Building Digital Trust:
A whitepaper on AI Governance at CSG

Version: 2026.2

Cloud Software Group, Inc.
851 W. Cypress Creek Road, Fort Lauderdale, Florida 33309

Cloud Software Group, Inc.
www.cloud.com

1. Executive Summary: Safety-First & Transparency-First

Cloud Software Group (CSG) is committed to providing secure, resilient, and transparent infrastructure. Our Artificial Intelligence (AI) strategy is built upon a "Safety-First" and "Transparency-First" philosophy. In alignment with our corporate AI Policy, we leverage AI for business purposes, including:

- **Operational Efficiency:** Enhancing productivity and internal workflows.
- **Product Innovation:** Delivering advanced technical optimization and administrative assistance.
- **Security & Compliance:** Bolstering infrastructure defense and regulatory monitoring.

CSG has established a robust governance program to support our products in meeting high standards of legal and ethical compliance under the EU AI Act and ISO 42001. This program serves as the cornerstone of our commitment to building and maintaining digital trust in every solution we provide.

2. About Cloud Software Group

Cloud Software Group (CSG) is a global enterprise software organization that provides cloud-based and on-premises solutions designed to enable secure application delivery, digital workspace management, and infrastructure optimization. The company operates a diverse portfolio of products and services that help organizations improve performance, scalability, and security across their IT environments. CSG's business units include Citrix, TIBCO, ArcTera, and other technology platforms that collectively serve customers across multiple industries worldwide.

Our Mission: To develop and operate secure, reliable, and compliant digital solutions that support business productivity, collaboration, and innovation while maintaining robust controls to protect customer data and meet regulatory compliance. This mission serves as the foundation for our AI Governance Framework, supporting the principle that innovation should not come at the expense of security or trust.

3. The Regulatory Landscape: EU AI Act

CSG recognizes its dual role within the global AI ecosystem:

- **As a Provider:** CSG develops and places AI systems on the market. We aim to classify these systems accurately and support the fulfillment of all transparency requirements.
- **As a Deployer:** CSG utilizes 3rd-party AI tools internally. We govern these through a specialized Internal Privacy & AI Governance Review (IPR) and rigorous vetting via risk-based framework.

3.1 Prohibited AI Practices

CSG explicitly prohibits the development, deployment, or use of AI for practices deemed unethical or illegal under the EU AI Act, including but not limited to:

- Social scoring or biometric categorization based on sensitive characteristics.

- Untargeted scraping of facial images or workplace emotion inference.
- Exploitative or deceptive techniques that bypass human consciousness.

4. Risk Classification & Intended Purpose

Under the EU AI Act, risk is determined by the Intended Purpose. CSG tools are designed as a horizontal IT Infrastructure.

4.1 Classification Triage

Based on our internal assessment, CSG features fall into:

- **Minimal Risk:** Under-the-hood features (e.g., NetScaler analytics, HDX upscaling) that optimize performance without impacting human behavior.
- **Limited Risk:** AI-powered assistants (e.g., Citrix Aidrien) that provide information or summaries, triggering transparency obligations fulfilled through clear user-facing indicators and technical documentation.

4.2 High-Risk Exclusion

CSG products are not intended for "High-Risk" use cases. Our systems are not designed for automated recruitment, credit scoring, or judicial sentencing.

5. Contextual Risk: IT vs. OT Boundaries

We distinguish between Operational Technology (OT), such as safety-critical systems running the grid or life-support, and Information Technology (IT), such as tools managing the digital network. CSG tools are IT management tools. Because our AI functions focus on technical performance rather than safety-critical operational control, they remain in non-high-risk categories even in critical infrastructure environments.

6. The Shared Responsibility Model

Compliance is a collaborative journey between CSG and its customers. To maintain the integrity and regulatory status of our solutions, we operate under a Shared Responsibility Model:

- **CSG Responsibility:** CSG focuses on "Safety by Design," providing the technical guardrails and transparency indicators necessary to support compliant use. We maintain the formal classification justifications for our systems to support our regulatory posture and internal compliance audits.
- **Customer Responsibility:** Customers manage the "Context of Use." To support the intended technical purpose of the infrastructure, customers are responsible for ensuring tools are not repurposed for prohibited or high-risk activities. It is important to note that under the EU AI Act, a significant modification to the intended purpose of a system may result in a change to its regulatory classification, potentially shifting additional "Provider" obligations to the deployer.

