Understanding	Clause 8.2, Annex A.5–A.7	Map	RA-8, PT-2, IP series	Visibility & Telemetry
Data Preparation & Controls	Phase III – Data Preparation	Clause 8.3, Annex A.5–A.7	Measure	SC-28, SC-8, AU-9, MP-2	Automation & AEP
Model Development & Documentation	Phase IV – Model Development	Clause 8.4, Annex A.11–A.13	Measure	SA-3, SA-8, SA-15, SI-6	Survivability / Resilience
Model Evaluation & Verification	Phase V – Model Evaluation	Clause 8.5, Annex A.14–A.15	Measure	CA-2, CA-5, RA-5	CCV, Resilience
Deployment & Operational Readiness	Phase VI – Operationalization	Clause 8.6	Manage	SI-4, AU-6, SC-5, SC-6	Visibility & Telemetry, CCV
Monitoring & Drift Detection	Phase VI	Clause 8.7, Annex A.16	Manage	SI-4, AU-6	CCV, Automation & AEP
Incident Management	Phase VI	Clause 8.8, Annex A.17	Manage	IR-4, IR-5, IR-6	Survivability / Resilience
Decommissioning & Lifecycle Closeout	Phase VI	Clause 8.9	Manage	MP-6, RA-5	Reciprocity & Inheritance
Continuous Improvement & Assurance	Continuous Activity	Clause 10, Annex A.18	Govern / Manage	CA-7, PM-6	CCV, Automation, Resilience
Governance Documentation & Recordkeeping	All Phases	Clause 7.5	Govern	AU-9, PL-2	Automation & AEP

CSRMC Modernization Elements Reference

To avoid repetition across multiple crosswalk tables, this guide uses a standardized interpretation of the CSRMC modernization elements. These elements serve as the basis for mapping CPMAI, ISO/IEC 42001, NIST AI RMF, and NIST SP 800-53 Rev. 5 controls to CSRMC's mission-centric and automation-enabled risk management model.

CSRMC Modernization Element	Purpose / Summary	Key Governance Themes
Mission-Driven Risk (MRP)	Aligns cybersecurity and AI assurance to mission outcomes, enabling Mission Risk Profiles and prioritization of controls and impacts based on mission criticality.	Mission alignment; critical functions; mission dependencies; risk prioritization; operational impact.
Automation & AEP	Enables automation of governance processes, automated evidence generation, and machine-readable control logic for faster assurance and reduced manual overhead.	Automated Evidence Packages; governance automation; continuous evidence generation; policy-as-code.
Continuous Compliance Validation (CCV)	Provides ongoing automated testing and verification of control effectiveness, ensuring systems remain continuously compliant and audit-ready.	Continuous control testing; automated validation; readiness assessment; ongoing assurance.
Survivability / Resilience	Ensures AI systems retain operational capability under adversarial conditions, failures, or degradation, supporting mission continuity.	Adversarial robustness; fail-over behavior; continuity; operational durability.
Reciprocity & Inheritance	Facilitates reuse of validated controls, shared services, and inherited evidence to reduce redundant assessment activities and accelerate accreditation.	Evidence reuse; shared platforms; inherited controls; common services; cross-system efficiency.
Visibility & Telemetry	Provides real-time observability, monitoring, drift detection, and analytics to support situational awareness and continuous assurance.	Telemetry; monitoring; observability; analytics; logging; drift detection.

CPMAI → ISO/IEC 42001

The following crosswalk maps each CPMAI phase to the corresponding ISO/IEC 42001:2023 Clauses and Annex A control families.

CPMAI Phase	Key Activities	ISO/IEC 42001 Clause Alignment	Annex A Control Alignment
Phase I – Business Understanding	Define business objectives, scope, stakeholders, value proposition, governance requirements, risk criteria	• Clause 4 – Context of the Organization (4.1–4.3) • Clause 5 – Leadership (5.1–5.3) • Clause 6 – Planning (6.1–6.3)	• A.2 Governance & Accountability • A.3 Risk Assessment • A.4 Responsible AI Policy
Phase II – Data Understanding	Data inventory, data profiling, privacy constraints, representativeness, suitability assessment	• Clause 8 – Operation (8.2 Data-related requirements) • Clause 9 – Performance Evaluation (9.1 Monitoring and measurement)	• A.5 Data Quality & Integrity • A.6 Dataset Documentation • A.9 Traceability & Transparency
Phase III – Data Preparation	Cleaning, transformation, labeling, lineage, reproducibility, dataset versioning, data pipeline readiness	• Clause 8 – Operation (8.3 Technical requirements for dataset creation & preparation)	• A.5 Data Quality • A.7 Dataset Governance • A.10 Records & Documentation
Phase IV – Model Development	Experimentation, feature engineering, model training, robustness testing, fairness assessment, explainability planning	• Clause 8 – Operation (8.4 AI system development requirements) • Clause 7 – Support (7.1–7.5 Documentation & Competence)	• A.11 AI System Design & Development • A.12 Robustness & Security • A.13 Explainability & Transparency
Phase V – Model Evaluation	Validation, independent review, bias assessment, robustness verification, uncertainty reporting, documentation of limitations	• Clause 8 – Operation (8.5 AI system evaluation requirements) • Clause 9 – Performance Evaluation	• A.14 Model Evaluation & Testing • A.15 Human Oversight Requirements
Phase VI – Operationalization	Deployment, monitoring, telemetry, incident management, post-deployment review, change management, decommissioning	• Clause 8 – Operation – 8.6 Deployment requirements – 8.7 Monitoring – 8.8 Incident Management – 8.9 Decommissioning • Clause 10 – Improvement	• A.16 Monitoring & Drift Management • A.17 Incident Response • A.18 Continuous Improvement

CPMAI → NIST AI RMF

The following crosswalk maps each CPMAI phase to the corresponding NIST AI Risk Management Framework (AI RMF) Core Functions: Govern, Map, Measure, and Manage.

CPMAI Phase	Key Activities	Aligned NIST AI RMF Functions	Supporting Notes
Phase I – Business Understanding	Define business objectives, success criteria, governance scope, stakeholder roles, risk posture, and intended AI use case	Govern – Establish governance structure, policies, accountability Map – Identify context, goals, impacts, and intended use	Establishes the foundation for governance expectations, risk criteria, and organizational alignment. Aligns with Govern: Organizational Governance (GOV 1.1–1.7).
Phase II – Data Understanding	Inventory data sources, evaluate quality, assess bias risks, analyze legal and ethical constraints, evaluate representativeness	Map – Characterize data, risks, and system context Measure – Identify data quality, bias, and gaps	Directly aligns with MAP 2.x tasks, including data assessment and risk identification; supports MEASURE 3.1–3.3 for data quality and bias analysis.
Phase III – Data Preparation	Clean, transform, label, engineer features, establish lineage, version datasets, ensure reproducibility	Measure – Evaluate data quality, integrity, statistical attributes Manage – Implement controls to ensure trustworthy data lifecycle	Supports MEASURE tasks for validating dataset quality and MANAGE tasks related to control execution and risk mitigation across data pipelines.
Phase IV – Model Development	Train models, log experiments, evaluate robustness, analyze fairness, develop explainability, document assumptions	Measure – Assess model performance, robustness, fairness, explainability Manage – Apply controls to reduce risks during development	Aligns with MEASURE 3.x (model evaluations, robustness assessments) and MANAGE 4.1–4.4 (risk mitigation, documentation, control implementation).
Phase V – Model Evaluation	Conduct independent evaluations, validate uncertainty, test for biases, verify limitations, update model card	Measure – Verify trustworthiness characteristics Govern – Confirm readiness for deployment decisions	Evaluations map to MEASURE tasks for validation and verification; GO/NO-GO alignment supports GOVERN decision-making (GOV 1.5).
Phase VI – Operationalization	Deploy model, monitor performance and drift, respond to incidents, execute CCV cycles, perform periodic reviews	Manage – Monitor system performance, mitigate emerging risks Govern – Maintain accountability, continuous oversight	Aligns with MANAGE 4.x on operational risk mitigation and GOVERN 1.6–1.7 on ensuring ongoing accountability and lifecycle governance.

ISO/IEC 42001 → NIST AI RMF

The following crosswalk maps ISO/IEC 42001:2023 Clauses and Annex A control families to the corresponding NIST AI Risk Management Framework (AI RMF) Core Functions: Govern, Map, Measure, and Manage.

ISO/IEC 42001 Clause / Annex A Control	Purpose / Requirement Summary	Aligned NIST AI RMF Functions	Supporting Notes
Clause 4 – Context of the Organization (4.1 Understanding the organization, 4.2 Needs & expectations, 4.3 AI Management System scope)	Establishes organizational context, stakeholders, scope, and dependencies for AI system governance	Govern – Organizational governance, roles, and accountability Map – Establish use case purpose, context, and risk environment	Aligns with GOV 1.1–1.7 for defining governance structure and MAP 1.x for establishing domain context and stakeholder needs.
Clause 5 – Leadership (5.1 Leadership & commitment, 5.2 Policy, 5.3 Organizational roles)	Requires leadership sponsorship, AI policy creation, and defined responsibilities	Govern – Governance policies, accountability, role authority	Direct alignment with GOV 1.x—leadership support, policy establishment, and accountability structure.
Clause 6 – Planning (6.1 Risk & opportunity planning, 6.2 Objectives, 6.3 Planning changes)	Establishes risk planning, objectives, and change management expectations	Govern – Governance risk planning Map – Identify risks and impacts	Aligns with MAP 2.x for identifying AI risks and GOVERN tasks for continuous policy and objective management.
Clause 7 – Support (7.1 Resources, 7.2 Competence, 7.3 Awareness, 7.5 Documented Information)	Provides requirements for competence, training, documentation, and resources	Govern – Role competence, policy adherence Manage – Documentation management & operational readiness	Aligns with GOVERN (competence & awareness) and MANAGE 4.x for documentation, recordkeeping, and training.
Clause 8 – Operation (8.2 Data requirements, 8.3 Dataset creation, 8.4 Development, 8.5 Evaluation, 8.6 Deployment, 8.7 Monitoring, 8.8 Incident management, 8.9 Decommissioning)	Defines operational requirements for full AI lifecycle including data, model development, evaluation, deployment, monitoring, and incident management	Map – Data provenance, data quality, context mapping Measure – Trustworthiness assessments & evaluation Manage – Deployment, monitoring, incident response	This Clause maps across MAP (data & system context), MEASURE (evaluation, robustness testing), and MANAGE (operations, incident response, drift handling).
Clause 9 – Performance Evaluation (Monitoring, measurement, internal audits, management review)	Requires evaluation of system performance, audits of governance controls, and management assessment	Govern – Accountability & oversight Manage – Continuous performance monitoring	Aligns strongly with GOVERN oversight tasks and MANAGE 4.x for operational monitoring and audit-driven improvements.
Clause 10 – Improvement (Nonconformity, corrective action, continual improvement)	Ensures continuous improvement of AI governance and operational controls	Manage – Risk mitigation, corrective action, lifecycle improvements	Aligns with MANAGE 4.4 (continuous improvement, risk mitigation, corrective action).
Annex A – A.2 Governance & Accountability	Defines governance structure, roles, policy requirements	Govern	Direct mapping to GOVERN governance structure requirements.
Annex A – A.3 Risk Assessment	Requires structured AI risk assessment and documentation	Map – Risk identification Measure – Risk evaluation	Aligns with MAP (risk identification) and MEASURE (risk evaluation).
Annex A – A.4 Responsible AI Policy	Defines responsible AI principles, commitments, and policy	Govern	Aligns with GOVERN policy establishment and oversight.
Annex A – A.5 Data Quality Requirements	Ensures data relevance, representativeness, integrity	Map – Data characterization Measure – Data quality evaluation	Matches MAP 2.x and MEASURE 3.x (data quality, bias analysis).
Annex A – A.6 Dataset Documentation	Requires dataset metadata, lineage, and documentation	Map – Data understanding Measure – Validation of dataset attributes	Supports MAP documentation requirements and MEASURE validation workflows.

