

ODA3 INSTITUTE

CROSSWALK

GAISSF™—CSA Cloud Controls Matrix Mapping

Cloud Security Alignment Crosswalk — CSA CCM v4.1

GAISSF-CRO-034 | Informative crosswalk | Draft for Publication

Version 1.0 | Updated 6 October 2026

© 2026 ODA3 Pvt Ltd

Document Control

Field	Controlled Value
Document ID	GAISSF-CRO-034
Title	GAISSF–CSA Cloud Controls Matrix Mapping
Version	1.0
Classification	Informative domain-level crosswalk / public
Publisher	ODA3 Institute
GAISSF baseline	GAISSF™ v1.0; 59 controls / 9 domains; Applicable-Control Baseline = 52 D1-D8 + applicable D9
External baseline	CSA CCM v4.1 / CAIQ v4.1; released 27 January 2026
Mapping unit	GAISSF control to CCM security domain
Publication status	Draft for Publication
Verification date	6 October 2026
Distribution	Public — docs.oda3.org / official ODA3 publication channels
Status	Draft for Publication
Updated	6 October 2026

Reliance and Attribution Notice

This crosswalk is an interpretive mapping aid. It does not establish CSA endorsement, STAR listing, STAR certification or attestation, CAIQ acceptance, control implementation, operating effectiveness, or equivalence between GAISSF and CCM. Cloud Security Alliance, CCM, CAIQ and STAR names and marks remain the property of their respective owners.

Executive Summary

GAISSF-CRO-034 maps all 59 GAISSF™ v1.0 controls to the 17 security domains of CSA Cloud Controls Matrix (CCM) v4.1. The register contains 281 domain-level mapping records. CSA CCM v4.1 contains 207 controls across 17 domains, and CAIQ v4.1 contains 283 assessment questions. The GAISSF Applicable-Control Baseline is all 52 controls in D1-D8 plus D9 where Physical AI or cyber-physical actuation is in scope.

The strongest domain-level relationships occur in Governance, Risk Management & Compliance; Data Security & Privacy; Application & Interface Security; Logging & Monitoring; Security Incident Management; Supply Chain Management; and Threat & Vulnerability Management. These relationships are directional analytical correspondences only; they do not establish coverage of individual CCM control specifications, CAIQ responses, shared-responsibility allocations, STAR submissions, evidence sufficiency, or operating effectiveness.

1. Purpose and Intended Use

- Support cloud-security gap analysis for AI systems and AI-enabled cloud services.
- Identify where GAISSF evidence may support CCM implementation activities.
- Help allocate control ownership among cloud service providers, customers and other supply-chain actors.
- Provide a controlled starting point for a future control-specification-level crosswalk.

2. Scope and Baseline

The controlling GAISSF sources are GAISSF-NOR-001 v1.0 and GAISSF-NOR-004 v1.0. The external baseline is CSA CCM v4.1, released 27 January 2026. CSA describes CCM v4.1 as 207 controls across 17 domains; CAIQ v4.1 contains 283 questions aligned to those controls.

3. Mapping Methodology

Each GAISSF control was decomposed by intended outcome and mapped to materially related CCM v4.1 domains. Relationship classifications are Strong Partial, Partial or Supporting unless a stronger conclusion is directly defensible. Because this is a domain-level crosswalk, no relationship code means equivalence, implementation of a CCM control, evidence sufficiency, STAR readiness, or automatic conformance.

Code	Meaning
SP	Strong partial: substantial shared outcome but material cloud-specific elements remain.
P	Partial: meaningful overlap with narrower or different scope.
S	Supporting: assists implementation but does not directly satisfy the

Code	Meaning
	domain.
C	Contextual only.
N	No material mapping.
O	Outside scope.
U	Unable to determine.

4. CCM Domain Coverage

Domain	Title	Mapped GAISSF controls	Mapping records	Coverage
A&A	Audit & Assurance	12	12	Partially Addressed
AIS	Application & Interface Security	28	28	Partially Addressed
BCR	Business Continuity Management & Operational Resilience	14	14	Partially Addressed
CCC	Change Control & Configuration Management	9	9	Partially Addressed
CEK	Cryptography, Encryption & Key Management	0	0	Not Addressed
DCS	Datacenter Security	7	7	Partially Addressed
DSP	Data Security & Privacy	22	22	Partially Addressed
GRC	Governance, Risk Management & Compliance	37	37	Partially Addressed
HRS	Human Resources Security	5	5	Partially Addressed
IAM	Identity & Access Management	18	18	Partially Addressed
IPY	Interoperability & Portability	7	7	Partially Addressed
IVS	Infrastructure & Virtualization Security	13	13	Partially Addressed
LOG	Logging & Monitoring	43	43	Partially Addressed
SEF	Security Incident Management, E-Discovery & Cloud Forensics	27	27	Partially Addressed
STA	Supply Chain Management, Transparency & Accountability	12	12	Partially Addressed
TVM	Threat & Vulnerability Management	27	27	Partially Addressed
UEM	Universal Endpoint Management	0	0	Not Addressed

5. Domain-Level Analysis

A&A — Audit & Assurance

Independent assessment, audit planning, evidence, control effectiveness and assurance.

