Control Framework & Mapping

Artificial Intelligence Controls Matrix (AICM Bundle)

Release Date: July 10, 2025

CSA cloud security alliance®

AICM™

AI Controls Framework Working Group

Introducing the AI Controls Matrix (AICM)

A Framework for Secure and Trustworthy AI Systems in the Cloud

AI Controls Matrix: Built on Proven Principles, Tips, and Tricks (built on upcoming CCM v4.1 (up to June 2025))

An approach that can offer a solid, robust, understandable, and measurable “outcomes”.

AI Controls Matrix = Control objectives framework, to support organizations develop, implement and use AI technologies in a secure and responsible way.

AI Controls Matrix (AICM) Structure

A Framework for Secure and Trustworthy AI Systems in the Cloud

AICM = *First vendor-agnostic framework for AI security & governance.*

Helps organizations:

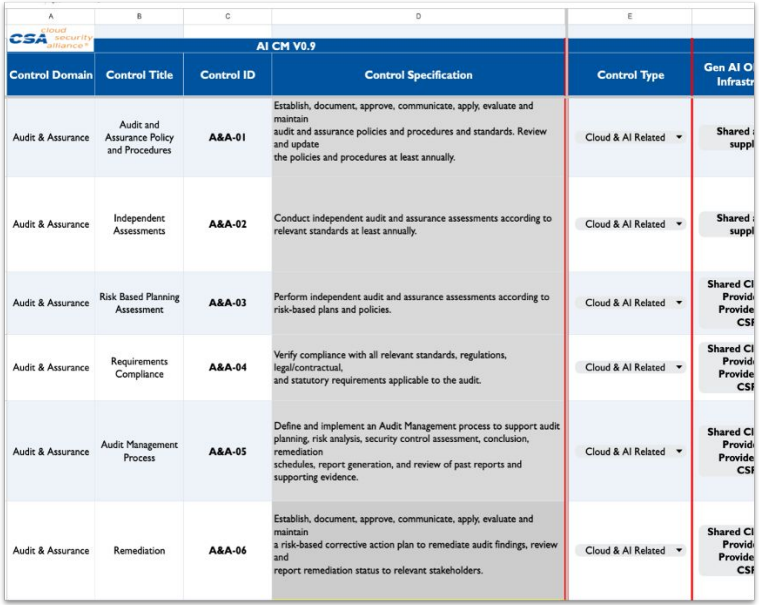
- Assess and manage AI-specific risks
- Build **trustworthy AI systems**
- Align with international standards (ISO, NIST, BSI, etc.)

Developed by **CSA and industry experts**.

The AI Controls Matrix – AICM

A Framework for Secure and Trustworthy AI Systems in the Cloud

- Developed by AI Controls Working Group
- Built on the foundation of the Cloud Control Matrix (CCM) (built on current CCM v4.0.13 and upcoming CCM v4.1 (AICM and CCM v4.1 have been synchronized up to June 2025. When CCM v4.1 is published in 2026 another AICM synchronization will follow)))
- Open
- Expert-driven
- Consensus-based
- Vendor-agnostic



Control Domain	Control Title	Control ID	Control Specification	Control Type	Gen AI O… Infrastr…
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Cloud & AI Related	Shared … suppl…
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Cloud & AI Related	Shared … suppl…
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	Cloud & AI Related	Shared Cl… Provid… Provide… CSP
Audit & Assurance	Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Cloud & AI Related	Shared Cl… Provid… Provide… CSP
Audit & Assurance	Audit Management Process	A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Cloud & AI Related	Shared Cl… Provid… Provide… CSP
Audit & Assurance	Remediation	A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	Cloud & AI Related	Shared Cl… Provid… Provide… CSP