ISO/IEC 42001 Clause / Annex A Control	Purpose / Requirement Summary	Aligned NIST AI RMF Functions	Supporting Notes
Annex A — A.7 Dataset Governance	Dataset controls for security, access, retention	Manage	Aligns with MANAGE 4.x for operational control of datasets.
Annex A — A.11 AI System Design & Development	Controls for system development, architecture, testing	Measure — Trustworthiness evaluation Manage — Controlled development	Aligns with MEASURE 3.x (model evaluation) and MANAGE 4.2 (risk treatment).
Annex A — A.12 Robustness & Security	Adversarial robustness, threat mitigation, security controls	Measure — Robustness evaluation Manage — Mitigation actions	Aligns with MEASURE robustness tasks and MANAGE risk mitigation.
Annex A — A.13 Explainability & Transparency	Explainability, interpretability, transparency of system behavior	Measure — Documentation & evaluation	Aligns with MEASURE documentation and transparency assessments.
Annex A — A.14 Model Evaluation & Testing	Requirements for evaluation, testing, validation	Measure	Direct alignment with MEASURE 3.x.
Annex A — A.15 Human Oversight Requirements	Human oversight, fallback procedures, decision authority	Govern — Oversight Manage — Escalation & control actions	Aligns with GOVERN (role authority) and MANAGE (fallback controls, escalation).
Annex A — A.16 Monitoring & Drift Management	Performance monitoring, drift detection, lifecycle tracking	Manage — Operational monitoring	Aligns with MANAGE 4.x operational risk mitigation.
Annex A — A.17 Incident Response	Incident reporting, mitigation, documentation	Manage — Incident management	Maps directly to MANAGE 4.4.
Annex A — A.18 Continuous Improvement	Governance and system improvement expectations	Manage — Continuous improvement	Aligns with MANAGE corrective action and continuous improvement tasks.

CPMAI → NIST SP 800-53 Rev. 5

The following crosswalk maps each CPMAI phase to NIST SP 800-53 Rev. 5 security and privacy controls. Only controls with meaningful applicability to AI governance, data management, system development, resilience, and operational assurance are included.

CPMAI Phase	Key Activities	Aligned NIST SP 800-53 Rev. 5 Controls	Supporting Notes
Phase I – Business Understanding	Define business objectives, stakeholder roles, AI use case scope, governance expectations, risk criteria	• PM-1–PM-11 (Program Management) • RA-1–RA-7 (Risk Assessment) • PL-1–PL-10 (Planning) • CA-1 (Assessment Policies)	Governance establishment maps directly to PM controls; risk posture definition aligns with RA controls; PL controls support security planning, objectives, and governance documentation.
Phase II – Data Understanding	Data inventory, data profiling, privacy analysis, representativeness assessments	• RA-3 (Risk Assessment – Data Impact) • RA-8 (Privacy Impact Assessment) • PT-2 (Personally Identifiable Information Processing) • IP-1–IP-4 (Individual Participation) • AR-2 (Privacy Reporting)	Data profiling and privacy assessments align with RA and privacy control families, including consent, minimization, and lawful processing requirements.
Phase III – Data Preparation	Data cleaning, labeling, transformation, lineage, reproducibility, dataset versioning	• SI-12 (Information Management & Retention) • MP-2 (Media Protections) • SC-28 (Data-at-Rest Protection) • SC-8 (Transmission Confidentiality & Integrity) • AU-9 (Audit Record Protection)	Dataset governance maps to confidentiality, integrity, auditability, and retention requirements enforced through SC, MP, and AU control families.
Phase IV – Model Development	Model training, testing, robustness evaluation, fairness & explainability development, experiment tracking	• SA-3 (System Development Processes) • SA-8 (Security Engineering Principles) • SA-15 (Development Process Documentation) • SR-11 (Supply Chain – Component Authenticity) • SI-6 (Security Function Verification)	Model development aligns with secure engineering, verifiable processes, supply chain assurance, and functional robustness verification.
Phase V – Model Evaluation	Independent evaluation, robustness & bias assessment, uncertainty analysis, documentation of limitations	• CA-2 (Assessment – Control Testing) • CA-5 (Independent Assessments) • SI-7 (Software, Firmware, Information Integrity) • RA-5 (Vulnerability Monitoring & Scanning)	Model evaluation maps to independent assessment, system integrity monitoring, and risk identification through CA, SI, and RA controls.
Phase VI – Operationalization	Deployment, monitoring, telemetry, drift detection, incident response, decommissioning	• AU-6 (Audit Review, Analysis, Reporting) • SI-4 (System Monitoring) • IR-4 (Incident Handling) • IR-5 (Incident Monitoring) • IR-6 (Incident Reporting) • SC-5 (Denial-of-Service Protection) • SC-6 (Resource Availability) • MP-6 (Media Sanitization)	Operationalization directly maps to monitoring, auditing, incident response, resilience, availability protections, and secure decommissioning.

CPMAI → CSRMC

The following crosswalk maps each CPMAI phase to the DoD Cyber Security Risk Management Construct (CSRMC) modernization elements. It shows how AI lifecycle activities contribute to mission-driven risk management, automation, continuous validation, resilience, reciprocity, and telemetry-driven visibility.

CPMAI Phase	Key Activities	Aligned CSRMC Modernization Elements	Supporting Notes
Phase I – Business Understanding	Define mission and business objectives, stakeholders, success criteria, governance scope, initial risk criteria, and AI use case boundaries	• Mission-Driven Risk (MRP) • Reciprocity & Inheritance	Mission outcomes and critical functions identified in this phase provide the basis for the Mission Risk Profile (MRP) and control prioritization. Early review of existing authorizations and control baselines supports reciprocity and inheritance planning from the outset.
Phase II – Data Understanding	Inventory and categorize data sources; perform data profiling; assess sensitivity, regulatory constraints, and mission impact; begin defining telemetry needs	• Mission-Driven Risk (MRP) • Visibility & Telemetry	Data understanding informs mission-centric risk assessments by identifying critical data assets and impacts to mission if compromised or corrupted. Telemetry and data flow needs begin to be defined to support CSRMC's visibility objective.
Phase III – Data Preparation	Clean, transform, and label data; establish lineage and versioning; design data pipelines and logging; prepare data for training and evaluation	• Automation & AEP • Visibility & Telemetry • Reciprocity & Inheritance	Data pipelines and lineage tracking feed Automated Evidence Packages (AEP) and enable telemetry-based visibility into data handling. Where shared datasets or common services exist, evidence and controls can be reused across systems, supporting reciprocity.
Phase IV – Model Development	Train models, document experiments, perform robustness and bias testing, design explainability and oversight, define resilience and fallback behavior	• Survivability / Resilience • Automation & AEP • Continuous Compliance Validation (CCV)	Robustness, resilience, and fallback strategies align with CSRMC survivability expectations. Experiment logs, testing outputs, and model documentation contribute to AEP content. Initial control checks and validation logic created in this phase form the basis for CCV rules.
Phase V – Model Evaluation	Conduct independent evaluations, validate trustworthiness criteria, finalize risk posture, prepare Go/No-Go recommendations	• Mission-Driven Risk (MRP) • Continuous Compliance Validation (CCV) • Survivability / Resilience	Evaluation links residual risk directly to mission impacts through the MRP lens. Pre-deployment CCV runs validate that required controls are functioning as intended, while resilience assessments confirm survivability under adverse or degraded conditions.
Phase VI – Operationalization	Deploy models, activate telemetry, run CCV cycles, monitor performance and drift, respond to incidents, update AEP and CRPR, manage changes and decommissioning	• Visibility & Telemetry • Continuous Compliance Validation (CCV) • Automation & AEP • Survivability / Resilience • Reciprocity & Inheritance	Production telemetry provides continuous visibility into AI system behavior and supports CCV. Automated evidence generation (AEP) and recurring resilience assessments (e.g., updated Cyber Resilience Posture Reports) sustain CSRMC's modernization goals. Where shared platforms or services are used, reciprocity and inherited evidence reduce redundant assessments while maintaining mission-driven assurance.

ISO/IEC 42001 → CSRMC Crosswalk

The following crosswalk maps ISO/IEC 42001:2023 Clauses and Annex A control families to the DoD Cyber Security Risk Management Construct (CSRMC) modernization elements. This matrix demonstrates how ISO/IEC 42001's AI Management System (AIMS) requirements naturally align to CSRMC's mission-driven, automation-enabled, continuously validated operational model.

ISO/IEC 42001 Clause / Annex A Control	Requirement Summary	Aligned CSRMC Elements	Supporting Notes
Clause 4 – Context of the Organization (4.1–4.3)	Defines organizational context, stakeholder expectations, and AIMS scope	• Mission-Driven Risk (MRP) • Reciprocity & Inheritance	Establishing AI system scope and mission context provides the baseline for developing the Mission Risk Profile and identifying opportunities for reuse of existing authorizations.
Clause 5 – Leadership (5.1–5.3)	Leadership commitment, policy establishment, roles, responsibilities	• Mission-Driven Risk (MRP) • Survivability / Resilience	Leadership accountability aligns with CSRMC's mission ownership and resilience expectations. Mission outcomes drive leadership decisions in both frameworks.
Clause 6 – Planning (6.1–6.3)	Risk planning, objectives, mitigation, change planning	• Mission-Driven Risk (MRP) • Continuous Compliance Validation (CCV)	Planning requirements align to CSRMC's mission risk prioritization and need for ongoing validation of risk mitigation effectiveness.
Clause 7 – Support (7.1–7.5)	Competence, awareness, resources, communication, documentation	• Automation & AEP • Visibility & Telemetry	Documentation and communication requirements align to evidence automation and telemetry-driven visibility in CSRMC. Competency expectations support mission-driven risk governance.
Clause 8 – Operation (8.2 Data requirements, 8.3 Dataset creation, 8.4 Development, 8.5 Evaluation, 8.6 Deployment, 8.7 Monitoring, 8.8 Incident Management, 8.9 Decommissioning)	Full lifecycle operational controls for AI systems	• Visibility & Telemetry • Continuous Compliance Validation (CCV) • Survivability / Resilience • Automation & AEP	Operational controls align directly with CSRMC's telemetry, CCV, resilience, and automation pillars. Monitoring and evidence generation form the core of continuous assurance.
Clause 9 – Performance Evaluation (Monitoring, measurement, audits, management review)	Evaluation of AIMS effectiveness, audits, metric review, leadership oversight	• Continuous Compliance Validation (CCV) • Visibility & Telemetry	Performance evaluation aligns with CCV cycles and telemetry analytics used for continuous oversight under CSRMC.
Clause 10 – Improvement (Corrective actions, continual improvement)	Required improvements to AIMS, policies, and controls	• Survivability / Resilience • Automation & AEP	Continuous improvement processes align to resilience expectations and automated evaluation of controls under CSRMC.
Annex A – A.2 Governance & Accountability	Governance structure, roles, oversight responsibilities	• Mission-Driven Risk (MRP)	Governance roles support mission alignment and ownership of mission-critical controls.
Annex A – A.3 Risk Assessment	Formal risk identification and documentation	• Mission-Driven Risk (MRP) • Continuous Compliance Validation (CCV)	Establishes mission-centric risk baselines and supports CCV assessment cycles.
Annex A – A.4 Responsible AI Policy	Principles and policies for responsible AI	• Mission-Driven Risk (MRP)	Policies reflect mission impacts, ethical considerations, and stakeholder needs.
Annex A – A.5 Data Quality Requirements	Data integrity, suitability, consistency	• Visibility & Telemetry • Automation & AEP	Data quality tracking feeds AEP and telemetry-driven visibility.
Annex A – A.6 Dataset Documentation	Metadata, lineage, documentation	• Automation & AEP	Structured dataset documentation directly contributes to AEP automation.

ISO/IEC 42001 Clause / Annex A Control	Requirement Summary	Aligned CSRMC Elements	Supporting Notes
Annex A — A.7 Dataset Governance	Data access, security, retention	• Survivability / Resilience	Protects mission-critical data assets and supports resilience against manipulation.
Annex A — A.11 AI System Design & Development	Requirements for design, architecture, testing	• Survivability / Resilience • Continuous Compliance Validation (CCV)	Design controls ensure resilience and inform CCV rule creation and validation activities.
Annex A — A.12 Robustness & Security	Adversarial testing, robustness, threat mitigation	• Survivability / Resilience • Visibility & Telemetry	Robustness and threat mitigation directly support mission durability; telemetry provides insight into resilience posture.
Annex A — A.13 Explainability & Transparency	Transparency and human interpretability	• Mission-Driven Risk (MRP)	Increased transparency supports risk-based decision-making in mission-critical environments.
Annex A — A.14 Model Evaluation & Testing	Testing, validation, trustworthiness evaluation	• Continuous Compliance Validation (CCV)	Evaluation results inform CCV cycles and automated validation logic.
Annex A — A.15 Human Oversight Requirements	Oversight, human-in-the-loop controls	• Mission-Driven Risk (MRP) • Survivability / Resilience	Human oversight supports mission assurance and resilience under operational stress.
Annex A — A.16 Monitoring & Drift Management	Monitoring of system behavior, drift detection	• Visibility & Telemetry • Continuous Compliance Validation (CCV)	Aligns directly with telemetry and CCV requirements for continuous operational visibility.
Annex A — A.17 Incident Response	Incident detection, mitigation, response procedures	• Survivability / Resilience	Incident response maps directly to mission continuity and resilience expectations.
Annex A — A.18 Continuous Improvement	Lessons learned, control updates, improvement cycle	• Automation & AEP • Survivability / Resilience	Automated evidence and resilience assessments inform continuous improvement cycles.

