GAI-S

Governed AI Infrastructure Standard

Enterprise Whitepaper

A Universal Governance Framework for Responsible AI Deployment

Version	1.0 — Public Draft
Classification	Enterprise Distribution
Date	2025
Issuing Body	James Derek Ingersoll | GodsIMiJ AI Solutions

Executive Summary

The Governed AI Infrastructure Standard (GAI-S) defines a universal, domain-agnostic governance framework for the responsible design, deployment, and operation of artificial intelligence systems across all industries and organizational contexts.

As AI capabilities expand into consequential decision-making across healthcare, finance, legal systems, public infrastructure, defense, and commercial enterprise, the absence of standardized governance architecture creates compounding institutional risk. Regulatory fragmentation, inconsistent audit practices, and the lack of shared accountability frameworks expose organizations to liability, reputational damage, and preventable harm.

GAI-S addresses this gap directly. It provides a structured, tiered certification model built on five universal compliance domains, applicable to any AI system regardless of modality, scale, or sector. It is designed to be implementable, auditable, and institutionally credible.

Core Positions

- AI governance is an infrastructure problem, not a policy overlay problem.
- Governance mechanisms must be embedded at the system architecture level.
- All AI systems operating in consequential contexts require demonstrable accountability.
- Certification must be achievable through documented evidence, not live demonstration.
- Human oversight authority must be structurally enforced, not assumed.

Document Scope

This whitepaper presents the GAI-S framework in full, including the problem statement, domain architecture, certification tiers, regulatory alignment, and deployment guidance. It is intended for enterprise technology leadership, compliance officers, AI governance practitioners, policy designers, and institutional review bodies.

Contents

Section 1 The Governance Gap in Artificial Intelligence

1.1 The Current State of AI Deployment

Artificial intelligence systems are operating in consequential domains at a pace that has outrun governance infrastructure. Medical AI tools advise on diagnoses. Financial AI systems approve credit and flag fraud. Legal AI systems summarize evidence and draft contracts. Hiring AI filters candidates. Infrastructure AI manages power grids, logistics networks, and emergency services.

Each of these deployments carries risk. Not inherent risk that cannot be managed, but unmanaged risk that stems from the absence of consistent, auditable governance frameworks applied at the point of system design and deployment.

Organizations are building AI systems. Regulators are drafting AI policies. Standards bodies are publishing AI principles. What is missing is the connective infrastructure between principle and practice: a framework that is simultaneously technical enough to guide architects, rigorous enough to satisfy compliance officers, and clear enough to provide institutional confidence.

1.2 What Inadequate AI Governance Produces

The consequences of inadequate AI governance are not theoretical. They manifest across categories:

- Accountability gaps: When AI systems produce adverse outcomes, organizations cannot trace decisions to their source, assign responsibility, or demonstrate due diligence.
- Audit failures: Regulators and internal auditors encounter AI systems that cannot be reviewed without live demonstration, making independent assessment structurally impossible.
- Undetected bias: Systematic disparate treatment across protected classes persists in deployed systems because bias monitoring was never built into the operational architecture.
- Escalation failures: High-risk outputs reach end users without triggering human review because intervention controls were designed as policy rather than enforced as architecture.
- Data boundary violations: Protected and sensitive data crosses undocumented organizational and jurisdictional boundaries through AI inference pipelines.
- Model drift: Risk classification accuracy degrades over time as data distributions shift, with no mechanism to detect or respond to the deterioration.

1.3 The Regulatory Environment

The global regulatory landscape for AI governance is expanding but fragmented. Key frameworks include:

Framework	Jurisdiction	Primary Scope	Enforcement Status
EU AI Act	European Union	Risk-based classification of AI systems	Enacted 2024
NIST AI RMF	United States	Voluntary AI risk management guidance	Published 2023
ISO/IEC 42001	International	AI management system standard	Published 2023

Framework	Jurisdiction	Primary Scope	Enforcement Status
UK AI Principles	United Kingdom	Sector-specific regulatory guidance	Ongoing
HIPAA (AI context)	United States	AI handling protected health information	Existing, evolving
SEC AI Guidance	United States	AI in financial services and disclosure	Evolving
GDPR (AI context)	European Union	Automated decision-making and profiling	Existing

GAI-S is designed to align with and complement these frameworks without requiring organizations to choose between them. Regulatory alignment tables within the standard enable organizations to demonstrate coverage across multiple frameworks from a single governance architecture.

Section 2 The GAI-S Framework

2.1 Design Principles

GAI-S is built on seven foundational design principles that govern the framework's structure, applicability, and implementation requirements.