AI Controls Matrix (AICM) Structure

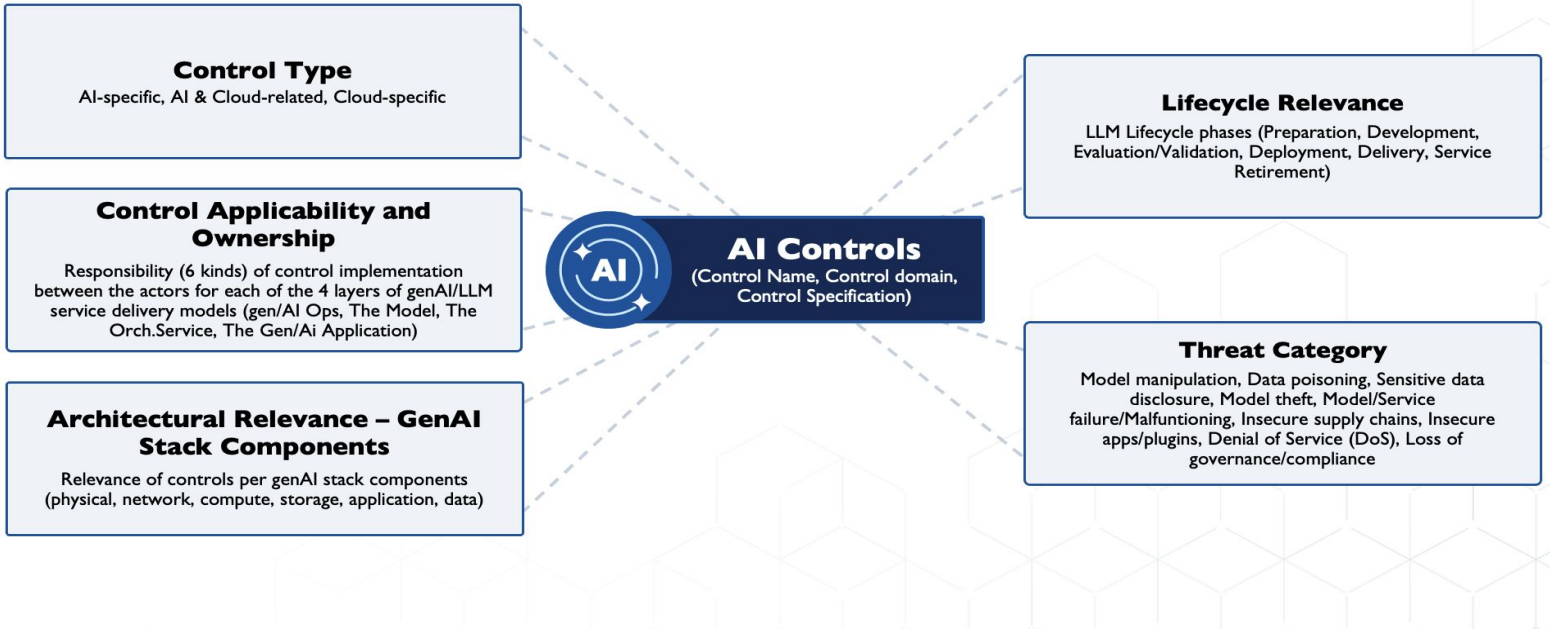
A Framework for Secure and Trustworthy AI Systems in the Cloud

A&A	Audit & Assurance
AIS	Application & Interface Security
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control & Configuration Management
CEK	Cryptography, Encryption & Key Management
DCS	Datacenter Security
DSP	Data Security & Privacy
GRC	Governance, Risk Management & Compliance
HRS	Human Resources Security
IAM	Identity & Access Management
IPY	Interoperability & Portability
I&S	Infrastructure Security
LOG	Logging & Monitoring
MDS	Model Security
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management
UEM	Universal EndPoint Management