NIST AI RMF → CSRMC Crosswalk

The following crosswalk maps the NIST Artificial Intelligence Risk Management Framework (AI RMF) Core Functions—Govern, Map, Measure, and Manage—to the DoD Cyber Security Risk Management Construct (CSRMC) modernization elements.

It shows how AI risk management activities reinforce mission-driven, automation-enabled, continuously validated cyber risk governance.

NIST AI RMF Function / Focus Area	Purpose / Core Activities	Aligned CSRMC Elements	Supporting Notes
Govern (GOV) – Organizational AI Governance	Establishes AI governance structures, roles, policies, accountability, and risk ownership at the organizational level	• Mission-Driven Risk (MRP) • Reciprocity & Inheritance	Governance outcomes define how mission priorities shape AI risk decisions and which existing authorizations or control baselines can be reused. This aligns directly with CSRMC's mission-centric risk construct and reciprocity expectations.
Govern – Policies, Procedures, & Accountability	Defines AI policies, risk tolerance, escalation paths, and oversight responsibilities	• Mission-Driven Risk (MRP) • Survivability / Resilience	Policy-driven accountability ensures mission owners remain responsible for AI-enabled capabilities, supporting CSRMC's emphasis on mission continuity and resilience.
Govern – Culture, Training, & Awareness	Promotes risk-aware culture, training, and awareness on AI risks and controls	• Mission-Driven Risk (MRP)	Training and awareness enable personnel to understand mission impacts of AI risk and their role in protecting mission outcomes, reinforcing CSRMC's mission focus.
Map (MAP) – Context & Use Case Definition	Identifies AI use case, context, objectives, stakeholders, and potential impacts	• Mission-Driven Risk (MRP)	MAP activities provide the input needed to construct and maintain the Mission Risk Profile, including mission-essential functions, dependencies, and impact paths.
Map – System & Data Characterization	Describes system boundaries, data sources, data flows, and dependencies	• Visibility & Telemetry • Reciprocity & Inheritance	Understanding data flows and dependencies informs telemetry design for CSRMC visibility and helps identify where inherited controls and shared services can be leveraged.
Map – Risk Identification & Categorization	Identifies AI-specific risks (bias, robustness, misuse, security, privacy, etc.) and categorizes them	• Mission-Driven Risk (MRP) • Survivability / Resilience	Categorized risks can be tied directly to mission impacts and survivability requirements, fueling the MRP and resilience posture assessments.
Measure (MEA) – Risk & Trustworthiness Assessment	Evaluates AI system behavior, performance, robustness, fairness, and other trustworthiness characteristics	• Continuous Compliance Validation (CCV) • Automation & AEP	Measurement outputs (tests, metrics, evaluation results) can be structured into Automated Evidence Packages and used as inputs to CCV logic for ongoing validation.
Measure – Data, Model, & System Metrics	Defines and calculates metrics for data quality, model performance, robustness, explainability, and operational behavior	• Visibility & Telemetry • Automation & AEP	Metrics can be integrated into telemetry dashboards and automated evidence pipelines, aligning with CSRMC's visibility and automation principles.
Measure – Evaluation & Validation Activities	Performs testing, red-teaming, robustness assessments, and independent evaluations	• Survivability / Resilience • Continuous Compliance Validation (CCV)	Evaluation activities directly support resilience assessments and can be encoded as part of CCV rule sets and periodic validation cycles.
Manage (MAN) – Risk Response & Mitigation	Selects and applies safeguards, mitigations, and compensating controls based on risk appetite and mission needs	• Mission-Driven Risk (MRP) • Survivability / Resilience	Risk responses are selected based on mission impact tolerance, reinforcing CSRMC's mission-driven risk management and survivability priorities.
Manage – Operations, Monitoring, & Control	Oversees deployed AI systems, monitors real-time behavior, and updates controls based on observed risk	• Visibility & Telemetry • Continuous Compliance Validation (CCV) • Automation & AEP	Operational monitoring and feedback loops align with CSRMC's requirement for telemetry-driven visibility, automated evidence updates, and continuous validation of control effectiveness.

NIST AI RMF Function / Focus Area	Purpose / Core Activities	Aligned CSRMC Elements	Supporting Notes
Manage – Incident Response & Recovery	Detects, triages, responds to, and recovers from AI-related incidents	• Survivability / Resilience	Incident handling supports CSRMC survivability by preserving mission continuity and informing resilience posture updates.
Manage – Lifecycle Improvement & Decommissioning	Updates models, data, and controls; manages material changes; decommissions AI systems when appropriate	• Reciprocity & Inheritance • Automation & AEP • Survivability / Resilience	Lifecycle changes and decommissioning rely on reusable evidence, inherited controls, and updated resilience assessments, aligning with CSRMC's emphasis on re-use and sustained mission resilience.

NIST SP 800-53 Critical Controls → CSRMC

The following crosswalk maps critical NIST SP 800-53 Rev. 5 security and privacy controls—those most relevant to AI system assurance—to the DoD Cyber Security Risk Management Construct (CSRMC) modernization elements.

Controls selected for this matrix are those with direct applicability to automation, telemetry, resilience, mission-driven risk management, and continuous validation.

NIST SP 800-53 Control	Control Purpose / Summary	Aligned CSRMC Elements	Supporting Notes
RA-3 – Risk Assessment	Identify, assess, and categorize risks to systems and data	• Mission-Driven Risk (MRP)	Inputs directly support MRP creation and mission-aligned risk categorization.
RA-5 – Vulnerability Monitoring & Scanning	Continuous identification of vulnerabilities and exposures	• Continuous Compliance Validation (CCV) • Visibility & Telemetry	Vulnerability data feeds CCV cycles and telemetry-driven visibility.
PL-2 – System Security & Privacy Plans	Define security and privacy requirements and control baselines	• Mission-Driven Risk (MRP) • Reciprocity & Inheritance	Supports mission-aligned baselines and reuse of common controls across systems.
PM-1–PM-11 – Program Management Controls	Governance, oversight, and enterprise risk management requirements	• Mission-Driven Risk (MRP)	Enterprise governance establishes mission-critical responsibilities and prioritization.
CA-2 – Security Assessments	Assess effectiveness of controls through testing and evaluation	• Continuous Compliance Validation (CCV)	Assessment results feed automated CCV routines.
CA-5 – Independent Assessments	Independent audits of system risk posture and control effectiveness	• Continuous Compliance Validation (CCV)	Provides authoritative evidence for automated or periodic validation cycles.
SI-4 – System Monitoring	Monitor system behavior, logging, alerts, anomaly detection	• Visibility & Telemetry • Continuous Compliance Validation (CCV)	A foundational telemetry source for real-time operational visibility and CCV triggers.
AU-6 – Audit Review, Analysis, & Reporting	Review and analyze audit logs for anomalous or malicious activity	• Visibility & Telemetry	Audit logs support CSRMC visibility and continuous situational awareness.
AU-9 – Audit Record Protection	Protect audit logs from modification or unauthorized access	• Visibility & Telemetry	Ensures integrity of telemetry and evidence used by AEP and CCV.
SC-7 – Boundary Protection	Enforce network segmentation, isolation, and traffic control	• Survivability / Resilience	Enhances resilience by protecting critical AI components and data paths.
SC-5 – Denial-of-Service Protection	Protect against service disruption and resource exhaustion	• Survivability / Resilience	Directly contributes to mission continuity under attack or degraded conditions.
SC-6 – Resource Availability	Ensure required system resources remain available	• Survivability / Resilience	Supports operational continuity for mission-essential functions.
SC-28 – Data-at-Rest Protection	Protect stored data from unauthorized access or modification	• Survivability / Resilience	Secures mission-critical datasets supporting AI model integrity.
SC-8 – Transmission Confidentiality & Integrity	Protect data in transit via encryption and integrity mechanisms	• Survivability / Resilience	Maintains integrity and confidentiality of mission-critical telemetry and training data.
MP-6 – Media Sanitization	Securely dispose of or sanitize storage media	• Survivability / Resilience	Supports secure decommissioning and mission protection during lifecycle transitions.

NIST SP 800-53 Control	Control Purpose / Summary	Aligned CSRMC Elements	Supporting Notes
IR-4 – Incident Handling	Detect, analyze, respond to, and mitigate incidents	• Survivability / Resilience • Visibility & Telemetry	Incident handling aligns with resilience expectations and uses telemetry for detection and response.
IR-6 – Incident Reporting	Report incidents according to policy and mission requirements	• Mission-Driven Risk (MRP)	Ensures that mission-critical impacts are communicated and escalated appropriately.
SA-3 – System Development Processes	Apply structured development and engineering processes	• Automation & AEP	Documentation and testing outputs contribute to automated evidence pipelines.
SA-8 – Security Engineering Principles	Incorporate security principles into system design and architecture	• Survivability / Resilience	Reinforces resilience and hardened design expectations.
SA-15 – Development Process Documentation	Require documented development processes and artifacts	• Automation & AEP	Structured documentation aligns with AEP formation requirements.

ISO/IEC 42001 Clause Reference Index

The table below provides a concise reference for the ISO/IEC 42001:2023 Clauses and key Annex A control families used within this guide. It summarizes each clause's purpose, primary governance themes, the core documentation artifacts that support conformance, where those topics are addressed in this guide, and how they align to the CPMAI lifecycle.

ISO/IEC 42001 Clause / Annex A Family	Purpose (Summary)	Primary Governance Themes	Associated Documentation	Where It Appears in the Guide	CPMAI Lifecycle Mapping
Clause 4 – Context of the Organization	Define internal and external context, stakeholder needs, and AIMS scope for AI systems	Organizational context, stakeholder expectations, AI system scope, mission alignment	AI Governance Scope Statement, Business Case, Stakeholder Register, AIMS Scope Definition	Section 0 – Executive Orientation; Section 1 – Methodology Overview; Section 2 – Phase I (Business Understanding)	Primarily Phase I – Business Understanding (with context reused across all phases)
Clause 5 – Leadership	Establish leadership commitment, AI policy, and assignment of roles, responsibilities, and authorities	Leadership accountability, AI policy, escalation paths, role authority, oversight	AI Policy, Governance Charter, RACI Matrix, Role Descriptions, Governance Board Charter	Section 0 – Executive Orientation; Section 3 – Cross-Cutting Controls & Governance; Section 4 – Roles & RACI	Cross-cutting across all CPMAI phases, anchored in Phase I and sustained through Phase VI
Clause 6 – Planning	Define AI governance objectives, address risks and opportunities, and plan changes to the AIMS	Governance objectives, risk planning, SoA planning, change planning	Risk Criteria & Impact Assessment, Risk Register, Statement of Applicability (SoA), Governance Objectives Register, Change Evaluation Procedure	Section 2 – Phase I (Business Understanding); Section 3 – Cross-Cutting Controls & Governance; Section 5 – Evidence & Documentation Index	Primarily Phase I – Business Understanding, with risk and planning elements feeding Phases II–VI
Clause 7 – Support	Ensure resources, competence, awareness, communication, and documented information for the AIMS	Competence and training, awareness, resource allocation, documentation control	AI Training & Awareness Plan, Role-based Training Matrix, Communications Plan, Document & Record Control Procedure, Evidence Repository Structure	Section 3 – Cross-Cutting Controls & Governance; Section 5 – Evidence & Documentation Index; Section 7 – Governance Operations & Sustainment	Cross-cutting support for all CPMAI phases, especially Phase IV–VI where operational competence and documentation are critical
Clause 8 – Operation	Define and control operational processes for data, AI system development, evaluation, deployment, monitoring, incident management, and decommissioning	Operational controls, data governance, lifecycle controls, monitoring, incident response, decommissioning	Data Management Plan, Data Inventory, Data Pipeline Specification, Threat Model, Model Card, Evaluation Report, AI Monitoring & Drift Plan, Incident Response Plan, Decommissioning Plan	Section 2 – Phases II–VI (Data Understanding through Operationalization); Section 3 – Cross-Cutting Controls & Governance; Section 7 – Governance Operations & Sustainment	Phase II – Data Understanding, Phase III – Data Preparation, Phase IV – Model Development, Phase V – Model Evaluation, Phase VI – Operationalization
Clause 9 – Performance Evaluation	Monitor, measure, analyze, and evaluate AIMS performance; conduct internal audits and management reviews	Performance metrics, internal audit, governance effectiveness, management review	Governance Metrics Dashboard, Internal Audit Plan & Reports, Management Review Pack, AI Governance Performance Summary	Section 3 – Cross-Cutting Controls & Governance; Section 5 – Evidence & Documentation Index; Section 7 – Annual Management Review & Sustainment	Cross-cutting, with strongest alignment to Phase V – Model Evaluation and Phase VI – Operationalization
Clause 10 – Improvement	Address nonconformities, drive corrective actions, and	Corrective actions, lessons learned, continuous	Nonconformity & Corrective Action Log, Continuous	Section 3 – Corrective & Preventive Action; Section 6 – Maturity & Rollout	Cross-cutting continuous improvement across all