P-01	*Governance is architecture, not policy. Controls must be embedded in system design, not applied as post-deployment overlays.*

P-02	*Human authority must be structurally enforced. High-consequence decisions require human oversight that the system cannot bypass.*

P-03	*Auditability is a first-class requirement. Systems must be fully reviewable by qualified personnel without live demonstration.*

P-04	*Risk must be quantified, not categorized. Governance controls must be triggered by measurable thresholds, not subjective assessments.*

P-05 *Data boundaries must be documented and enforced. AI inference must operate within defined and controlled trust perimeters.*

P-06 *Governance must be continuous, not point-in-time. Model performance, bias metrics, and risk thresholds require ongoing monitoring and validation.*

P-07 *Certification must reflect operational reality. Claims must be supported by documented evidence and verifiable through independent review.*

2.2 The Five Compliance Domains

GAI-S is organized around five universal compliance domains. Each domain addresses a distinct governance dimension applicable across all AI deployment contexts.

Domain	Name	Core Requirement	Primary Risk Addressed
D1	Authority Separation	Explicit boundary between AI advisory function and human decision authority	Unauthorized autonomous action
D2	Data Governance	Controlled data residency, classification, encryption, and access management	Data breach, boundary violation
D3	Risk Classification	Quantified risk scoring with measurable escalation thresholds	Undetected high-risk outputs
D4	Deployment Containment	Environment separation, dependency control, and continuity planning	System failure, supply chain risk
D5	Documentation Readiness	Complete institutional documentation enabling paper-based compliance review	Audit failure, accountability gap

2.3 Certification Tiers

GAI-S defines three certification tiers. Each tier builds on the prior, adding governance depth, operational maturity requirements, and verification rigor.

Level 1 — Structured Advisory

AI system operating in an advisory capacity with documented governance and basic human-in-the-loop enforcement. Suitable for lower-stakes applications where human review is accessible and consequential decisions remain with humans by convention.

- Documented AI role and authority boundaries

- Basic risk classification (qualitative)
- Human escalation pathway exists and is documented
- Core data protection controls implemented
- Responsible AI statement published

Level 2 — Controlled Operational Deployment

AI system embedded in operational workflows with enforced governance controls, quantitative risk thresholds, and full documentation readiness. Suitable for regulated and semi-regulated environments where institutional review is required.

- All Level 1 requirements
- Quantitative risk classification with automated escalation thresholds
- Human-in-the-loop enforcement (architecturally enforced, not assumed)
- Complete trust boundary architecture documented
- Incident response and breach protocols operational
- Deployment containment with environment separation
- Full institutional documentation package

Level 3 — Institutional Grade Deployment

AI system operating in the highest-consequence contexts with formal governance board structures, validated performance metrics, external audit capability, and full regulatory alignment documentation. Suitable for healthcare, financial services, public infrastructure, legal systems, and critical enterprise applications.

- All Level 2 requirements
- Formal governance board with defined membership and meeting cadence
- Quantitative risk model with drift detection and quarterly recalibration
- Clinical or domain validation study (where applicable)
- 24/7 human oversight infrastructure (for continuous-operation systems)
- Annual independent audit with signed attestation
- Business continuity and disaster recovery plan with defined RTO/RPO
- Regulatory alignment cross-mapping table
- Governance feedback loop: incident-driven model retraining and board review
- Third-party security assessment

Section 3 Domain Specifications

Domain 1 — Authority Separation

3.1.1 Purpose

Authority Separation defines the explicit structural boundary between AI-generated outputs and human decision-making authority. It ensures that AI systems cannot execute consequential actions autonomously in contexts where human judgment is required.

3.1.2 Universal Requirements

- AI system role must be formally defined in writing, specifying what the system is authorized to do and what it is explicitly prohibited from doing autonomously.
- Human decision authority hierarchy must be documented, mapping who has authority over which categories of decisions.
- Escalation pathways must exist for all high-consequence output categories, with defined triggers, routing, and response timelines.
- Override and intervention actions must be logged with actor identity, rationale, and outcome.
- User-facing disclosure must inform all users of the AI system's advisory nature and limitations.

3.1.3 Sector Application Examples

Sector	AI Advisory Function	Prohibited Autonomous Action	Required Human Authority
Healthcare	Symptom analysis, risk flagging, care pathway suggestions	Diagnosis, prescription, clinical intervention	Licensed clinician
Finance	Credit scoring input, fraud signals, portfolio risk analysis	Loan approval, fund disbursement, account action	Authorized officer
Legal	Document review, case research, contract drafting assistance	Legal advice, court filing, binding agreement execution	Licensed attorney
HR / Hiring	Resume screening, skills matching, interview scheduling	Employment decisions, offer issuance, termination	HR authority
Public Safety	Threat scoring, dispatch optimization, pattern analysis	Arrest, detention, enforcement action	Law enforcement officer
Infrastructure	Load prediction, anomaly detection, maintenance scheduling	System shutdown, emergency response, access control	Qualified operator

Domain 2 — Data Governance

3.2.1 Purpose

Data Governance establishes control over the classification, residency, movement, and access of all data processed by AI systems. It ensures that sensitive data remains within defined trust boundaries and that all access is authorized, logged, and auditable.