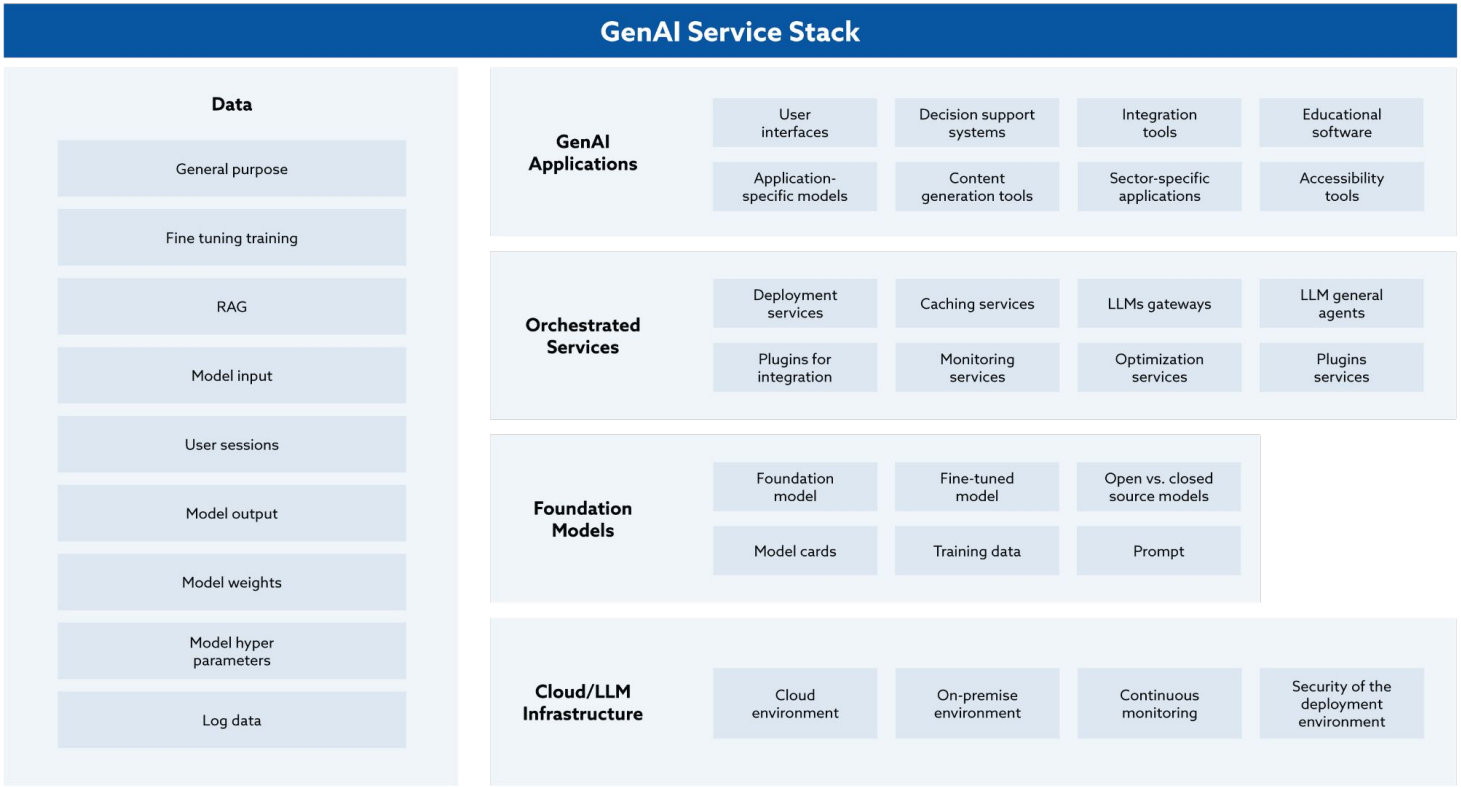
18 Security Domains, Containing 243 Control Objectives