ISO/IEC 42001 Clause / Annex A Family	Purpose (Summary)	Primary Governance Themes	Associated Documentation	Where It Appears in the Guide	CPMAI Lifecycle Mapping
	ensure continual improvement of the AIMS	improvement, remediation planning	Improvement Register, Lessons Learned Repository, Governance Improvement Roadmap	Model; Section 7 – Governance Operations & Sustainment	CPMAI phases, with emphasis on post-deployment feedback loops
Annex A.2 – Governance & Accountability	Define governance structure, oversight mechanisms, and accountability for AI systems	Governance structure, roles, decision-making, escalation	Governance Charter, RACI Matrix, Governance Board Terms of Reference, Delegation of Authority Matrix	Section 3 – Cross-Cutting Controls & Governance; Section 4 – Roles & RACI	Cross-cutting, primarily influencing Phase I – Business Understanding and governance activities in Phases IV–VI
Annex A.3 – Risk Assessment	Require structured, documented AI risk assessments	Risk identification, analysis, evaluation, prioritization	AI Risk Assessment Template, Risk Register, MRP-aligned Risk Views	Section 2 – Phase I (Risk Criteria); Section 3 – Risk Management & Risk Register Integration; Appendix B – Crosswalk Matrices	Initiated in Phase I and updated in Phases II–VI as risks evolve
Annex A.4 – Responsible AI Policy	Establish responsible AI principles and policy commitments	Ethics, fairness, transparency, accountability, human rights	Responsible AI Policy, Ethical AI Guidelines, Policy Acknowledgment Records	Section 0 – Executive Orientation; Section 3 – Cross-Cutting Controls & Governance	Cross-cutting normative baseline for all CPMAI phases
Annex A.5 – Data Quality Requirements	Ensure that data used for AI is appropriate, accurate, complete, and timely	Data quality, integrity, representativeness	Data Quality Criteria, Data Profiling & Quality Reports, Data Acceptance Checklist	Section 2 – Phase II (Data Understanding); Phase III (Data Preparation); Section 3 – Data Governance	Primarily Phase II – Data Understanding and Phase III – Data Preparation
Annex A.6 – Dataset Documentation	Require comprehensive dataset metadata, provenance, and documentation	Documentation, provenance, traceability	Data Inventory, Dataset Documentation Sheets, Data Lineage Diagrams, Metadata Catalog	Section 2 – Phases II–III; Section 5 – Evidence & Documentation Index	Phase II – Data Understanding and Phase III – Data Preparation
Annex A.7 – Dataset Governance	Govern dataset access, security, retention, and lifecycle	Data governance, access control, retention	Data Governance Policy, Access Control Matrix for Datasets, Retention & Disposal Schedule	Section 2 – Phases II–III; Section 3 – Cross-Cutting Controls & Governance	Mainly Phases II–III, with implications for Phase VI – Operationalization
Annex A.11 – AI System Design & Development	Establish requirements for AI system design, development, and testing	Secure design, development controls, engineering practices	System Architecture Description, Design Decision Logs, Model Development Plan, Test Plan	Section 2 – Phase IV (Model Development); Section 3 – Cross-Cutting Controls & Governance	Phase IV – Model Development, with dependencies from Phases II–III
Annex A.12 – Robustness & Security	Ensure AI systems are robust, resilient, and secure against threats and misuse	Robustness, adversarial resilience, security controls	Threat Model, Security Test Results, Adversarial Testing Reports, Cyber Resilience Posture Report (CRPR)	Section 2 – Phases IV–V; Section 3 – AI Risk & Security; Section 7 – CSRMC-Aligned Sustainment	Phase IV – Model Development, Phase V – Model Evaluation, and Phase VI – Operationalization for resilience validation
Annex A.13 – Explainability & Transparency	Define expectations for explainability, interpretability, and transparency of AI systems	Explainability, transparency, user understanding	Explainability Plan, Model Card, User & Stakeholder Communication Artifacts	Section 2 – Phases IV–V; Section 3 – Human Oversight & Transparency	Phase IV – Model Development and Phase V – Model Evaluation
Annex A.14 – Model	Require rigorous evaluation and testing	Evaluation, testing, validation, verification	Evaluation Plan, Evaluation Report, Test Results Archive, Go/No-	Section 2 – Phase V (Model Evaluation); Section 5 –	Phase V – Model Evaluation

ISO/IEC 42001 Clause / Annex A Family	Purpose (Summary)	Primary Governance Themes	Associated Documentation	Where It Appears in the Guide	CPMAI Lifecycle Mapping
Evaluation & Testing	of AI systems prior to and during deployment		Go Recommendation Memo	Evidence & Documentation Index	
Annex A.15 – Human Oversight Requirements	Define human oversight mechanisms, decision authority, and intervention points	Oversight, human-in-the-loop, escalation	Oversight & Escalation Matrix, Human-in-the-Loop Procedures, Operational Runbooks	Section 2 – Phases IV–VI; Section 3 – Human Oversight & Role Authority	Primarily Phases IV–VI, where operational decision-making and oversight occur
Annex A.16 – Monitoring & Drift Management	Require monitoring of AI system behavior and management of model/data drift	Monitoring, drift detection, lifecycle tracking	AI Monitoring & Drift Management Plan, Telemetry Specification, Performance Dashboards	Section 2 – Phase VI (Operationalization); Section 3 – Continuous Monitoring; Section 7 – Continuous Monitoring Workflow	Phase VI – Operationalization
Annex A.17 – Incident Response	Require documented incident response procedures for AI system failures and security/privacy incidents	Incident handling, response, communication	AI Incident Response Plan, Incident Log, Post-Incident Review Reports	Section 2 – Phase VI; Section 3 – Corrective & Preventive Actions; Section 7 – CSRMC-Based Sustainment Activities	Phase VI – Operationalization
Annex A.18 – Continuous Improvement	Require continuous improvement of AI systems and AIMS processes	Lessons learned, corrective actions, optimization	Continuous Improvement Register, Lessons Learned Reports, Governance Improvement Roadmap	Section 3 – Corrective & Preventive Actions; Section 6 – Maturity & Rollout Model; Section 7 – Governance Operations & Sustainment	Cross-cutting across all CPMAI phases, with emphasis on post-deployment learning

Note: This index is designed to support practical implementation and audit preparation by focusing on the clauses and Annex A families most directly leveraged in this guide. It can be extended with additional detail as your organization's AIMS matures.

End Of Section

Appendix D – Governance & Lifecycle Artifact Reference

This appendix serves as the comprehensive reference index for all governance, lifecycle, security, resilience, and compliance artifacts required throughout the AI system lifecycle. It outlines the full set of artifacts—templates, required deliverables, and evidence records—that support CPMAI activities and ensure alignment with ISO/IEC 42001, the NIST AI RMF, NIST SP 800-53, and the DoD CSRMC. Rather than providing the templates themselves, this appendix identifies what must be produced, maintained, or validated at each stage, enabling program managers, engineers, and auditors to navigate governance expectations with clarity and consistency.

The CPMAI Lifecycle

CPMAI Phase I – Business Understanding

This section consolidates all templates, required deliverables, and evidence artifacts associated with Phase I of the CPMAI methodology. Phase I establishes the strategic and organizational foundation that guides every AI initiative. During this phase, teams define the business problem, articulate the value proposition, identify stakeholders and decision authorities, and determine the governance expectations that will frame the remainder of the lifecycle. This stage also formalizes the initial risk posture, establishes scoping boundaries, and ensures alignment with organizational objectives, regulatory obligations, and mission-driven priorities. Together, these artifacts create the structure, clarity, and accountability necessary to execute an AI project responsibly and effectively.

Phase I Combined Artifact Table – Business Understanding

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
Templates	Business Case Template	Defines the value hypothesis, expected outcomes, and justification for the AI initiative.	Clause 4, Clause 5	Govern	MRP
	AI Governance Scope Statement Template	Establishes system boundaries, responsible roles, and applicable governance requirements.	Clause 4	Govern	MRP, REC
	Stakeholder Register Template	Documents all stakeholders, responsibilities, and communication pathways.	Clause 4.2	Govern	—
	Risk Criteria Template	Captures organizational thresholds for risk acceptance, impact categories, and decision boundaries.	Clause 6	Map	MRP
	Initial Statement of Applicability (SoA) Template	Identifies ISO/IEC 42001 Annex A controls applicable to the project and rationale.	Clause 6, Annex A	Govern	REC
	Governance Communication Plan Template	Outlines communication expectations, review cycles, and decision-making pathways.	Clause 7.4	Govern	—
Required Deliverables	Business Case	Documented rationale, strategic alignment, and expected benefits of the AI project.	Clause 4, 5	Govern	MRP

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
	AI Governance Scope Statement	Defines governance boundaries for the system and required oversight.	Clause 4	Govern	REC
	Stakeholder Register	Identifies key actors, roles, responsibilities, and communication expectations.	Clause 4.2	Map	—
	Initial Risk Register	Captures early risks, assumptions, uncertainties, and mitigation considerations.	Clause 6	Map	MRP
	Initial SoA (v1)	Documents applicable annex controls and scoping decisions.	Clause 6, Annex A	Govern	REC
	Governance Charter (if applicable)	Establishes the authority structure for oversight and decision-making.	Clause 5	Govern	MRP
Evidence Artifacts	Context of Organization Analysis	Documentation of internal/external factors impacting AI system governance.	Clause 4	Govern	—
	Leadership Commitment Evidence	Proof of leadership endorsement (memos, approvals, meeting minutes).	Clause 5	Govern	REC
	Risk Criteria Justification	Evidence supporting selected thresholds, impacts, and decision logic.	Clause 6	Map	MRP
	Authority & Role Assignments	Records demonstrating defined responsibilities and authorities.	Clause 5.3	Govern	—
	Repository Initialization Evidence	Proof that governance repositories and document structures were created.	Clause 7.5	Govern	AEP
	Gate 1 – Business Understanding Review Output	Signed decision record for progressing to Phase II.	Clause 9	Manage	CCV

CPMAI Phase II – Data Understanding

This section consolidates all templates, required deliverables, and evidence artifacts associated with Phase II of the CPMAI methodology. Phase II focuses on understanding the data required for the AI initiative, including its sources, quality, structure, representativeness, legal/ethical constraints, and potential risks. These artifacts ensure responsible data handling aligned with ISO/IEC 42001, NIST AI RMF, and CSRMC expectations.