3.2.2 Universal Requirements

- Data classification model must define categories (e.g., Restricted, Sensitive, Internal, Public) with handling requirements for each.
- Data residency must be declared: where data is stored, processed, and transmitted.
- Encryption must be enforced at rest and in transit using current industry standards.
- Role-based access control (RBAC) must govern all data access with least-privilege enforcement.
- AI inference boundaries must be defined: what data the model receives, where inference occurs, and what is returned and stored.
- Audit logging must capture all access to sensitive data with tamper-evident storage.
- Data retention and deletion policies must be documented and enforced.

3.2.3 AI Inference Boundary Control

A unique governance requirement introduced by AI systems is the inference boundary: the perimeter within which user data is processed by the model. This boundary must be explicitly defined and controlled.

- Local inference: Model runs within organizational infrastructure. Highest data control. Requires adequate compute resources.
- External API inference: Prompts transmitted to third-party model provider. Requires contractual data protection terms, zero-retention clauses, and organizational disclosure to users.
- Hybrid: Tiered approach where sensitive data triggers local inference and general queries use external providers. Requires clear routing logic and audit trail.

Domain 3 — Risk Classification

3.3.1 Purpose

Risk Classification provides a quantitative, consistent methodology for assessing the potential harm of AI system outputs and routing them to appropriate review or escalation pathways. Qualitative risk tiers are insufficient for enterprise governance; measurable scoring is required.

3.3.2 Quantitative Risk Model

GAI-S mandates a Composite Risk Index (CRI) for Level 2 and above deployments:

CRI = Probability Score (1–5) × Severity Score (1–5)

CRI Range	Classification	Required Action	Human Review SLA
1 – 6	Low	Standard processing, routine logging	None required
7 – 12	Moderate	Enhanced logging, periodic audit sampling	Periodic (weekly/monthly)
13 – 18	High	Mandatory human review before final output delivery	Within 4 hours
19 – 25	Critical	Immediate escalation, human review prior to any user-facing response	Within 15 minutes

3.3.3 Model Confidence Score

All AI outputs must include a model confidence score (0.0–1.0). Low-confidence outputs in elevated risk categories trigger additional human review regardless of the CRI classification. A confidence score below 0.60 combined with a CRI of 13 or above constitutes an automatic escalation trigger.

3.3.4 Drift Detection and Recalibration

Risk classification accuracy is not static. Model performance degrades over time as data distributions shift, user populations change, and real-world conditions evolve. GAI-S requires active drift monitoring:

- Probability and severity score distributions monitored weekly.
- Statistically significant shifts (>15% change in mean CRI over 30 days) trigger mandatory model validation review.
- False positive and false negative rates tracked monthly with defined action thresholds.
- Quarterly recalibration review required at Level 3, with governance approval for threshold changes.

Domain 4 — Deployment Containment

3.4.1 Purpose

Deployment Containment ensures AI systems operate within controlled infrastructure boundaries with documented dependencies, defined environment separation, and operational continuity plans. It prevents undocumented external data flows and ensures recovery capability.

3.4.2 Environment Segmentation

All production AI systems must maintain strict separation across three environments:

- Development: Feature development with synthetic data only. No production data permitted.
- Test/Staging: Pre-production validation with production-equivalent architecture. Anonymized or synthetic data only.
- Production: Live deployment with full security controls. All changes require change control approval.

3.4.3 Dependency Transparency

All AI system dependencies must be inventoried and disclosed:

- Foundation model providers: Name, version, data handling terms, applicable agreements.
- Third-party libraries: Name, version, license, known vulnerabilities, update cadence.
- Infrastructure dependencies: Compute, storage, network, monitoring services.
- External APIs: Purpose, data transmitted, provider compliance posture.

3.4.4 Business Continuity Requirements (Level 3)

Objective	Definition	Level 3 Target
RTO (Recovery Time Objective)	Maximum time from failure to resumption of critical functions	< 1 hour for safety-critical functions
RPO (Recovery Point Objective)	Maximum acceptable data loss measured in time	< 15 minutes for sensitive user data
Backup Frequency	How often data is backed up	Transaction logs: 15-min; Full backup: daily
Redundancy	Infrastructure duplication for fault tolerance	Active-active or active-passive with auto-failover

Domain 5 — Documentation Readiness

3.5.1 Purpose

Documentation Readiness requires that all AI systems produce and maintain a complete institutional documentation package enabling qualified reviewers to assess system governance, safety, and compliance without requiring live system access.

This domain exists because live demonstration is not a valid compliance methodology. Governance must be evidenced through documentation.

