Building Digital Trust :

A Whitepaper on AI Governance at Cloud Software Group

Table of contents

1. Executive Summary: AI Governance & Design Integrity 3
2. About Cloud Software Group 3
3. The Regulatory Landscape: EU AI Act 3
3.1 Prohibited AI Practices 3
4. Risk Classification & Design Purpose 4
4.1 Classification Triage 4
4.2 High-Risk Exclusion 4
5. The Shared Responsibility Model 4
6. Human Oversight 4
7. AI Governance & Lifecycle Management 5
7.1 Cross-Functional Oversight 5
7.2 Data Governance Rules 5
7.3 Security & Privacy Credentials 5
7.4 Product Security & Technical Integrity 5
7.5 Integrated Control Framework & Common Mapping 6
8. Conclusion: Empowering Secure Innovation 6
Appendix A: Frequently Asked Questions (FAQ) 7
A.1 General AI Strategy 7
A.2 Shared Responsibility & Risk 7
A.3 EU AI Act Compliance (The "High-Risk" Question) 7
A.4 Lifecycle & Governance 7
A.5 Operational Controls 8
Appendix B: References 9

1. Executive Summary: AI Governance & Design Integrity

Cloud Software Group (the “Company”, “we”, “us”, “our”) is committed to providing secure, resilient, and enterprise-grade infrastructure. Our Artificial Intelligence (AI) strategy is built upon a risk-based governance framework focused on technical integrity and a shared responsibility model. In alignment with our corporate AI Policy, we leverage AI for defined technical purposes, including:

- **Operational Efficiency:** Enhancing productivity and internal workflows.
- **Technical Optimization:** Delivering advanced performance insights and administrative assistance.
- **Security & Resilience:** Bolstering infrastructure defense and security monitoring.

The Company has established a robust governance program to support compliance with applicable requirements of the EU AI Act and align with the ISO 42001 standard. This program serves as the foundation of our commitment to building and maintaining trust across our AI solutions.

2. About Cloud Software Group

Cloud Software Group 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. The Company’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

The Company recognizes its dual role within the global AI ecosystem:

As a Provider: The Company develops and delivers products with AI-enabled functionality. We support our customers' compliance efforts by providing the necessary technical documentation regarding the product’s design purpose and AI capabilities.
As a Deployer: The Company utilizes 3rd-party AI tools internally. We govern these through the use of an Internal Privacy Review (IPR), which includes a section dedicated to AI governance and rigorous vetting via a risk-based framework.

3.1 Prohibited AI Practices

The Company maintains strict governance standards that prohibit the development or deployment of AI systems for practices deemed to carry 'unacceptable risk' under the EU AI Act. These include but are not limited to:

- Social scoring or biometric categorization based on sensitive characteristics.
- Untargeted scraping of facial images or workplace emotion inference.
- Deceptive data collection or processing.

4. Risk Classification & Design Purpose

4.1 Classification Triage

Based on our internal assessment, the AI-enabled features within our products are categorized as follows under the EU AI Act:

- **Minimal Risk:** The underlying architecture (e.g., NetScaler analytics, HDX upscaling) that optimizes technical performance and infrastructure efficiency.
- **Limited Risk:** AI-powered assistants (e.g., Citrix Aidrien) that provide information or summaries. For these features, we provide technical documentation to support the customer's understanding of AI's role and intended output and provide context for the customer to review and validate the results.

4.2 High-Risk Exclusion

Based on internal assessments, features in Company products are classified as Minimal or Limited Risk. Our products are not designed for high-risk use cases such as recruitment, creditworthiness evaluation, or safety-critical infrastructure control.

5. The Shared Responsibility Model

We operate under a Shared Responsibility Model:

Company Responsibility: We provide our customers with product documentation, such as AI data sheets and technical documentations, that detail the AI components and models integrated into our products. Our features are built to provide administrators with controls to configure, enable or disable AI-assisted capabilities. This ensures that the customers retain full control over where and how AI is utilized within their environment to meet their needs.

Customer Responsibility: Customers manage the context of use. To support the designed technical purpose of the infrastructure, customers are responsible for ensuring tools are not repurposed for prohibited or high-risk activities.

6. Human Oversight

We design our AI-assisted features to function as assistive tools that provide recommendations and insights for human review. These features are not designed for fully autonomous decision-making in safety-critical or high-risk contexts. By providing administrators with the ability to configure these features and providing users with the underlying data insights, we enable our customers to exercise their own professional judgment and maintain operational control over AI-generated outputs.

7. AI Governance & Lifecycle Management

The Company's AI Governance follows the core principles of ISO 42001. We manage AI as a continuous lifecycle, incorporating risk management and periodical reviews into our development and procurement processes. As of the release of this document, the Company has not performed an ISO 42001 audit for its AI governance program.

7.1 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.