Phase II Combined Artifact Table – Data Understanding

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
Templates	Data Inventory Template	Captures all datasets, sources, owners, sensitivities, and access requirements.	Clause 8.2, 8.3	Map	TEL, MRP
	Data Profiling Report Template	Structures the assessment of quality, completeness, representativeness, and drift signals.	Clause 8.3	Measure	TEL
	Data Sensitivity & Privacy Assessment Template	Evaluates legal, privacy, CUI/PII exposure, and ethical constraints.	Clause 8.2	Govern / Map	MRP
	Data Provenance & Lineage Template	Documents origins, transformations, and movement of data.	Clause 8.3	Map	AEP
	Data Risk Assessment Template	Identifies risks linked to data bias, gaps, quality defects, and security exposures.	Clause 6, 8	Map / Measure	MRP, CCV
Required Deliverables	Data Inventory	Complete listing of datasets, sources, ownership, sensitivity level, and compliance requirements.	Clause 8.2	Map	TEL, MRP
	Data Profiling Report	Analysis of data quality, structure, relevance, and statistical characteristics.	Clause 8.3	Measure	TEL
	Privacy Impact Assessment (PIA)	Identifies privacy impacts, required protections, and compliance obligations.	Clause 8.2	Govern	MRP
	Data Sensitivity Classification	Documents classification for CUI/FOUO/PII/PHI or internal sensitivity levels.	Clause 8.2	Map	MRP
	Data Source Documentation	Identifies upstream systems, data governance constraints, and interoperability considerations.	Clause 8.2, 8.3	Map	REC
	Updated Risk Register (Data Risks Added)	Consolidates risks from Phase II related to bias, data quality, and representativeness.	Clause 6	Map	MRP
Evidence Artifacts	Data Quality Metrics & Profiling Logs	Evidence supporting data representativeness, completeness, and statistical validity.	Clause 8.3	Measure	TEL
	Data Access Authorization Records	Demonstrates proper access controls and approvals for data retrieval.	Clause 7, 8.7	Govern / Manage	RES
	Data Lineage Documentation	Proof of how data moves, transforms, and is governed across systems.	Clause 8.3	Map	AEP
	Privacy Impact Assessment Record	Official PIA documentation for audit or compliance validation.	Clause 8.2	Govern	MRP
	Bias & Representativeness Assessment	Evidence of bias scanning, statistical comparison, and fairness checks.	Clause 8.3	Measure	TEL
	Gate 2 – Data Understanding Review Output	Signed approval confirming readiness to proceed to Phase III.	Clause 9	Manage	CCV

CPMAI Phase III – Data Preparation

This section consolidates all templates, required deliverables, and evidence artifacts associated with Phase III of the CPMAI methodology. Phase III focuses on preparing, transforming, labeling, and governing data for model development. It emphasizes quality, reproducibility, lineage, privacy preservation, and documentation of all transformations. These artifacts support ISO/IEC 42001 operational requirements, NIST AI RMF risk mitigation, and CSRMC automation and validation expectations.

Phase III Combined Artifact Table – Data Preparation

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
Templates	Data Preparation & Transformation Plan Template	Documents required transformations, cleaning approaches, feature engineering, and reproducibility steps.	Clause 8.3	Measure	AEP
	Data Labeling Guidelines Template	Standardizes labeling procedures, quality controls, roles, and oversight.	Clause 8.3	Measure / Manage	TEL
	Data Versioning & Lineage Log Template	Captures dataset versions, change history, and lineage.	Clause 7.5, 8.3	Govern / Map	AEP, CCV
	Data Quality Report Template	Defines quality thresholds, defects, resolution steps, and validation outcomes.	Clause 8.3	Measure	TEL
	Privacy-Preserving Techniques Template	Defines anonymization, minimization, perturbation, and security controls.	Clause 8.3, 8.7	Map / Manage	RES, MRP
Required Deliverables	Data Preparation & Transformation Plan	Formal documentation of all cleaning, transformation, and pre-processing activities.	Clause 8.3	Measure	AEP
	Labeled Dataset (w/ QA Results)	Completed labeled dataset with validation checks.	Clause 8.3	Measure	TEL
	Data Version Control Logs	Records tracking dataset versions, lineage, and change management.	Clause 7.5	Govern	AEP, CCV
	Data Quality Assessment Report	Final quality evaluation, covering completeness, accuracy, drift risk, and representativeness.	Clause 8.3	Measure	TEL
	Privacy-Preserving Data Documentation	Evidence of de-identification, minimization, and handling of sensitive attributes.	Clause 8.7	Manage	RES
	Updated Risk Register (Data Prep Risks Added)	Includes risks related to privacy, quality, transformations, leakage, and bias.	Clause 6	Map	MRP, CCV
Evidence Artifacts	Data Transformation Scripts / Records	Evidence showing how data was transformed, cleaned, and encoded.	Clause 7.5, 8.3	Measure	AEP
	Version Control Repository Logs	Git or equivalent logs demonstrating lineage and reproducibility.	Clause 7.5	Govern	AEP, CCV
	Quality Validation Logs	QA test results validating accuracy, consistency, and completeness.	Clause 8.3	Measure	TEL
	Privacy Technique Validation Evidence	Proof that privacy-preserving methods were applied correctly.	Clause 8.7	Manage	RES, MRP
	Access Authorization Records (Data Prep Environment)	Evidence that only authorized personnel handled sensitive data.	Clause 7, 8.7	Govern / Manage	RES

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
	Gate 3 – Data Preparation Review Output	Signed approval confirming readiness to proceed to Phase IV.	Clause 9	Manage	CCV

CPMAI Phase IV – Model Development

This section consolidates all templates, required deliverables, and evidence artifacts associated with Phase IV of the CPMAI methodology. Phase IV focuses on designing, developing, training, and documenting machine learning and AI models. It includes experimentation tracking, performance evaluation, explainability planning, and alignment with security and resilience expectations. These artifacts support ISO/IEC 42001 development controls, NIST AI RMF risk identification and mitigation, and CSRMC's emphasis on automation, resilience, and visibility.

Phase IV Combined Artifact Table – Model Development

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
Templates	Model Development Plan Template	Documents model objectives, architecture, data inputs, assumptions, constraints, and evaluation criteria.	Clause 8.4	Map / Measure	MRP, RES
	Experiment Tracking Log Template	Captures model experiments, hyperparameters, data versions, and results for reproducibility.	Clause 7.5, 8.4	Measure	AEP
	Threat Modeling Template (AI/LLM/GenAI)	Identifies adversarial risks, misuse scenarios, and model-specific threat vectors.	Clause 8.4, Annex A	Measure / Manage	RES, TEL
	Explainability & Transparency Plan Template	Defines how the model's behavior will be explained to users, stakeholders, and auditors.	Clause 8.4	Map	—
	Model Performance Evaluation Template	Standardizes recording of accuracy, robustness, fairness, and operational metrics.	Clause 8.4	Measure	TEL
Required Deliverables	Model Development Plan	Completed documentation defining the model structure, evaluation metrics, constraints, and assumptions.	Clause 8.4	Map	MRP
	Experiment Tracking Log	Full record of model training steps, experiments, data versions, and outcomes.	Clause 7.5	Measure	AEP
	Threat Model (AI-Specific)	Documentation of threats such as poisoning, extraction, evasion, hallucinations, or misuse.	Clause 8.4, Annex A	Measure / Manage	RES
	Draft Model Card (v1)	Early documentation capturing model intent, performance, risks, and limitations.	Clause 8.4	Map / Measure	—
	Explainability & Human Oversight Strategy	Plan detailing required human review, decision boundaries, and transparency expectations.	Clause 8.4	Govern	—
	Preliminary Robustness & Bias Test Results	Initial tests assessing sensitivity, stability, and fairness.	Clause 8.4, 8.7	Measure	TEL
	Updated Risk Register (Model Risks Added)	Adds model-specific risks related to adversarial behavior, uncertainty, and failure modes.	Clause 6	Map	MRP, CCV
Evidence Artifacts	Model Training Logs	Machine-generated logs documenting parameters, epochs, accuracy, loss, and training environment.	Clause 7.5	Measure	AEP
	Hyperparameter & Architecture Documentation	Evidence of model design integrity and reproducibility.	Clause 7.5, 8.4	Measure	AEP
	Threat Modeling Outputs	Structured evidence of identified threats and mitigation steps.	Clause 8.4	Measure / Manage	RES, TEL

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
	Explainability Artifacts	SHAP/LIME outputs, feature attribution plots, or interpretability tools.	Clause 8.4	Measure	—
	Bias & Fairness Evaluation Logs	Evidence documenting fairness tests, parity gaps, and mitigation actions.	Clause 8.4	Measure	TEL
	Gate 4 – Model Development Review Output	Signed approval confirming readiness to proceed to Phase V.	Clause 9	Manage	CCV

CPMAI Phase V – Model Evaluation

This section consolidates all templates, required deliverables, and evidence artifacts associated with Phase V of the CPMAI methodology. Phase V focuses on the independent evaluation, validation, and verification of AI models prior to deployment. It emphasizes robustness, fairness, security, uncertainty evaluation, compliance validation, and readiness for operational use. These artifacts support ISO/IEC 42001 evaluation and audit requirements, NIST AI RMF measurement and management functions, and CSRMC expectations for Continuous Compliance Validation (CCV), resilience, and mission-driven assurance.

Phase V Combined Artifact Table – Model Evaluation

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
Templates	Independent Evaluation Plan Template	Defines evaluation scope, criteria, methods, tools, and independence requirements.	Clause 9	Measure	CCV
	Model Evaluation Report Template	Standardized structure for summarizing evaluation results, findings, deviations, and approvals.	Clause 9	Measure / Manage	AEP
	Risk Acceptance Record Template	Documents residual risks, acceptance rationale, and leadership approval.	Clause 6, 9	Manage	MRP
	Go/No-Go Recommendation Memo Template	Provides a structured decision document summarizing model readiness.	Clause 9	Manage	CCV
	Updated Model Card Template (Release Candidate)	Captures final model performance, risks, controls, and operational recommendations.	Clause 8.4	Measure	—
Required Deliverables	Independent Evaluation Plan	Defines the criteria, methods, and required outputs for model validation activities.	Clause 9	Measure	CCV
	Evaluation Report	Summarizes all validation activities, robustness tests, fairness assessments, and residual risks.	Clause 9	Measure / Manage	AEP
	Updated Model Card (RC Version)	A near-final Model Card capturing detailed model characteristics, risks, and governance.	Clause 8.4	Measure	—
	Residual Risk Assessment & Acceptance Record	Documentation of unresolved risks and decision authority sign-off.	Clause 6, 9	Manage	MRP
	Go/No-Go Decision Memo	Formal decision record determining whether the model may proceed to deployment.	Clause 9	Manage	CCV
	Updated Risk Register (Evaluation Risks Added)	Incorporates findings from bias, robustness, adversarial testing, and uncertainty evaluations.	Clause 6	Map / Manage	MRP
Evidence Artifacts	Robustness Test Results	Evidence of model behavior under stress, perturbation, and adversarial scenarios.	Clause 8.4, 9	Measure	RES
	Fairness & Harm Evaluation Logs	Documentation of fairness testing, harm analysis, and mitigation verification.	Clause 9	Measure	TEL
	Uncertainty & Reliability Metrics	Evidence of calibration, uncertainty quantification, and failure mode mapping.	Clause 8.4	Measure	TEL
	Security Evaluation Results	Outputs from adversarial, extraction, or poisoning assessments.	Clause 8.4	Measure / Manage	RES
	Independent Review Records	Evidence of evaluation independence (roles, approvals, separation of duties).	Clause 5, 9	Govern	REC

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
	Gate 5 – Model Evaluation Review Output	Signed approval confirming readiness to proceed to Phase VI.	Clause 9	Manage	CCV

CPMAI Phase VI – Operationalization

This section consolidates all templates, required deliverables, and evidence artifacts associated with Phase VI of the CPMAI methodology. Phase VI focuses on deploying the AI system into production, establishing monitoring and telemetry, enabling continuous compliance, defining operational roles, validating resilience, and ensuring readiness for long-term governance. These artifacts support ISO/IEC 42001 operational and monitoring requirements, NIST AI RMF management functions, and CSRMC's expectations for automation, resilience, and continuous validation.