AI Controls Matrix (AICM) Architecture

A Framework for Secure and Trustworthy AI Systems in the Cloud

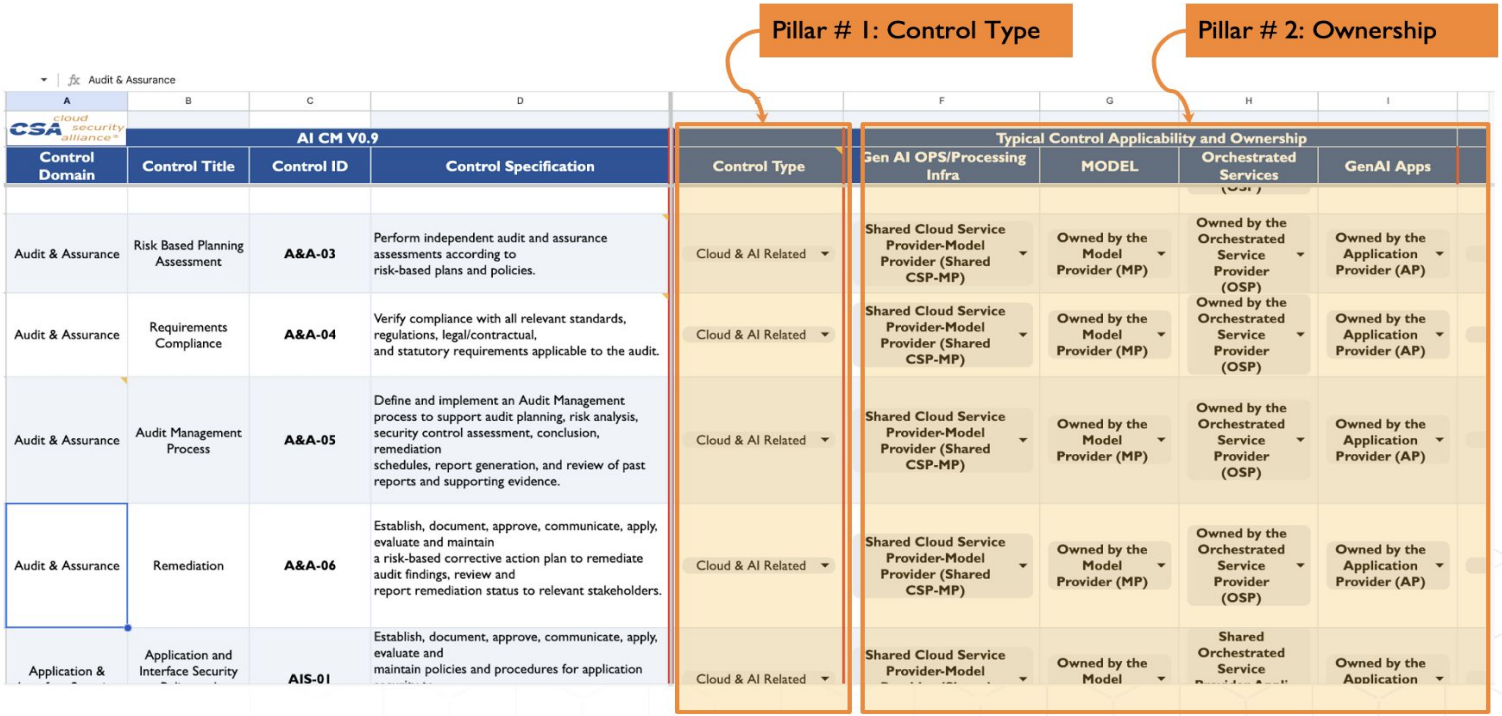


AICM Scope


GenAI Service Stack
Data
General purpose
Fine tuning training
RAG
Model input
User sessions
Model output
Model weights
Model hyper parameters
Log data
GenAI Applications
User interfaces
Decision support systems
Integration tools
Educational software
Application-specific models
Content generation tools
Sector-specific applications
Accessibility tools
Orchestrated Services
Deployment services
Caching services
LLMs gateways
LLM general agents
Plugins for integration
Monitoring services
Optimization services
Plugins services
Foundation Models
Foundation model
Fine-tuned model
Open vs. closed source models
Model cards
Training data
Prompt
Cloud/LLM Infrastructure
Cloud environment
On-premise environment
Continuous monitoring
Security of the deployment environment

AI Controls Matrix (AICM) Architecture (2)

A Framework for Secure and Trustworthy AI Systems in the Cloud



AI Controls Matrix (AICM) Architecture (3)

A Framework for Secure and Trustworthy AI Systems in the Cloud

Pillar # 3: Arch Relevance

A	B	C	D	J	K	L	M	N	O
CSA cloud security alliance	AI CM V0.9			Architectural Relevance - GenAI Stack Components					
Control Domain	Control Title	Control ID	Control Specification	Phys	Network	Compute	Storage	App	Data
Governance, Risk and Compliance	AI Impact Assessment	GRC-11	Relevant stakeholders an ongoing AI Impact Assessment process that evaluates the ethical, societal, operational, legal, and security impacts of the AI system throughout its lifecycle.	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE
Governance, Risk and Compliance	Bias and Fairness Assessment	GRC-12	Regularly evaluate AI systems, models, datasets & algorithms for bias and fairness to ensure compliance with ethical standards.	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE
Governance, Risk and Compliance	Ethics Committee	GRC-13	Establish an ethics committee to review AI applications, ensuring alignment with ethical standards and organizational values.	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE
Governance, Risk and Compliance	Explainability Requirement	GRC-14	Establish, document, and communicate the degree for the AI Services.	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE
Governance, Risk and Compliance	Explainability Evaluation	GRC-15	Evaluate, document, and communicate the degree explainability of the AI Services, including possible and exceptions.	FALSE	TRUE	TRUE	TRUE	TRUE	TRUE

AI Controls Matrix (AICM) Architecture (4)