7.2 Data Governance Rules

The Company maintains a formal information governance program and data handling standards to manage and protect its information assets. We apply strict data handling tiers to AI development and deployment:

- **Cloud Software Group Confidential Information:** Protected by policy and controls from being used in AI training to ensure that proprietary or sensitive assets are not incorporated into a model's permanent knowledge base.
- **Customer Data:** Processed only where contractually and legally permitted, or upon explicit customer instruction.
- **Synthetic Data:** Leveraged for training, testing, and proof-of-concepts where appropriate to reduce the reliance on sensitive datasets.

7.3 Security & Privacy Credentials

Our AI governance is anchored in a mature security and privacy foundation. Our platforms and infrastructure maintain industry-recognized certifications, including:

- **Security Frameworks:** ISO/IEC 27001 (Information Security), ISO/IEC 27017 (Cloud Security), and AICPA's Trust Services Criteria (TSC), on which SOC 2 Type II reports are based.
- **Privacy Frameworks:** ISO/IEC 27018 (PII Protection) and ISO/IEC 27701 (Privacy Information Management).

For further information on our security and privacy certifications, visit the Cloud Software Group Trust Center.

7.4 Product Security & Technical Integrity

The security of our AI features is integrated directly into the product lifecycle through the Company's Product Security program:

- **Secure Software Development Life Cycle (SSDLC):** 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 Cloud Software Group Product Security page and our Secure Software Development Lifecycle documentation.

7.5 Integrated Control Framework & Common Mapping

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

- **Common Control Mapping:** Rather than managing siloed compliance requirements, we utilize a set of common controls that map across the ISO 42001, SOC2, and the ISO 27001 frameworks. This facilitates the use of a single validated safeguard.
- **Governance Controls:** Corporate AI policies and mandatory AI literacy training establish a consistent baseline for our personnel.
- **Operational Controls:** Mandatory Risk Triage gates and risk-based vendor vetting.
- **Monitoring & Response Controls:** Periodic audits, technical monitoring, and established incident response procedures to remediate potential AI anomalies.

8. Conclusion: Empowering Secure Innovation

Cloud Software Group provides the foundations for modern enterprises to deploy AI with confidence. By uniting the specialized capabilities of Citrix, TIBCO, and Arctera under a single AI governance framework, we offer a unified approach to digital trust. We continue to evolve our practices by using ISO 42001 and ISO 27001 as guiding frameworks for our internal standards, ensuring our approach is built on technical integrity and the principle of human oversight. 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: Our approach to AI is grounded in secure-by-design principles and a shared responsibility model. The AI features in our products are engineered for specific purposes, such as optimizing infrastructure, enhancing security, and providing administrative assistance. We provide a secure technical foundation and the documentation necessary for informed use, while the customer retains control over the final business use cases and deployment context.

A.2 Shared Responsibility & Risk

Q: From a "shared responsibility" perspective, how is Cloud Software Group supporting customer obligations?

A: We support our customers by providing technical documentation and administrative controls. While we secure the technology and define its design purpose, customers retain final oversight and control over how AI is configured and governed within their specific environments.

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

A: The risk classification of our products is based on their design purpose as defined in our documentation. We provide our products for functions primarily focused on IT infrastructure and administrative support, which are assessed as Minimal or Limited Risk. While this risk assessment is based on the product's designed use, a customer acting as a Deployer who chooses to utilize the tool for a purpose outside of that defined scope is responsible for any additional obligations under the EU AI Act.

A.3 EU AI Act Compliance (The "High-Risk" Question)

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

A: Based on internal assessments, features in Company products are classified as Limited Risk (e.g., AI assistants with information or summaries) or Minimal Risk (e.g., backend performance and security optimizations). Our products are not designed for high-risk use cases such as recruitment, creditworthiness evaluation, or safety-critical infrastructure control.

Q: Why aren't Cloud Software Group systems classified as High-Risk?

A: Our AI features are specifically engineered for technical functions, such as infrastructure optimization and administrative assistance. This focused architecture is designed to provide insights rather than make autonomous decisions, ensuring that all outputs remain subject to human oversight. By maintaining this distinction, we ensure that the final review and decision-making control always remain with the customer.

A.4 Lifecycle & Governance

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

A: We utilize a mandatory risk assessment procedure for all new AI-enabled features during the development lifecycle. Additionally, we conduct periodic reviews of our risk classification to ensure they remain aligned with our design purpose and established AI governance standards as technology evolves.

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

A: We perform rigorous due diligence through a risk-based framework. This includes assessing vendor AI practices and security controls to verify alignment with our internal security and data privacy requirements.

A.5 Operational Controls

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

A: Our AI features are engineered to provide technical insights and recommendations rather than function as autonomous agents. These features are designed to serve as decision-support tools that deliver data summaries for human review within the administrator's workflow, ensuring the customer retains full control over any final actions.

Q: Can AI features be disabled?

A: We provide administrative controls that allow for the management of AI-enabled features according to customer needs. Depending on the product, these features are designed as opt-in or can be configured via policy settings. For definitive guidance on a specific feature and its configuration options, please refer to the relevant technical product documentation.

Appendix B: References

For detailed information regarding the regulation, standards and 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:** NIST AI RMF 1.0