Phase VI Combined Artifact Table – Operationalization

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
Templates	Deployment Readiness Checklist Template	Confirms all operational, security, monitoring, and documentation requirements are complete prior to go-live.	Clause 8.6	Manage	CCV, RES
	AI System Runbook Template	Defines operational procedures, escalation paths, monitoring actions, and failover behaviors.	Clause 8.7	Manage	RES
	AI Monitoring & Drift Management Plan Template	Describes metrics, signals, thresholds, logs, and monitoring workflows.	Clause 8.7	Manage	TEL, CCV
	Telemetry Specification Template	Defines telemetry sources, logging formats, drift metrics, anomaly indicators, and evidence automation.	Clause 7.5, 8.7	Measure / Manage	TEL, AEP
	Incident Response Plan (AI-Specific) Template	Documents detection, response, reporting, and containment procedures tailored for AI systems.	Clause 8.8	Manage	RES
	Material Change Evaluation (MCE) Template	Defines criteria and procedures for evaluating changes impacting risk, governance, or approvals.	Clause 8.9	Manage	CCV, REC
	Post-Deployment Review Template	Standardizes early operational assessments following go-live.	Clause 9	Manage	CCV
	Model Card (Release Version) Template	Final model documentation used for operational governance, monitoring, and audit.	Clause 8.4	Measure	—
Required Deliverables	Deployment Readiness Checklist	Final validated checklist confirming operational, security, monitoring, and documentation readiness.	Clause 8.6	Manage	CCV, RES
	AI System Runbook	Operational procedures for day-to-day and emergency system management.	Clause 8.7	Manage	RES
	AI Monitoring & Drift Management Plan	Defines ongoing monitoring, drift detection, drift thresholds, and anomaly workflows.	Clause 8.7	Manage	TEL, CCV
	Telemetry Specification	Documentation of telemetry events, monitoring thresholds, and evidence automation requirements.	Clause 7.5, 8.7	Measure / Manage	TEL, AEP
	Continuous Compliance Validation (CCV) Configuration	Documentation of CCV triggers, testing routines, evidence sources, and automation.	Clause 9	Measure / Manage	CCV, AEP
	Cyber Resilience Posture Report (CRPR)	Evaluation of survivability, continuity, adversarial robustness, and mission assurance.	Clause 8.7	Measure / Manage	RES, MRP
	AI-Specific Incident Response Plan	Tailored IR plan covering AI-related events such as hallucinations, drift, data leakage, or adversarial disruption.	Clause 8.8	Manage	RES

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
	Role Authorization & Access Review	Review of operational access rights, privileges, and segregation of duties.	Clause 7, 8.7	Govern / Manage	RES
	Material Change Evaluation Documentation	Documentation of change reviews affecting model performance, risk, or governance.	Clause 8.9	Manage	CCV, REC
	Model Card (Release Version)	Final structured summary of the deployed model, required for governance and audit.	Clause 8.4	Measure	—
	Post-Deployment Review Report	Initial evaluation of early operational performance, stability, and incidents.	Clause 9	Manage	CCV
	Updated Risk Register (Operational Risks Added)	Captures deployment-related risks, operational risks, monitoring gaps, and resilience risks.	Clause 6	Map / Manage	MRP, CCV
Evidence Artifacts	Monitoring & Telemetry Activation Logs	Evidence that monitoring and telemetry systems are active and collecting data.	Clause 8.7	Measure / Manage	TEL, AEP
	Drift Detection Logs	Evidence of drift monitoring, triggered drift events, or thresholds reached.	Clause 8.7	Measure / Manage	TEL
	CCV Output Logs	Machine-generated results validating control effectiveness.	Clause 9	Measure / Manage	CCV
	Failover & Recovery Test Results	Evidence supporting resilience, continuity, and survivability.	Clause 8.7	Manage	RES
	Incident Response Exercise Results	Documentation of tests validating IR readiness for AI-specific scenarios.	Clause 8.8	Manage	RES
	Operational Access Logs	Logs documenting operational access and administrative actions for accountability.	Clause 7.5, 8.7	Govern / Manage	TEL
	Evidence of AEP Generation	Records confirming evidence was automatically produced and packaged.	Clause 9, 7.5	Measure / Manage	AEP, CCV
	Gate 6 – Operationalization Review Output	Signed approval confirming readiness for sustainment and monitoring phases.	Clause 9	Manage	CCV

Cross-Phase Governance Artifacts

This section consolidates all templates, required deliverables, and evidence artifacts that span multiple CPMAI phases and form the operational backbone of the AI Governance Framework. These artifacts are foundational governance components maintained throughout the AI lifecycle, updated iteratively, and required for ISO/IEC 42001 conformity, NIST AI RMF execution, and CSRMC modernization activities.

The table below includes all cross-phase governance artifacts with mappings to ISO clauses, AI RMF functions, and CSRMC elements.

Cross-Phase Governance Artifact Table

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
Templates	Governance Charter Template	Establishes AI governance authority, leadership commitments, and oversight structure.	Clause 5	Govern	MRP
	RACI Matrix Template	Defines accountability and responsibilities across all governance roles.	Clause 5.3	Govern	—
	Communication Plan Template	Establishes communication mechanisms, reporting cadence, and escalation pathways.	Clause 7.4	Govern	—
	Document Control Template	Standardizes versioning, approval, retention, and archiving.	Clause 7.5	Govern	AEP
	Training & Competency Record Template	Tracks AI governance training, competency requirements, and certifications.	Clause 7.2	Govern	—
	Risk Register Template	Standardized structure for recording risks, impacts, owners, and mitigations.	Clause 6	Map / Manage	MRP, CCV
	SoA (Statement of Applicability) Template	Defines applicable ISO controls and justification for inclusion/exclusion.	Clause 6, Annex A	Govern	REC
Required Deliverables	Governance Charter	Leadership-approved document establishing governance authority and oversight boundaries.	Clause 5	Govern	MRP
	RACI Matrix	Complete definition of role responsibilities across the AI lifecycle.	Clause 5.3	Govern	—
	Communication Plan	Defines communication cadence, governance reporting, stakeholder engagement.	Clause 7.4	Govern	—
	Document Control Records	Maintains document versioning, approvals, and retention logs.	Clause 7.5	Govern	AEP
	Training & Competency Records	Evidence of personnel readiness, certifications, and skills.	Clause 7.2	Govern	—
	Risk Register (Continuous Updates)	Continuously maintained record of risks across all phases.	Clause 6	Map / Manage	MRP, CCV
	SoA (Continuous Updates)	Updated after each phase to reflect maturity, control applicability, and decisions.	Clause 6, Annex A	Govern	REC
	Governance Repository Structure	Controlled storage environment for all governance artifacts and evidence.	Clause 7.5	Govern	AEP
Evidence Artifacts	Leadership Commitment Evidence	Signed approvals, meeting minutes, governance reviews.	Clause 5	Govern	—

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
	Updated Risk Register	Evidence of iterative governance and risk updates across lifecycle.	Clause 6	Map / Manage	MRP
	Updated SoA	Evidence of control applicability decisions and updates.	Clause 6	Govern	REC
	Document Control Logs	Version history showing lifecycle compliance and audit readiness.	Clause 7.5	Govern	AEP
	Training Completion Records	Evidence supporting competency and readiness.	Clause 7.2	Govern	—
	Governance Review Meeting Records	Minutes documenting governance decisions, escalations, and actions.	Clause 9	Govern / Manage	—

Cross-Phase Security & Resilience Artifacts

This section consolidates templates, required deliverables, and evidence artifacts related to security, privacy, resilience, and mission assurance that operate across multiple CPMAI phases. These artifacts represent the continuous security posture of AI systems and align with ISO/IEC 42001 operational controls, NIST AI RMF security functions, NIST SP 800-53 expectations, and CSRMC modernization pillars such as resilience, telemetry, CCV, and mission-driven risk.

Cross-Phase Security & Resilience Artifact Table

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
Templates	Security Governance Plan Template	Outlines ongoing security responsibilities, controls, escalation paths, and monitoring expectations.	Clause 8.7	Govern / Manage	RES
	Cyber Resilience Posture Report (CRPR) Template	Establishes structure for resilience, survivability, stress testing, and mission continuity documentation.	Clause 8.7	Measure / Manage	RES, MRP
	AEP (Automated Evidence Package) Template	Defines the structure of machine-readable evidence used for continuous validation and audits.	Clause 7.5, 9	Measure	AEP, CCV
	CCV Configuration Template	Specifies automated validation routines, triggers, telemetry sources, and compliance logic.	Clause 9	Measure / Manage	CCV
	Telemetry & Logging Configuration Template	Defines the logging schema, telemetry sources, monitoring signals, and retention requirements.	Clause 8.7	Measure / Manage	TEL
	Incident Response (AI-Specific) Template	Provides structure for IR scenarios unique to AI systems (drift, hallucination, model misuse).	Clause 8.8	Manage	RES
	Security Test & Evaluation (ST&E) Template	Standardizes robustness, adversarial testing, and vulnerability scanning outputs.	Clause 8.4	Measure	RES
Required Deliverables	Security Governance Plan	Defines the security responsibilities, controls, and practices for AI systems across all phases.	Clause 8.7	Govern	RES
	Cyber Resilience Posture Report (CRPR)	Captures resilience findings, continuity performance, and survivability testing results.	Clause 8.7	Manage	RES, MRP
	AEP (Automated Evidence Package)	Machine-readable evidence prepared for audits, CCV, and automated governance workflows.	Clause 7.5, 9	Measure	AEP, CCV
	CCV Configuration Document	Records configuration of continuous compliance validation routines.	Clause 9	Measure / Manage	CCV
	Telemetry & Logging Configuration	Required for monitoring, resilience evaluation, anomaly detection, and operational assurance.	Clause 8.7	Measure / Manage	TEL
	AI-Specific Incident Response Plan	Required across all phases to address AI-related failure and misuse conditions.	Clause 8.8	Manage	RES
	Security Controls Verification Logs	Records continuous verification of 800-53 controls via CCV workflows.	Clause 9	Measure	CCV
	Configuration Baseline (Security)	Records versions of security configurations, controls, and monitoring settings.	Clause 7.5, 8.4	Govern / Manage	AEP
Evidence Artifacts	Robustness Test Logs	Evidence of adversarial robustness, stress testing, and degradation analysis.	Clause 8.4	Measure	RES

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
	Vulnerability Scan Reports	Evidence of tested controls, software integrity, and model/system vulnerabilities.	Clause 8.4	Measure	CCV
	Telemetry Activation Records	Proof that telemetry services are enabled and feeding monitoring systems.	Clause 8.7	Measure	TEL
	Incident Response Exercise Records	Evidence of periodic IR drills relevant to AI behaviors.	Clause 8.8	Manage	RES
	CCV Output Logs	Evidence that continuous control checks were run, validated, and recorded.	Clause 9	Measure / Manage	CCV
	AEP Generation Logs	Evidence confirming automated evidence creation.	Clause 7.5, 9	Measure	AEP
	Security Audit Trail Logs	Evidence of security-relevant actions and system events across the lifecycle.	Clause 7.5, 8.7	Govern / Manage	TEL
	Updated Resilience Findings	Evidence of resilience posture changes, mitigation steps, and survivability improvements.	Clause 8.7	Measure / Manage	RES

AEP & CCV Evidence Artifacts

This section consolidates all templates, required deliverables, and evidence artifacts supporting Automated Evidence Packages (AEP) and Continuous Compliance Validation (CCV) across the AI lifecycle. These artifacts represent the automation backbone of CSRMC-aligned governance, enabling continuous monitoring, mission-driven risk evaluation, and real-time assurance of control effectiveness.

AEP artifacts support machine-readable documentation, automated governance workflows, audit acceleration, and version-controlled evidence generation.
CCV artifacts support automated control testing, continuous validation of requirements, and detection of deviations or security gaps.

The table below includes all AEP/CCV-associated templates, deliverables, and evidence artifacts with mappings to ISO/IEC 42001, NIST AI RMF, and CSRMC modernization elements.