A Framework for Secure and Trustworthy AI Systems in the Cloud

Pillar # 4:Lifecycle Relevance

A	B	C	D	P	Q	R	S	T	U		
CSA cloud security alliance	AI CM V0.9			Lifecycle Relevance							
Control Domain	Control Title	Control ID	Control Specification	Preparation	Development	Evaluation/Validation	Deployment	Delivery	Service Retirement		
Governance, Risk and Compliance	AI Impact Assessment	GRC-11	Establish, document, and communicate to all relevant stakeholders an ongoing AI Impact Assessment process that evaluates the ethical, societal, operational, legal, and security impacts of the AI system throughout its lifecycle.	Team and e…	Guardrails	Evaluation Validation/Red …	Orchestration AI Services …	Operations Maintenance Continuous … Continuous …	Archiving Data deletion Model disposal		
Governance, Risk and Compliance	Bias and Fairness Assessment	GRC-12	Regularly evaluate AI systems, models, datasets & algorithms for bias and fairness to ensure compliance with ethical standards.	Team and e…	Guardrails	Evaluation Validation/Red … Re-evaluation	AI applicati… Orchestration	Operations Maintenance Continuous … Continuous …	Data deletion Archiving		
Governance, Risk and Compliance	Ethics Committee	GRC-13	Establish an ethics committee to review AI applications, ensuring alignment with ethical standards and organizational values.	Team and e…	Guardrails	Evaluation Validation/Red …	Orchestration AI Services …	Operations Maintenance Continuous … Continuous …	Archiving Data deletion Model disposal		
Governance, Risk and Compliance	Explainability Requirement	GRC-14	Establish, document, and communicate the degree for the AI Services.	Data collecti… Data curation Data storage Team and e…	Design Training Guardrails Supply Chain	Evaluation Validation/Red … Re-evaluation	Orchestration AI Services … AI applicati…	Operations Maintenance Continuous … Continuous …	Archiving Data deletion Model disposal		
Governance, Risk and Compliance	Explainability Evaluation	GRC-15	Evaluate, document, and communicate the degree explainability of the AI Services, including possible and exceptions.	Data collecti… Data curation Data storage	Design Training Guardrails	Evaluation Validation/Red … Re-evaluation	Orchestration AI Services … AI applicati…	Operations Maintenance Continuous …	Archiving Data deletion Model disposal		

AI Controls Matrix (AICM) Architecture (5)

Pillar # 5:Threat Category

AICM V0.9				Threat Category								
Control Domain	Control Title	Control ID	Control Specification	Model manipulation	Data poisoning	Sensitive data disclosure	Model theft	Model/Service Failure/Malfunctioning	Insecure supply chain	Insecure apps/plugins	Denial of Service (DoS)	Loss of governance/compliance
Audit & Assurance	Audit and Assurance Policy and Procedures	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Audit & Assurance	Independent Assessments	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Audit & Assurance	Risk Based Planning Assessment	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	TRUE
Audit & Assurance	Requirements Compliance	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Audit & Assurance	Audit Management Process	A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
Audit & Assurance	Remediation	A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE

AI Controls Matrix (AICM) Example

•**Control Description:** Conduct independent audit and assurance assessments to evaluate compliance, risk mitigation, and overall security across AI systems.

How This Control Aligns with Values in Columns:

1.Control Type: Cloud & AI Related: This control specifically addresses aspects relevant to cloud and AI infrastructure, making it applicable to these domains.

2.Applicability and Ownership: GenAI OPS/Processing Infra: Shared responsibility among the Cloud Service Provider (CSP), Model Provider (MP), and Application Provider (AP).

Owned by the Model Provider (MP), **Orchestrated Service Provider (OSP)**, and **Application Provider (AP)**. This ensures accountability across key stakeholders involved in AI system operations.

3.Architectural Relevance: The control is relevant to **Physical Infrastructure**, **Network**, **Compute**, **Storage**, **Application**, and **Data** layers of the GenAI stack, ensuring comprehensive security coverage.

4.Lifecycle Alignment:

1. The control applies to multiple stages in the AI lifecycle:
    1. **Preparation:** Addresses risks in data collection, curation, and storage.
    2. **Development:** Ensures secure design, training, and guardrails.
    3. **Evaluation/Validation:** Requires independent assessment during evaluation, validation, and red-teaming phases.
    4. **Deployment:** Includes supply chain security, application monitoring, and orchestration.
    5. **Service Retirement:** Covers data deletion, model disposal, and archiving.