3.5.2 Required Documentation Package

Document	Purpose	Required From Level
System Architecture Diagram	Technical overview of all components and data flows	Level 1
Authority Boundary Document	Defines AI role, prohibited actions, and escalation pathways	Level 1
Responsible AI Statement	Intended use, limitations, bias mitigation, transparency commitments	Level 1
Risk Classification Matrix	Tier definitions, scoring methodology, escalation rules	Level 2
Data Governance Architecture	Classification model, residency, encryption, RBAC, trust boundary	Level 2
Deployment Architecture	Environment separation, dependencies, fallback mechanisms	Level 2
Incident Response Plan	Classification, timelines, breach response, regulatory notification	Level 2
Change Management Log	All system changes with approval trail and impact assessment	Level 2
Governance Board Charter	Board composition, mandate, meeting cadence, decision authority	Level 3
Regulatory Alignment Matrix	Cross-mapping of GAI-S controls to applicable frameworks	Level 3
Model Validation Report	Quarterly performance audit, bias metrics, recalibration decisions	Level 3
Business Continuity Plan	RTO/RPO, backup strategy, recovery procedures, manual workflows	Level 3
Annual Attestation Statement	Signed compliance affirmation by Compliance Officer of Record	Level 3

Section 4 Governance Architecture

4.1 Human-in-the-Loop Enforcement Architecture

GAI-S distinguishes between two approaches to human oversight: assumed oversight and enforced oversight. Only enforced oversight is acceptable for Level 2 and above certification.

Aspect	Assumed Oversight (Insufficient)	Enforced Oversight (GAI-S Compliant)
Implementation	Policy document states humans will review high-risk outputs	System architecture prevents high-risk outputs from reaching users without review
Bypass risk	High — any operator can bypass the policy	Low — architectural gate cannot be bypassed without system modification
Audit evidence	Policy document (intent)	System logs, review queue records, SLA compliance metrics (evidence)
Failure mode	Silent — oversight failures may not be detected	Loud — SLA breach alerts, queue monitoring, automated escalation

4.2 Governance Board Structure (Level 3)

Level 3 certification requires formal governance institutionalization through defined boards with documented membership, mandate, and accountability.

Domain Oversight Board

Senior oversight body with cross-functional membership. Responsible for strategic governance, policy approval, and executive accountability.

- Chair: Chief Compliance Officer or equivalent
- Members: Information Security Officer, Privacy Officer, Domain Lead (e.g., CMO for healthcare AI)
- Meeting cadence: Quarterly minimum
- Authority: Major system changes, policy approvals, incident governance

Technical Safety Review Board

Operational body responsible for risk model performance, model validation, and technical safety assessment.

- Chair: Senior domain professional with AI governance expertise
- Members: Risk classification lead, data science representative, clinical/domain safety expert
- Meeting cadence: Quarterly minimum; ad-hoc for critical incidents
- Authority: Risk threshold changes, model retraining approval, bias remediation

Compliance Officer of Record

Named individual responsible for day-to-day compliance monitoring, regulatory liaison, and audit coordination. Must have documented qualifications and clear reporting structure.

4.3 Incident Governance Loop

GAI-S Level 3 requires that critical incidents and recurring incident patterns trigger formal governance responses beyond operational remediation. The governance loop ensures that systemic risks are addressed at the institutional level.

Trigger 1

Any Critical-severity incident where model error contributed to root cause requires mandatory Technical Safety Review Board assessment and model retraining evaluation within 48 hours.

Trigger 2

Three or more incidents of similar classification within 90 days constitute a pattern requiring Domain Oversight Board review and documented root cause analysis.

Trigger 3

Sustained false negative rate exceeding 8% or false positive rate exceeding 25% triggers mandatory risk model recalibration with governance approval.

Section 5 Regulatory Alignment

5.1 Framework Alignment Matrix

The following table maps GAI-S domains to the primary requirements of major regulatory and standards frameworks. This mapping enables organizations to use a single GAI-S implementation to demonstrate alignment across multiple regulatory obligations.

GAI-S Domain	EU AI Act	NIST AI RMF	ISO/IEC 42001	HIPAA	SOC 2	GDPR
D1: Authority Separation	Art. 14 (Human oversight)	GOVERN 1.2	Cl. 8.4	164.308 Admin Safeguards	CC6.1	Art. 22 (Automated decisions)
D2: Data Governance	Art. 10 (Data governance)	MANAGE 2.2	Cl. 8.2	164.312 Technical Safeguards	CC6.7	Art. 5 (Data principles)

GAI-S Domain	EU AI Act	NIST AI RMF	ISO/IEC 42001	HIPAA	SOC 2	GDPR
D3: Risk Classification	Art. 9 (Risk management)	MAP 1.5	Cl. 6.1	164.308(a)(1) Risk analysis	CC7.2	Art. 35 (DPIA)
D4: Deployment Containment	Art. 17 (Quality mgmt)	MEASURE 2.6	Cl. 8.5	164.308(a)(7) Contingency	CC6.6 / CC7.5	Art. 25 (Privacy by design)
D5: Documentation Readiness	Art. 11 (Technical docs)	GOVERN 5.1	Cl. 7.5	164.316 Policies	CC2.2	Art. 30 (Records)

5.2 EU AI Act Alignment

The EU AI Act establishes a risk-based classification of AI systems with specific requirements for high-risk AI. GAI-S Level 2 addresses the minimum governance requirements for EU AI Act high-risk systems. GAI-S Level 3 addresses the full compliance posture including conformity assessment requirements.