7. Human-in-the-Loop (HITL) Principle

A cornerstone of CSG governance is the requirement that AI does not have the authority to take final

operational, legal, or administrative actions. Final authority rests with a human administrator. This approach supports the role of technology as a service to human expertise and is a key technical control mapped across our compliance frameworks to mitigate automation bias.

8. AI Governance & Lifecycle Management

CSG maintains an AI Management System (AIMS) aligned with ISO 42001 to facilitate that AI is managed throughout its entire lifecycle from design and procurement to deployment and periodic review.

8.1 Cross-Functional Oversight

AI governance is a shared responsibility across the organization. Our dedicated AI Governance Committee includes stakeholders from Legal & Privacy, Product Security, Information Security, IT, and Procurement.

8.2 Data Governance Rules

Cloud Software Group (CSG) maintains a formal information governance program and specific data handling standards to manage and protect its information assets. We apply strict data handling tiers to AI development and deployment:

- **Confidential Information:** Prohibited from being used to train any AI model.
- **Customer Data:** Only utilized with explicit contractual or legal instruction.
- **Synthetic Data:** Preferred for model training, POCs, and testing to maximize privacy.

8.3 Security & Privacy Credentials

CSG's AI governance is anchored in a mature, global foundation of security and privacy excellence. Our platforms and infrastructure maintain industry-recognized certifications, including:

- **Security Frameworks:** ISO/IEC 27001 (Information Security), ISO/IEC 27017 (Cloud Security), and SOC 2 Type II reports.
- **Privacy Frameworks:** ISO/IEC 27018 (PII Protection) and ISO/IEC 27701 (Privacy Information Management).

For further information on our global certifications, visit the Cloud Software Group Trust Center.

8.4 Product Security & Technical Integrity

The security of our AI features is integrated directly into the product lifecycle through the CSG Product Security program to support technical integrity:

- **Secure Development (SSDL):** Features are subject to design-phase security reviews, threat modeling, and automated scanning.
- **Vulnerability Management:** Proactive 24/7 monitoring, internal audits, and a coordinated disclosure program.
- **Responsible Patching:** Standardized processes for efficient release of security updates.

For more details on our security practices and foundational SDLC, visit the CSG Product Security page

and our Secure Software Development Lifecycle documentation.

8.5 Integrated Control Framework & Common Mapping

To support efficient and comprehensive compliance across numerous audit cycles, CSG employs a unified control framework mapped to multiple regulatory requirements:

- **Common Control Mapping:** Rather than managing siloed compliance requirements, CSG utilizes a set of common controls that map across the EU AI Act, ISO 42001, SOC 2, and various ISO standards. This facilitates the use of a single validated safeguard to satisfy multiple regulatory and audit demands simultaneously.
- **Governance Controls:** Corporate AI policies and mandatory AI literacy training to establish an ethical cultural baseline.
- **Operational Controls:** Mandatory Risk Triage gates and risk-based vendor vetting.
- **Monitoring & Response Controls:** Periodic audits of justifications, technical monitoring, and established incident response procedures to remediate potential AI performance anomalies.

9. Conclusion: Empowering Secure Innovation

Building digital trust is an ongoing journey that requires transparency, accountability, and technical rigor. As Artificial Intelligence continues to redefine the digital landscape, Cloud Software Group remains steadfast in its commitment to providing the secure, reliable, and transparent foundations upon which modern enterprises thrive. By uniting the specialized capabilities of Citrix, TIBCO, and Arctera under a single, rigorous AI Governance Framework, we provide our customers with a unified approach to trust and compliance.