AEP & CCV Evidence Artifact Table

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
Templates	Automated Evidence Package (AEP) Template	Defines standardized structure for machine-readable evidence bundles supporting audits and automation.	Clause 7.5, 9	Measure	AEP
	AEP Metadata Schema Template	Provides metadata fields for traceability, timestamps, controls, source systems, and evidence context.	Clause 7.5	Measure	AEP
	CCV Configuration Template	Defines automated control tests, validation triggers, telemetry sources, and control mappings.	Clause 9	Measure / Manage	CCV
	CCV Test Case Template	Structures automated test cases for validating security, privacy, and operational controls.	Clause 9	Measure	CCV
	Telemetry Evidence Specification Template	Defines telemetry fields, log formats, data retention, and monitoring evidence requirements.	Clause 8.7	Measure	TEL
	Machine-Readable Control Mapping Template	Maps security controls (e.g., 800-53, ISO, CSRMC) to specific evidence signals for automation.	Clause 7.5	Measure	AEP, CCV
Required Deliverables	Automated Evidence Package (AEP)	Machine-readable evidence bundle automatically generated during lifecycle operations.	Clause 7.5, 9	Measure	AEP
	Evidence Register (AEP/CCV Integrated)	Consolidated index of all evidence files, metadata, and lifecycle references.	Clause 7.5	Measure	AEP
	CCV Configuration Document	Records CCV triggers, routines, telemetry inputs, and testing logic.	Clause 9	Measure / Manage	CCV
	CCV Test Suite	Automated test suite validating controls, resilience conditions, and operational requirements.	Clause 9	Measure	CCV
	Telemetry Evidence Package	Machine-generated telemetry snapshots supporting monitoring, resilience, and anomaly detection.	Clause 8.7	Measure	TEL

Category	Artifact Name	Purpose / Description	ISO/IEC 42001 Clause	AI RMF Function	CSRMC Alignment
	AEP/CCV Version Control Records	Version-controlled logs for AEP updates and CCV configuration changes.	Clause 7.5	Govern	AEP, CCV
Evidence Artifacts	AEP Generation Logs	Proof that evidence bundles were automatically produced and packaged at expected intervals.	Clause 7.5, 9	Measure	AEP
	CCV Output Logs	Logs documenting successful or failed automated control checks.	Clause 9	Measure / Manage	CCV
	Telemetry Snapshots	Evidence of real-time indicators, drift signals, anomaly metrics, and system health status.	Clause 8.7	Measure	TEL
	Machine-Readable Control Evidence	JSON/YAML evidence mappings supporting automation and audit requirements.	Clause 7.5	Measure	AEP
	Automated Performance/Compliance Alerts	Evidence of automated detections for drift, anomalies, or control degradation.	Clause 9	Manage	CCV
	Evidence Integrity Hash Records	Cryptographic or system-generated validation that evidence has not been modified.	Clause 7.5	Govern	AEP
	Lifecycle Evidence Archive Records	Documentation of long-term storage, retention, and indexing of lifecycle evidence bundles.	Clause 7.5	Govern	AEP

ISO/IEC 42001 Clause-Based Required Records

This section provides a consolidated table of all ISO/IEC 42001 required records, reorganized from the standard's clause structure into a practical reference for governance teams. Each record type is mapped to the corresponding CPMAI phases, AI RMF functions, and CSRMC modernization elements, showing how ISO documentation requirements are fulfilled throughout the lifecycle.

These records are mandatory for demonstrating conformity with ISO/IEC 42001 and form part of the evidence base used in audits, internal assessments, Automated Evidence Packages (AEP), and Continuous Compliance Validation (CCV) workflows.

ISO/IEC 42001 Required Records Table

ISO/IEC 42001 Clause	Record / Required Document	Purpose / Description	CPMAI Phases	AI RMF Function	CSRMC Alignment
Clause 4 – Context of the Organization	Organizational Context Analysis	Documents internal/external issues, interested parties, and governance boundaries.	Phase I	Govern	MRP
	AI System Scope Statement	Defines the scope of the AI management system and governed AI systems.	Phase I	Govern	MRP
Clause 5 – Leadership	Leadership Commitment Records	Evidence of leadership endorsement, resource support, and governance direction.	All Phases	Govern	—
	Roles, Responsibilities, and Authorities	Formal documentation assigning governance accountability.	Phase I	Govern	—
Clause 6 – Planning	Risk Management Records	Documented risk identification, analysis, mitigation, and tracking.	All Phases	Map / Manage	MRP, CCV
	Responsible AI Objectives	Evidence of objectives aligned with ethical and organizational goals.	Phase I	Govern	—
	Statement of Applicability (SoA)	Records control applicability decisions and justification.	All Phases	Govern	REC
Clause 7 – Support	Competence & Training Records	Documentation of training, skills, and qualifications for AI roles.	All Phases	Govern	—
	Awareness Records	Evidence of organization-wide understanding of AI governance and responsibilities.	All Phases	Govern	—
	Communication Records	Documentation of internal/external communication related to AI governance.	All Phases	Govern	—
	Documented Information Control Records	Controlled documentation for governance artifacts, templates, and evidence.	All Phases	Govern	AEP
Clause 8 – Operation	Data Quality Records	Evidence of data suitability, integrity, representativeness, and governance.	Phases II–III	Map / Measure	TEL
	Model Development & Evaluation Records	Experiment logs, testing results, performance evidence, robustness assessments.	Phases IV–V	Measure / Manage	RES
	Monitoring & Logging Records	Telemetry, drift logs, anomaly detection, performance monitoring.	Phase VI	Measure / Manage	TEL, CCV
	Incident Response Records	AI-specific incident documentation, exercises, and corrective actions.	Phase VI	Manage	RES

ISO/IEC 42001 Clause	Record / Required Document	Purpose / Description	CPMAI Phases	AI RMF Function	CSRMC Alignment
Clause 9 – Performance Evaluation	Monitoring & Measurement Records	Evidence of governance effectiveness, KPIs, review outputs.	All Phases	Measure	CCV
	Internal Audit Records	Documentation of audit scope, findings, and follow-up actions.	Phase VI	Manage	CCV
	Management Review Records	Annual review outputs, decisions, and improvement directives.	Phase VI	Govern	—
Clause 10 – Improvement	Nonconformity & Corrective Action Records	Documentation of issues, root causes, mitigation, and verification.	All Phases	Manage	CCV
	Continual Improvement Records	Evidence of improvements across governance processes and lifecycle operations.	All Phases	Govern / Manage	—

NIST AI RMF Function-Based Artifacts

This section maps key governance, security, operational, and documentation artifacts to the four core functions of the NIST AI Risk Management Framework (AI RMF):

- Govern – Establish organizational policies, oversight, accountability, and documentation
- Map – Understand context, risks, requirements, and system characteristics
- Measure – Evaluate, test, and assess performance, robustness, and security
- Manage – Operationalize controls, monitoring, incident response, and continuous improvement

These artifacts are arranged according to the AI RMF functions that they primarily support. All artifacts are aligned with CPMAI lifecycle phases, ISO/IEC 42001 requirements, and CSRMC modernization elements to demonstrate unified governance coverage.

NIST AI RMF Artifact Table by Function

AI RMF Function	Artifact Name	Purpose / Description	CPMAI Phases	ISO/IEC 42001 Clause	CSRMC Alignment
Govern	Governance Charter	Establishes oversight, accountability, decision rights, and governance structure.	Phase I	Clause 5	MRP
	RACI Matrix	Defines role responsibilities and decision authority throughout lifecycle.	Phase I	Clause 5.3	—
	Communication Plan	Outlines reporting, escalation pathways, and communication expectations.	Phase I	Clause 7.4	—
	SoA (Statement of Applicability)	Identifies applicable controls with justification and lifecycle alignment.	All Phases	Clause 6, Annex A	REC
	Training & Competency Records	Evidence of skills, qualifications, and readiness for AI responsibilities.	All Phases	Clause 7.2	—
	Document Control Records	Ensures versioning, approvals, retention, and audit traceability.	All Phases	Clause 7.5	AEP
	AI Governance Policy	Defines organizational principles, rules, and acceptable practices.	Phase I	Clause 5	—
	AI System Scope Statement	Defines the governance scope and boundaries for AI systems.	Phase I	Clause 4	MRP
Map	Business Case & Value Definition	Establishes objectives, constraints, and business alignment.	Phase I	Clause 4, 5	MRP
	Initial Risk Assessment	Identifies early risks, impacts, and constraints.	Phase I	Clause 6	MRP, CCV
	Data Inventory & Provenance Records	Documents datasets, sources, access controls, and legal/ethical constraints.	Phase II	Clause 8.2	TEL
	Data Profiling & Quality Assessment	Documents data suitability, representativeness, and bias indicators.	Phase II	Clause 8.2	TEL
	Threat Modeling Documentation	Identifies adversarial, operational, and misuse risks.	Phase IV	Clause 8.4	RES
	Mission Risk Profile (MRP)	Aligns system risks with mission objectives and criticality.	All Phases	Clause 4, 6	MRP

AI RMF Function	Artifact Name	Purpose / Description	CPMAI Phases	ISO/IEC 42001 Clause	CSRMC Alignment
	Requirements & Constraints Register	Documents system requirements, constraints, and compliance needs.	Phases I–II	Clause 4, 6	—
Measure	Model Evaluation Reports	Documents model performance, robustness, and validation results.	Phase V	Clause 8.4	RES
	Bias & Fairness Assessment	Evaluates representativeness, bias, and fairness across datasets and outputs.	Phases II–V	Clause 8.4	—
	Drift Detection Logs	Evidence of drift monitoring and anomaly signals.	Phase VI	Clause 8.7	TEL
	Robustness / Stress Test Results	Evaluates model resilience under adversarial or degraded conditions.	Phase IV–V	Clause 8.4	RES
	CCV Configuration & Test Results	Automated validation of compliance, security, and operational controls.	Phase VI	Clause 9	CCV
	Telemetry Evidence Snapshots	Monitoring evidence documenting system performance and operational health.	Phase VI	Clause 8.7	TEL
	Performance Metric Dashboards	Visual dashboards showing operational KPIs and governance indicators.	Phase VI	Clause 9	CCV
Manage	AI System Runbook	Operational procedures, escalation paths, and maintenance workflows.	Phase VI	Clause 8.7	RES
	Incident Response Plan (AI-Specific)	Defines procedures for AI-related incidents (hallucinations, drift, misuse).	Phase VI	Clause 8.8	RES
	Change & Material Change Evaluation Records	Determines governance impacts of system or data changes.	Phase VI	Clause 8.9	REC
	Post-Deployment Review Report	Early operational review validating stability and readiness.	Phase VI	Clause 9	CCV
	Risk Register (Lifecycle Updates)	Continual updates reflecting operational and emerging risks.	All Phases	Clause 6	MRP, CCV
	AEP Generation Logs	Evidence of automated evidence generation supporting audits.	Phase VI	Clause 7.5, 9	AEP
	CCV Output Logs	Evidence of continuous compliance validation.	Phase VI	Clause 9	CCV
	Continuous Monitoring Plan	Defines monitoring, telemetry, and anomaly detection routines.	Phase VI	Clause 8.7	TEL

End Of Section

Appendix E – Security & Privacy Control Crosswalk

NIST SP 800-53 Rev 5 Crosswalk & CSRMC Modernization Summary

To support clarity across this guide's governance structure, this appendix includes a dedicated crosswalk for NIST SP 800-53 Rev. 5 controls and their modernization under CSRMC. While earlier appendices focus on framework-to-framework alignment, this section provides the control-level perspective, enabling teams to understand how specific security and privacy controls operate within the AI lifecycle. This distinction helps ensure that both conceptual alignment and practical control implementation are comprehensively addressed.

This section provides a unified overview of how NIST SP 800-53 Rev. 5 controls align to the AI system lifecycle and how the DoD Cyber Security Risk Management Construct (CSRMC) modernizes their application. It summarizes:

- Mapping of NIST SP 800-53 control families to CPMAI lifecycle phases, ISO/IEC 42001 clauses, NIST AI RMF functions, and organizational governance activities.
- Expected evidence artifacts required to demonstrate compliance for each lifecycle stage.

CSRMC-driven enhancements, including:

- Mission-driven risk prioritization (MRP)
- Automated Evidence Packages (AEP) and control automation
- Continuous Compliance Validation (CCV)
- AI system resilience and survivability requirements
- Reciprocity and inheritance of controls across shared platforms
- Telemetry-enabled monitoring and visibility for operational assurance

Together, these elements ensure that NIST SP 800-53 controls are applied in a mission-focused, automation-enabled, and continuously validated manner aligned with DoD's risk management modernization priorities.

This serves as the authoritative security & privacy control alignment table for AI system governance.