- Prohibited AI systems: GAI-S Authority Separation domain enforces boundaries that prevent deployment in prohibited use categories.
- High-risk AI systems: GAI-S Levels 2 and 3 address Articles 9 through 17, covering risk management, data governance, technical documentation, logging, transparency, human oversight, accuracy, and robustness.
- General-purpose AI models: GAI-S Data Governance and Deployment Containment domains address model transparency and incident reporting requirements.

5.3 NIST AI Risk Management Framework Alignment

The NIST AI RMF organizes AI risk management into four functions: GOVERN, MAP, MEASURE, and MANAGE. GAI-S domains map directly to these functions and provide the implementation architecture that the NIST framework identifies as necessary but does not specify.

- GOVERN: GAI-S Domain 5 (Documentation) and Level 3 Governance Board requirements directly address GOVERN function outcomes.
- MAP: GAI-S Domain 1 (Authority Separation) and Domain 3 (Risk Classification) address context establishment and risk identification.
- MEASURE: GAI-S Domain 3 quantitative risk model and drift monitoring directly implement MEASURE function requirements for ongoing performance assessment.
- MANAGE: GAI-S Domains 4 and 5, plus incident response requirements, address MANAGE function outcomes.

Section 6 Implementation Pathway

6.1 Pre-Assessment: Existing System Evaluation

Organizations deploying or operating AI systems should begin with a gap assessment against GAI-S requirements before targeting a certification level. The assessment evaluates current governance posture across all five domains.

Assessment Area	Key Questions
Authority Separation	Is the AI role formally defined? Are prohibited autonomous actions documented and enforced? Do escalation pathways exist?
Data Governance	Is data classified? Is residency declared? Are encryption standards documented and enforced? Is access controlled and logged?
Risk Classification	Is there a risk scoring methodology? Are thresholds quantified? Are escalation triggers automated and enforced?
Deployment Containment	Are environments separated? Are dependencies inventoried? Is there a continuity plan with defined RTO/RPO?
Documentation Readiness	Can the system be fully reviewed without live access? Is the documentation package current and complete?

6.2 Level 1 Implementation — Structured Advisory

Target timeline: 4–8 weeks for new deployments; 2–4 weeks for existing systems with existing governance foundations.

1. Define AI role and authority boundaries in writing.
2. Document human decision authority hierarchy.
3. Implement basic data classification and access control.
4. Establish escalation pathway (even if manual) for high-risk outputs.
5. Publish Responsible AI Statement.
6. Implement basic audit logging.
7. Assemble Level 1 documentation package.

6.3 Level 2 Implementation — Controlled Operational Deployment

Target timeline: 3–6 months from Level 1, or 4–8 months from baseline.

8. Implement Composite Risk Index (CRI) scoring engine.
9. Automate escalation triggers at defined CRI thresholds.
10. Enforce human-in-the-loop at architecture level for High and Critical classifications.
11. Document and implement trust boundary architecture.
12. Implement environment separation (Dev/Test/Prod).
13. Complete dependency and model provider inventory.
14. Implement incident response plan with breach procedures.
15. Establish change control process.
16. Assemble complete Level 2 documentation package.

6.4 Level 3 Implementation — Institutional Grade Deployment

Target timeline: 6–12 months from Level 2 certification.

17. Establish formal governance board structure with defined membership.
18. Implement drift detection and model performance monitoring.
19. Establish quarterly model validation and recalibration process.
20. Develop and test Business Continuity and Disaster Recovery plan.
21. Produce regulatory alignment cross-mapping table.
22. Conduct initial internal audit and establish annual audit cycle.
23. Implement governance incident feedback loop.
24. Engage external advisor for independent review (recommended).
25. Obtain signed annual attestation from Compliance Officer of Record.
26. Assemble complete Level 3 documentation package.

Section 7 Responsible AI Alignment

7.1 Transparency Requirements

GAI-S mandates transparency at three levels: user-facing disclosure, institutional disclosure, and algorithmic transparency.

- User-facing disclosure: All users interacting with AI systems must be informed of the system's AI nature, advisory limitations, and human oversight mechanisms.
- Institutional disclosure: Organizations must document and disclose AI system dependencies, data flows, and governance controls to institutional reviewers.

- Algorithmic transparency: Risk classification methodology, threshold settings, and model selection criteria must be documented and available for review.