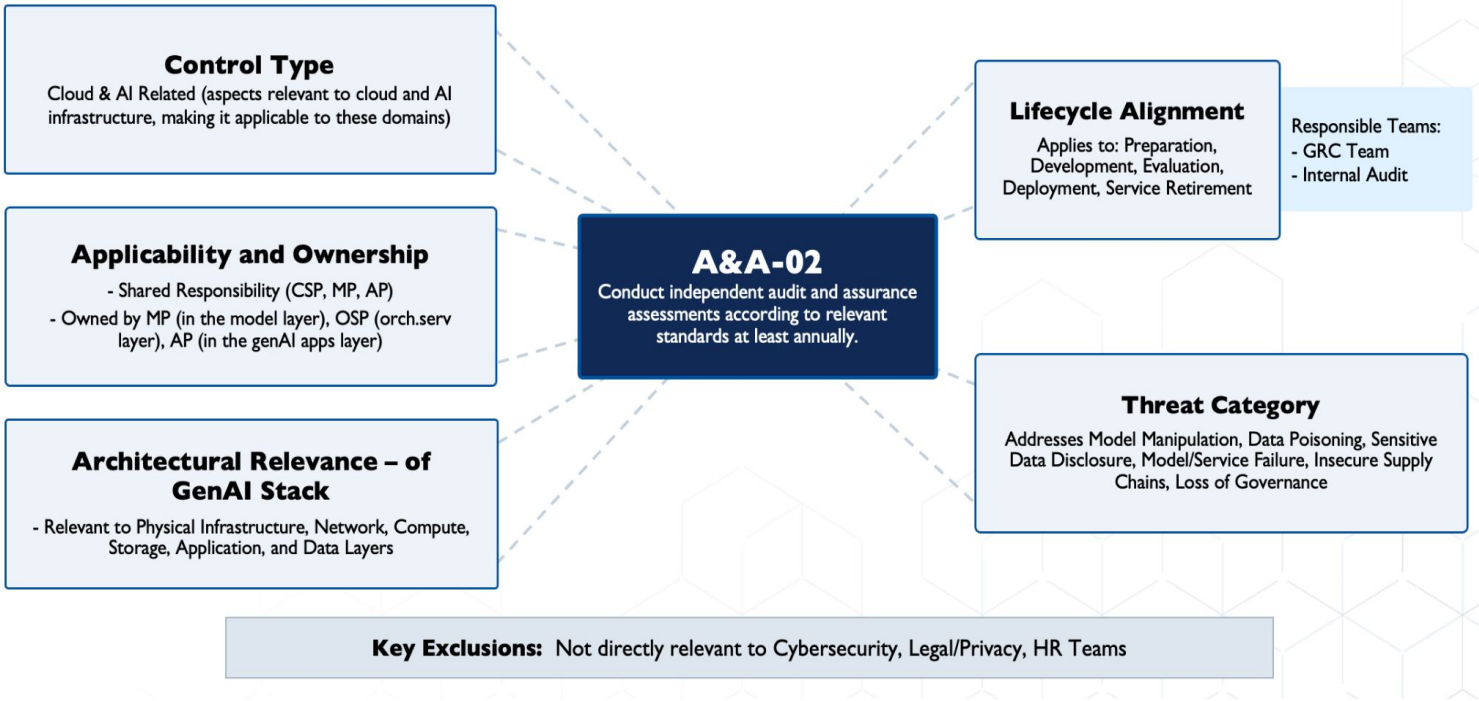
2.Responsible Teams:

1. **GRC Team**: Governance, risk, and compliance teams are responsible for overseeing independent assessments.
2. **Internal Audit Teams**: Perform detailed compliance reviews.

5.Threat Mitigation:

1. Mitigates specific risks such as:
    1. **Model Manipulation**
    2. **Data Poisoning**
    3. **Sensitive Data Disclosure**
    4. **Model/Service Failure or Malfunction**
    5. **Insecure Supply Chains**
    6. **Loss of Governance/Compliance**

AI Controls Matrix (AICM) Control Example: A&A-02 (Independent Assessments)



AI Controls Matrix (AICM) Bundle

Published

- Control Objectives to Mitigate Threats - Control Matrix (Relevance, Applicability, etc)
- Consensus Assessment Initiative Questionnaire for AI (AI-CAIQ)
- Mapping to the BSI AIC4 Catalog
- Mapping to NIST AI 600-1 (2024)

Peer Reviewed (or Currently in Peer Review)

- Mapping to ISO 42001
- Implementation Guidelines

In Progress (Releasing Soon)

- Mapping to EU AI Act
- Auditing Guidelines

AI Controls Matrix (AICM) Bundle (2)

(to be completed by the Implementation and Auditing Guidelines in August 2025. Please see previous slide)

Download the Paper

https://cloudsecurityalliance.org/artifacts/ai-controls-matrix