CSG aims to evolve its governance practices alongside global regulations and industry standards. Through our ongoing alignment with ISO 42001 and the EU AI Act, we empower our customers to embrace AI with confidence, supported by a framework built on transparency, technical integrity, and the enduring principle of human-in-the-loop oversight. We believe that by fostering this foundation of digital trust, we enable our customers to innovate safely and effectively in the age of AI.

For further information, technical documentation, and the latest updates on our compliance posture, please visit the Cloud Software Group Trust Center.

Appendix A: Frequently Asked Questions (FAQ)

A.1 General AI Strategy

Q: What is Cloud Software Group's approach to AI?

A: CSG (Citrix, TIBCO, and Arctera) follows a Safety-First and Transparency-First AI strategy. Our AI features are designed to optimize infrastructure, enhance security, and provide administrative assistance. We operate under a "Shared Responsibility Model" where we provide secure, transparent tools, and the customer manages the final business use cases.

A.2 Regulatory Foundations

Q: What is the EU AI Act, and what is its scope?

A: The EU AI Act is a comprehensive legal framework aimed at ensuring AI systems used in the EU that are safe, transparent, and respect fundamental rights. It applies to developers and users of AI systems placed on the market or used within the EU.

Q: What is the difference between the EU AI Act and ISO 42001?

A: The EU AI Act is a mandatory regulation that dictates requirements based on risk levels. ISO 42001 is a voluntary international standard providing a framework for an Artificial Intelligence Management System (AIMS). CSG uses ISO 42001 to demonstrate the maturity of its AI governance.

A.3 Shared Responsibility & Risk

Q: From a "shared responsibility" perspective, how is CSG supporting customer obligations?

A: Compliance is a joint effort. CSG supports customers by providing foundational transparency, classification evidence, and administrative controls. While CSG secures the technology and defines its intended purpose, customers retain final control over how AI is deployed and governed within their specific environment.

Q: Does the customer's specific use case change the risk level?

A: Yes. Risk classification depends heavily on the context of use. While CSG provides tools as Minimal or Limited Risk for infrastructure tasks, customers are responsible for managing their implementation to avoid triggering high-risk obligations.

A.4 EU AI Act Compliance (The "High-Risk" Question)

Q: Are CSG products considered "High-Risk" under the EU AI Act?

A: No. Based on internal assessments, CSG features are classified as Limited Risk (e.g., AI assistants with transparency labels) or Minimal Risk (e.g., backend performance optimizations). They are not intended for high-risk use cases such as recruitment, creditworthiness evaluation, or safety-critical

infrastructure control.

Q: Why aren't CSG systems classified as High-Risk?

A: Our systems perform narrow functions such as technical optimization and administrative assistance. They do not replace safety mechanisms and do not possess the authority to make final decisions that impact fundamental rights.

A.5 Lifecycle & Governance

Q: How does CSG manage the risk of new features becoming "High-Risk" later?

A: We utilize a mandatory Risk Triage Procedure for all new releases. Additionally, we conduct periodic reviews of our AI justifications to support the accuracy of our classifications as technology and regulations evolve.

Q: How does CSG vet the third-party AI vendors it uses?

A: We perform rigorous due diligence via risk-based framework and conduct periodic audits on vendor AI assessments to verify compliance with safety and transparency standards.

A.6 Operational Controls

Q: Can the AI make final decisions or take actions automatically?

A: No. All CSG AI features follow a "Human-in-the-Loop" principle. The systems provide technical insights or suggestions, but do not have the authority to make final operational or administrative decisions. Final authority rests with the human administrator.

Q: Can AI features be disabled?

A: CSG provides varying levels of administrative control depending on the product. Many AI features are designed as opt-in or can be managed via policy settings. For definitive guidance on a specific feature, refer to the relevant technical product documentation.

Appendix B: References

For detailed information regarding the regulatory frameworks mentioned in this whitepaper, please refer to the following official resources:

- **EU AI Act (Regulation (EU) 2024/1689):** Official Journal of the European Union Text
- **ISO/IEC 42001:2023 Standard:** Information technology — Artificial intelligence — Management system
- **ISO/IEC 27001 Standard:** Information security, cybersecurity and privacy protection
- **NIST AI Risk Management Framework:** AI RMF 1.0