7.2 Bias Mitigation Framework

Bias in AI systems is not a single problem with a single solution. GAI-S addresses bias across multiple dimensions:

Bias Type	Description	GAI-S Control	Domain
Training data bias	Model reflects biases present in training datasets	Model selection criteria, training data audit	D2, D3
Classification bias	Risk scoring produces disparate outcomes across demographic groups	Bias metrics in quarterly model validation	D3
Escalation bias	Disproportionate escalation rates for specific populations	Override analysis, population-level outcome tracking	D3
Feedback loop bias	Biased outputs generate biased training data for future models	Human oversight in model retraining, diverse validation sets	D3

7.3 Non-Autonomy Principles

For all regulated AI deployments, GAI-S defines a set of non-autonomy principles that must be architecturally enforced:

- No autonomous contact with external authorities or emergency services without human authorization.
- No autonomous modification of records in external systems.
- No autonomous execution of financial transactions.
- No autonomous issuance of communications on behalf of individuals or organizations.
- No autonomous execution of legal, medical, or regulatory actions.

These are architectural constraints, not policy constraints. They must be enforced by system design, not by operator instruction.

7.4 User Rights Protections

GAI-S requires that AI systems respect user rights throughout the interaction lifecycle:

- Right to disclosure: Users have the right to know they are interacting with an AI system.
- Right to explanation: Users have the right to understand the basis for AI-influenced decisions affecting them (subject to applicable law).

- Right to human review: Users have the right to request human review of consequential AI outputs.
- Right to correct: Users have the right to correct inaccurate information held by the system.
- Right to withdraw: Users have the right to disengage from AI interactions without penalty.

Section 8 Sector Application Guidance

8.1 Healthcare AI

Healthcare AI deployments operate in the highest-consequence context for GAI-S. Clinical advisory systems, diagnostic support tools, care pathway optimizers, and patient engagement platforms must achieve GAI-S Level 2 minimum, with Level 3 required for systems embedded in clinical workflows.

- Additional requirement: Business Associate Agreement (BAA) for any external model provider receiving Protected Health Information (PHI).
- Additional requirement: Clinical validation study for systems influencing clinical decisions.
- Prohibited autonomous actions include diagnosis, prescription, clinical intervention, and emergency response.
- Escalation pathways must route to licensed clinical professionals for high and critical risk classifications.

8.2 Financial Services AI

Financial services AI deployments include credit decisioning, fraud detection, algorithmic trading, customer advisory, and regulatory reporting systems. These deployments require GAI-S Level 2 at minimum, with Level 3 for systems influencing individual financial outcomes.

- Additional requirement: Model explainability documentation for credit and adverse action decisions (aligned with Equal Credit Opportunity Act, Fair Credit Reporting Act, and equivalent regulations).
- Prohibited autonomous actions include loan approval, fund disbursement, account freezing, and regulatory filings.
- Bias monitoring must include analysis across protected class proxies (age, income proxies, geographic indicators).

8.3 Legal and Professional Services AI

Legal AI deployments include document review, case research, contract analysis, regulatory compliance monitoring, and client communication support. GAI-S Level 1 minimum for internal productivity tools; Level 2 for client-facing advisory functions.

- Prohibited autonomous actions include legal advice, court filing, contract execution, and engagement letter issuance.
- Attorney review required for all AI-assisted outputs delivered to clients.
- Jurisdiction-specific bar association guidance on AI use must be incorporated into governance documentation.

8.4 Public Sector and Government AI

Government AI deployments include benefits determination, infrastructure management, public safety analytics, and citizen services. These deployments carry significant accountability implications and require GAI-S Level 2 at minimum.

- Prohibited autonomous actions include benefits denial, enforcement action, detention, and legally binding determinations.
- Transparency requirements include public disclosure of AI use in citizen-facing decisions.
- Procurement requirements must specify GAI-S certification level in AI vendor contracts.

8.5 Enterprise Operations AI

Enterprise AI deployments include human resources, supply chain optimization, customer service, internal analytics, and productivity tools. GAI-S Level 1 is appropriate for low-stakes productivity tools; Level 2 for systems influencing personnel decisions or external stakeholder interactions.

- HR and hiring AI: Level 2 required where AI influences employment outcomes. Bias monitoring across protected characteristics is mandatory.
- Customer-facing AI: Level 1 for informational chatbots; Level 2 for AI influencing purchasing, service, or financial decisions.
- Supply chain AI: Level 1 for optimization recommendations; Level 2 for autonomous procurement actions.

Section 9 Audit and Certification

9.1 Evidence-Based Certification Model

GAI-S certification is based on documented evidence, not live system demonstration. This is a foundational design requirement. Any governance standard that can only be assessed through live access is not a governance standard — it is a product demo.

The complete documentation package must enable a qualified reviewer with no prior knowledge of the system to independently assess compliance across all five domains. This is the test of documentation readiness.