AI Governance Security & Privacy Control Alignment Matrix

800-53 Control Family / Representative Controls	Primary Purpose	CPMAI Lifecycle Phase(s)	ISO/IEC 42001 Alignment	NIST AI RMF Function	CSRMC Modernization Elements
PM – Program Management (PM-1–PM-11)	Enterprise governance, roles, risk posture, planning	Phase I (Business Understanding)	Clauses 4, 5, 6	Govern	MRP, REC
PL – Planning (PL-1–PL-10)	Security planning, objectives, baselines	Phase I	Clauses 4, 6	Govern	MRP
RA – Risk Assessment (RA-1–RA-7)	Risk identification, analysis, categorization	Phase I → V	Clauses 6, 8	Map / Measure	MRP, CCV
RA – Privacy Impact Assessment (RA-8)	Identify privacy and sensitivity impacts	Phase II	Clause 8.2	Map	TEL, MRP
IP / PT – Privacy Controls (IP-1–IP-4, PT-2)	PII handling, transparency, participation	Phase II	Clauses 5, 8	Govern / Map	MRP
SI – System Integrity & Monitoring (SI-2, SI-4, SI-6, SI-7, SI-12)	Monitoring, anomaly detection, integrity validation	Phase IV–VI	Clauses 8.4–8.7	Manage	TEL, CCV, RES
AU – Audit & Accountability (AU-6, AU-9)	Logging, audit review, log integrity	Phase III–VI	Clause 7.5, Clause 8	Govern / Manage	TEL, AEP
SC – System & Communications Protection (SC-5, SC-6, SC-7, SC-8, SC-28)	Availability, encryption, segmentation, data protection	Phase III–VI	Clause 8 (Ops)	Manage	RES
MP – Media Protection (MP-2, MP-6)	Media access, sanitization, data lifecycle	Phase III, VI	Clause 8.9	Manage	RES, REC
CA – Assessment (CA-2, CA-5, CA-7)	Control testing, independent evaluation, continuous monitoring	Phase V–VI	Clauses 9, 10	Measure / Manage	CCV, AEP
IR – Incident Response (IR-4, IR-5, IR-6)	Incident handling, monitoring, reporting	Phase VI	Clause 8.8	Manage	RES, MRP
SA – System & Software Development (SA-3, SA-8, SA-15)	Secure development, engineering, documentation	Phase IV	Clause 8.4, 7.5	Measure	RES, AEP
AC – Access Control (AC-2, AC-3, AC-5)	Access management, role enforcement	Phase II–VI	Clause 7, 8.7	Govern / Manage	RES
CM – Configuration Management (CM-2, CM-3, CM-5)	Baseline control, configuration integrity	Phase III–VI	Clause 8.4–8.6	Manage	CCV, AEP
CP – Contingency Planning (CP-2, CP-4, CP-6)	Backup, recovery, operational continuity	Phase VI	Clause 8.7	Manage	RES, MRP

Evidence Artifact Tables

The tables below list the expected evidence artifacts required to demonstrate compliance with NIST SP 800-53 Rev. 5 control families throughout the AI lifecycle. These artifacts support audit readiness, Automated Evidence Package (AEP) generation, and CSRMC Continuous Compliance Validation (CCV).

Program Management (PM) Evidence Artifacts

Required Artifact	Description / Purpose	Lifecycle Phase
Governance Charter	Defines AI governance structure and mission alignment	Phase I
AI Policy & Responsible AI Principles	Organizational commitments and boundaries	Phase I
Risk Appetite Statement	Defines acceptable mission and operational risk	Phase I
Stakeholder & Role Register	Documents PM, Governance Lead, Risk Officer, etc.	Phase I

Planning (PL) Evidence Artifacts

Required Artifact	Description / Purpose	Lifecycle Phase
AI Governance Scope Statement	Establishes boundaries, systems, and use cases	Phase I
Risk Register (Initial + Updates)	Captures mission-based risk considerations	Phase I–VI
Statement of Applicability (SoA)	Identifies applicable controls and rationale	Phase I

Risk Assessment (RA) Evidence Artifacts

Required Artifact	Description / Purpose	Lifecycle Phase
Risk Assessment Report	Identifies risks from data, model, system	Phase I–V
Bias & Representativeness Analysis	Identifies fairness concerns	Phase II–V
Vulnerability Scan Results	Supports CCV and resilience	Phase IV–VI

Privacy Risk & Compliance Evidence (RA-8, IP/PT)

Required Artifact	Description / Purpose	Lifecycle Phase
Privacy Impact Assessment (PIA)	Ensures sensitive data risks addressed	Phase II
Data Sensitivity Assessment	Evaluates CUI/PII/PHI exposure	Phase II
Consent & Notification Documentation	Required for user-impacting systems	Phase II

System Integrity & Monitoring (SI) Evidence Artifacts

Artifact	Purpose	Lifecycle Phase
Monitoring & Telemetry Specification	Defines logs, metrics, drift signals	Phase VI
System Integrity Check Results	Confirms no tampering/modification	Phase IV–VI
Anomaly Detection Logs	Supports telemetry-driven visibility	Phase VI

Audit & Accountability (AU) Evidence Artifacts

Artifact	Purpose	Lifecycle Phase
Audit Log Configuration	Documents log types and retention	Phase III–VI
Audit Trail Records	Evidence of access, actions, and changes	Phase IV–VI
Log Integrity Validation	Supports AEP/CCV	Phase VI

System & Communications Protection (SC) Artifacts

Artifact	Purpose	Lifecycle Phase
Encryption Configuration	Documents protections at-rest and in-transit	Phase III–VI
Network Architecture Diagram	Shows segmentation and boundary controls	Phase IV
Availability & Failover Validation	Supports survivability	Phase VI

Media Protection (MP) Evidence Artifacts

Artifact	Purpose	Lifecycle Phase
Media Sanitization Record	Proof of secure disposal	Phase VI
Data Handling Workflow	Governs dataset transport and protection	Phase III

Assessment (CA) Evidence Artifacts

Artifact	Purpose	Lifecycle Phase
Independent Assessment Report	Required prior to deployment	Phase V
Continuous Monitoring Plan	CSRMC CCV integration	Phase VI
Automated Evidence Package Inputs	Machine-readable evidence	Phase IV–VI

Incident Response (IR) Evidence Artifacts

Artifact	Purpose	Lifecycle Phase
AI Incident Response Plan	Defines AI-specific incident scenarios	Phase VI
Incident Handling Log	Required for resilience/mission continuity	Phase VI
Incident Notification Proof	For mission-critical reporting	Phase VI

Secure Development (SA) Evidence Artifacts

Artifact	Purpose	Lifecycle Phase
Model Development Plan	Tracks architecture, components, risks	Phase IV
Test Plan & Test Results	Evaluates robustness and security	Phase IV–V
Code Review & Supply Chain Checks	Ensures integrity of components	Phase IV

Access Control (AC) Evidence Artifacts

Artifact	Purpose	Lifecycle Phase
Access Control Matrix	Defines who can access what	Phase II–VI
Role Authorization Evidence	Supports oversight and segregation	Phase VI
Privileged Access Log	Captures sensitive operations	Phase VI

Configuration Management (CM) Evidence Artifacts

Artifact	Purpose	Lifecycle Phase
Configuration Baseline	Required for drift detection and CCV	Phase III
Change Log & MCE Approvals	Tracks changes to models/data	Phase IV–VI
Configuration Validation (CCV Output)	Supports automated validation	Phase VI

Contingency Planning (CP) Evidence Artifacts

Artifact	Purpose	Lifecycle Phase
Backup & Recovery Plan	Ensures survivability and continuity	Phase VI
Failover Test Results	Proof of resilience	Phase VI
Business Continuity Documentation	Supports mission-driven risk	Phase VI

End Of Section

Appendix F – External Reference Alignment

This appendix summarizes how the AI Governance Framework aligns with major external standards, policies, and emerging regulatory requirements. These references provide broader context for governance decisions, assurance expectations, and compliance strategy.

EU AI Act: Provides mandatory requirements for high-risk AI systems, including transparency, data governance, risk management, and post-market monitoring.

ISO/IEC 23894 – AI Risk Management: Supports ISO/IEC 42001 by providing AI-specific risk identification, analysis, evaluation, and treatment guidance.

DoD RAISE – Responsible AI Guidelines: Establishes the DoD's expectations for ethical, trustworthy, and mission-aligned AI development and operation.

OWASP LLM Top 10: Defines the leading security risks for LLM and generative AI applications, informing threat modeling and mitigation activities.

NIST AI 100-1 – GenAI Security & Resilience: Provides U.S. federal guidance on GenAI security, robustness, and operational safeguards.

NIST SP 1270 – Bias & Fairness in AI: Defines methods for assessing, detecting, and mitigating harmful bias throughout the AI lifecycle.

NIST Generative AI Framework (Draft/Anticipated): Expected to define U.S. federal governance, security, and evaluation practices for GenAI systems.

DoD Digital Engineering Strategy: Promotes modern engineering practices that support integrated lifecycle management for AI-enabled systems.

OMB M-25-21 – Federal AI Governance Memo: Outlines requirements for federal agencies and contractors on AI inventories, governance controls, responsible AI safeguards, and system monitoring.

End Of Section

Appendix G – Glossary & Acronyms

This appendix provides unified terminology and acronyms consistent across all referenced frameworks, including CPMAI, ISO/IEC 42001, NIST AI RMF, NIST SP 800-53 Rev. 5, DoD CSRMC, EU AI Act, and related federal and DoD policy documents. These definitions ensure consistency, avoid ambiguity, and support both governance practitioners and auditors.

Glossary of Key Terms

Adversarial Robustness: The ability of an AI system to withstand malicious inputs or perturbations designed to confuse or subvert the model's behavior.

AI Governance Repository: The centralized, access-controlled location for all governance artifacts, evidence, decision records, and lifecycle documentation.

AI System Resilience: The capability of an AI system to maintain safe, reliable, and mission-aligned functionality under stress, failure, or adversarial conditions.

Explainable AI (XAI): Processes and methods that make an AI system's behavior interpretable to humans, supporting transparency, trust, and safety assessments.

Lifecycle Documentation Archive: The structured set of required records maintained at each CPMAI phase, ensuring traceability, audit readiness, and compliance.

MLOps: Engineering discipline that integrates machine learning development with operational deployment, monitoring, and continuous improvement.

Reciprocity & Inheritance: The reuse of validated controls, authorizations, or evidence packages across systems, as supported by CSRMC's modernization principles.

Residual Risk: Risk that remains after all mitigation measures have been applied, formally documented and accepted prior to deployment.

Risk Register: A managed record of identified risks, their classifications, likelihood, impact, and required treatments across the AI lifecycle.

Safety Constraint: Defined operational boundaries intended to limit harmful or unintended outcomes from AI system actions or recommendations.

AI Management System (AIMS): The organizational management system defined by ISO/IEC 42001 for establishing, implementing, maintaining, and continually improving AI governance.

Automated Evidence Package (AEP): A machine-readable, automation-enabled evidence bundle supporting continuous authorization and CSRMC-aligned compliance.

Bias & Representativeness Analysis: Assessment of datasets or model behavior to identify and mitigate harmful or unintended bias, consistent with NIST SP 1270.

Continuous Compliance Validation (CCV): CSRMC practice of ongoing, automated checks that confirm security controls remain effective throughout operations.

Cyber Resilience Posture Report (CRPR): Evaluation of system survivability under degraded or adversarial conditions, used in CSRMC and Phase VI operational readiness.

Data Management Plan (DMP): Documentation outlining data governance, quality, security, lineage, and lifecycle management across CPMAI Phases II–VI.

Drift Detection: Monitoring process that identifies changes in model performance, data distributions, or environment conditions.

Governance Lead: The organizational role responsible for oversight of AI governance execution, risk alignment, documentation, and compliance.

Material Change Evaluation (MCE): The formal review required when a system undergoes changes that may impact risk, documentation, or approvals.

Mission Risk Profile (MRP): CSRMC construct defining mission-aligned risk prioritization for systems impacting critical functions or operations.

Model Card: A structured documentation artifact detailing a model's purpose, performance, risks, limitations, fairness considerations, and operational constraints.

Post-Deployment Review: Operational assessment conducted after model deployment to evaluate performance, safety, and compliance.

Statement of Applicability (SoA): Document listing applicable ISO/IEC 42001 Annex A controls and justifying inclusion or exclusion.

Telemetry Specification: Documentation defining operational metrics, logs, drift signals, anomaly indicators, and resilience monitoring used in CSRMC and operational governance.

Acronyms

Acronym	Meaning
AEP	Automated Evidence Package
AFC	Assisted Failure Conditioning (resilience testing concept)
AIMS	AI Management System (ISO/IEC 42001)
AI RMF	NIST Artificial Intelligence Risk Management Framework
CCV	Continuous Compliance Validation (CSRMC)
CDRL	Contract Data Requirements List
CM	Configuration Management
CPMAI	Cognitive Project Management for AI
CRPR	Cyber Resilience Posture Report
CSRMC	Cyber Security Risk Management Construct (DoD)
CUI	Controlled Unclassified Information
DMP	Data Management Plan
DoD	Department of Defense
IR	Incident Response
ISO	International Organization for Standardization
LLM	Large Language Model
MCE	Material Change Evaluation
ML	Machine Learning
MRP	Mission Risk Profile
NIST	National Institute of Standards and Technology
PIA	Privacy Impact Assessment
PM	Program Manager / Program Management
RA	Risk Assessment
RACI	Responsible, Accountable, Consulted, Informed
SoA	Statement of Applicability
SP	Special Publication (NIST)
TEL	Telemetry & Visibility (CSRMC)

End Of Section