9.2 Internal Audit Requirements

Level	Audit Type	Frequency	Scope	Deliverable
Level 1	Self-assessment	Annual	All five domains against Level 1 checklist	Self-assessment report
Level 2	Internal audit	Annual	All five domains, technical control testing, incident review	Internal audit report with findings
Level 3	Full internal audit	Annual	All domains, governance board effectiveness, model validation, DR test	Audit report + management response

9.3 External Review (Level 3)

Level 3 certification includes a recommendation for periodic external advisor review. External review provides independent validation of governance maturity and identifies gaps invisible to internal auditors.

- External reviewer qualifications: AI governance expertise, domain knowledge, no conflict of interest.
- Review scope: GAI-S Level 3 requirements, technical control effectiveness, governance board operations.
- Deliverable: External Assessment Report with findings and recommendations.
- Frequency: Every 2–3 years, or prior to material system changes.

9.4 Annual Attestation

Level 3 certification requires an annual signed attestation by the Compliance Officer of Record, reviewed and co-signed by the Domain Oversight Board Chair. The attestation affirms ongoing compliance across all GAI-S domains and acknowledges any open findings with documented remediation plans.

Attestation is not self-certification. It is a formal statement of compliance posture that creates institutional accountability and supports regulatory credibility.

9.5 Certification Maintenance

GAI-S certification is not a point-in-time achievement. It is an ongoing operational status that requires:

- Annual audit cycle completion.
- Governance board meeting cadence maintained.
- Model validation reports produced quarterly (Level 3).
- Incident response procedures tested at least annually.
- Documentation package updated within 30 days of material system changes.
- Annual attestation signed and filed.

Material changes to system architecture, risk classification methodology, or governance structure require a gap assessment against current certification level requirements and may require re-certification.

Section 10 Future Development

10.1 GAI-S Roadmap

Version	Target	Key Additions
v1.0 (Current)	2025	Core framework: five domains, three certification tiers, regulatory alignment
v1.1	2026 Q1	Sector-specific annex: Healthcare (GAI-S HC), Finance (GAI-S FS), Public Sector (GAI-S PS)
v1.2	2026 Q3	Agentic AI governance extension: multi-agent systems, autonomous pipeline governance
v2.0	2027	Formal third-party certification body framework, accredited auditor program

10.2 Emerging Governance Challenges

The AI governance landscape continues to evolve. GAI-S v1.0 addresses current deployment patterns, but the following areas require expanded treatment in future versions:

Agentic AI Systems

Multi-step autonomous AI pipelines executing sequences of actions with limited human checkpoints introduce governance challenges beyond the scope of single-inference advisory systems. Future GAI-S versions will define governance requirements for agentic pipelines including inter-agent authority delegation, action reversibility requirements, and aggregate risk accumulation across pipeline steps.

Foundation Model Governance

Organizations deploying AI on top of third-party foundation models face a governance dependency: their system's safety partially depends on the foundation model's alignment and safety properties. GAI-S will develop requirements for foundation model assessment, ongoing monitoring of model updates, and governance documentation for models used in production.

AI in Physical Systems

AI systems controlling physical infrastructure, robotics, autonomous vehicles, and medical devices require governance extensions that address physical consequence chains. GAI-S will develop domain-specific annexes for physical system AI with hardened non-autonomy requirements and enhanced failure mode documentation.

Cross-Jurisdictional Deployment

Organizations deploying AI across multiple jurisdictions face compounding regulatory obligations. GAI-S will develop a multi-jurisdiction compliance mapping service and model clauses for cross-border AI data processing agreements.

Section 11 Conclusion

AI governance is not a compliance cost. It is the infrastructure that makes consequential AI deployment institutionally credible, operationally defensible, and sustainably scalable.

The Governed AI Infrastructure Standard provides the first universally applicable, domain-agnostic governance architecture for AI systems. It defines what governance looks like in practice, not in principle. It specifies what needs to be built, documented, and maintained. It establishes what institutional confidence in an AI system actually requires.

GAI-S is designed to grow with the technology. Its domain structure is stable. Its certification tiers are incremental. Its documentation requirements are achievable. And its evidence-based certification model means that compliance is demonstrable — not assumed, not claimed, but documented and reviewable.

Organizations that build AI systems under GAI-S are building systems that can be reviewed, audited, challenged, and trusted.

That is the standard AI deployment requires.

James Derek Ingersoll | GodsIMiJ AI Solutions
GAI-S v1.0 | © 2026 | Enterprise Distribution

Appendix A — GAI-S Certification Checklist

Level 1 — Structured Advisory

Requirement	Domain	Evidence Type
AI role formally defined in writing	D1	Authority Boundary Document
Prohibited autonomous actions documented	D1	Authority Boundary Document
Escalation pathway documented	D1	Process Documentation
User-facing advisory disclosure	D1	UI/System Documentation
Data classification model defined	D2	Data Governance Document
Basic encryption controls implemented	D2	Technical Architecture
Access control enforced	D2	RBAC Documentation
Risk tier definitions documented	D3	Risk Matrix
Human review pathway for high-risk outputs	D3	Process Documentation
Audit logging implemented	D2, D5	Technical Architecture
Responsible AI Statement published	D5	Published Document
Architecture diagram available	D5	Technical Documentation

Level 2 — Controlled Operational Deployment

All Level 1 requirements plus:

Requirement	Domain	Evidence Type
Composite Risk Index (CRI) implemented	D3	Technical Architecture, Code

Requirement	Domain	Evidence Type
Automated escalation at CRI thresholds	D3	System Documentation
Human-in-the-loop architecturally enforced	D1, D3	System Architecture Diagram
Trust boundary diagram documented	D2	Architecture Documentation
Environment separation implemented	D4	Deployment Architecture
Dependency inventory complete	D4	Dependency Manifest
Model provider disclosure documented	D4	Transparency Documentation
Offline/fallback mechanisms implemented	D4	System Documentation
Incident response plan operational	D5	Incident Response Plan
Change management process defined	D4, D5	Change Management Documentation
Breach response protocol documented	D5	Incident Response Plan
Complete documentation package assembled	D5	Compliance Binder

Level 3 — Institutional Grade Deployment

All Level 2 requirements plus:

Requirement	Domain	Evidence Type
Governance board structure operational	D1, D5	Board Charter, Meeting Minutes
Compliance Officer of Record designated	D5	Organizational Documentation
CRI with Probability x Severity model	D3	Risk Model Documentation
Confidence score tracking implemented	D3	Technical Architecture
Drift detection monitoring operational	D3	Monitoring Documentation
Quarterly model validation process	D3	Validation Reports
False positive/negative rate tracking	D3	Performance Metrics
Bias metrics review in quarterly cycle	D3	Validation Reports
Regulatory alignment matrix documented	D5	Compliance Documentation
Business continuity plan with RTO/RPO	D4	BC/DR Plan
DR testing performed and documented	D4	Test Records
Annual internal audit completed	D5	Audit Report
Signed annual attestation on file	D5	Attestation Statement
Incident governance feedback loop	D3, D5	Governance Records

Appendix B — Glossary

Term	Definition
Agentic AI System	An AI pipeline that executes multiple actions in sequence with limited human checkpoints between steps.
Audit Trace	A structured, tamper-evident log record of a system event, user interaction, or administrative action.
Authority Separation	The structural separation between AI advisory function and human decision-making authority.
Composite Risk Index (CRI)	The product of Probability Score and Severity Score, yielding a quantitative risk assessment for AI outputs.
Compliance Officer of Record	Named individual with documented qualifications responsible for ongoing GAI-S compliance management.
Confidence Score	AI model output expressing certainty of classification or recommendation (0.0–1.0).
Deployment Containment	The set of controls ensuring AI systems operate within defined infrastructure boundaries with documented dependencies.
Drift Detection	Active monitoring for statistical shifts in risk classification distributions that may indicate model performance degradation.
Escalation	Transfer of an AI system interaction to a qualified human reviewer for assessment and disposition.
Foundation Model	A large-scale AI model trained on broad data and used as the basis for downstream applications.
GAI-S	Governed AI Infrastructure Standard — the universal governance framework defined in this document.
Governed Invocation	A model call that has passed all policy and risk evaluation steps required by the governance framework.
Human-in-the-Loop	Architectural requirement for human review before AI system outputs in high-risk categories reach end users or execute consequential actions.
Inference Boundary	The defined perimeter within which user data is processed by an AI model.
Institutional Documentation Readiness	The state in which an AI system's governance can be fully assessed by qualified reviewers using documentation alone.
Model Drift	Degradation in AI model performance over time as real-world data distributions diverge from training data.

Term	Definition
Non-Autonomy Declaration	Formal statement that an AI system has no independent decision-making authority and cannot execute consequential actions without human authorization.
Policy Engine	Rule-based system that evaluates AI outputs against defined governance policies and routes outputs accordingly.
Protected Data	Any data category requiring special handling controls including PHI, PII, financial data, and legally privileged information.
Recovery Point Objective (RPO)	Maximum acceptable data loss measured in time.
Recovery Time Objective (RTO)	Maximum time from system failure to resumption of critical functions.
Risk Score	Numerical classification (0–100 or CRI equivalent) representing assessed safety or harm risk of an AI output.
Trust Boundary	The logical or physical perimeter defining the security control scope for an AI system.
Verification Pass	A secondary AI reasoning evaluation step used to validate the quality and safety of primary model outputs.

Appendix C — Document Version History

Version	Date	Description	Status
0.1	Q3 2024	Initial framework concept — healthcare domain only	Superseded
0.2	Q4 2024	Five-domain structure formalized; Level 2 requirements defined	Superseded
0.3	Q1 2025	Quantitative risk model added; regulatory alignment introduced	Superseded
1.0	2025	Universal domain-agnostic framework; all three certification levels; full regulatory alignment; sector guidance	Current