GAISSF linkage: 12 controls across 12 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

AIS — Application & Interface Security

Secure application lifecycle, interfaces, APIs and application-layer protections.

GAISSF linkage: 28 controls across 28 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

BCR — Business Continuity Management & Operational Resilience

Continuity, recovery, resilience, backup and service restoration.

GAISSF linkage: 14 controls across 14 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

CCC — Change Control & Configuration Management

Controlled changes, configuration baselines, approvals and integrity.

GAISSF linkage: 9 controls across 9 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

CEK — Cryptography, Encryption & Key Management

Cryptographic controls, key lifecycle, secrets and protected communications.

GAISSF linkage: 0 controls across 0 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

DCS — Datacenter Security

Physical facilities, environmental safeguards and infrastructure protection.

GAISSF linkage: 7 controls across 7 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

DSP — Data Security & Privacy

Data governance, classification, privacy, retention, protection and secure disposal.

GAISSF linkage: 22 controls across 22 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

GRC — Governance, Risk Management & Compliance

Policies, accountability, risk management, legal obligations and oversight.

GAISSF linkage: 37 controls across 37 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

HRS — Human Resources Security

Personnel screening, awareness, responsibilities and workforce lifecycle.

GAISSF linkage: 5 controls across 5 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

IAM — Identity & Access Management

Identity lifecycle, authentication, authorization, privileged access and segregation.

GAISSF linkage: 18 controls across 18 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

IPY — Interoperability & Portability

Portability, interoperability, exit planning and dependency management.

GAISSF linkage: 7 controls across 7 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

IVS — Infrastructure & Virtualization Security

Cloud infrastructure, compute, network, containers, virtualization and hardening.

GAISSF linkage: 13 controls across 13 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

LOG — Logging & Monitoring

Security logging, monitoring, alerting, time synchronization and evidence.

GAISSF linkage: 43 controls across 43 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

SEF — Security Incident Management, E-Discovery & Cloud Forensics

Incident preparation, response, investigation, evidence and forensics.

GAISSF linkage: 27 controls across 27 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

STA — Supply Chain Management, Transparency & Accountability

Third-party risk, supply chain, contracts, transparency and shared responsibility.

GAISSF linkage: 12 controls across 12 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

TVM — Threat & Vulnerability Management

Threat intelligence, vulnerability discovery, remediation, testing and exposure management.

GAISSF linkage: 27 controls across 27 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

UEM — Universal Endpoint Management

Endpoint inventory, configuration, protection and lifecycle management.

GAISSF linkage: 0 controls across 0 mapping records. A domain-level relationship does not establish coverage of all 207 CCM v4.1 control specifications, CAIQ questions, shared-responsibility assignments, auditing guidelines or STAR assurance requirements.

6. Shared Responsibility and Cloud Context

CCM is designed for cloud environments and explicitly supports a Shared Security Responsibility Model across cloud service providers (CSPs) and cloud service customers (CSCs). GAISSF control implementation must therefore be evaluated against the selected cloud service model, deployment model, provider architecture, inherited controls, customer responsibilities, and system boundary. A domain mapping does not allocate responsibility by itself.

7. CAIQ and STAR Treatment

CAIQ v4.1 is the assessment questionnaire aligned to CCM v4.1 and contains 283 questions. STAR Level 1 uses a self-assessment questionnaire, while STAR Level 2 uses third-party assurance routes. CSA states that CCM/CAIQ v4.1 are accepted for STAR submissions, with a transition period during which v4.0 remains accepted through December 2027. Neither a GAISSF mapping nor GAISSF conformance automatically completes CAIQ, establishes STAR eligibility, or satisfies STAR attestation/certification requirements.

8. Evidence Reuse

Evidence class	Potential reuse	Important limitation
Governance and risk	Policies, risk registers, ownership records, exception approvals	Must be scoped to cloud service and shared-responsibility allocation.
Technical security	Threat models, test reports, access records, configuration evidence	Provider-specific configuration and inherited controls require separate validation.
Monitoring and incidents	Logs, alerts, incident records, forensic procedures	Cloud log sources, retention and provider access must be confirmed.
Supply chain	Vendor assessments, contracts, model provenance records	Cloud subcontractors, locations, portability and exit obligations remain separate.
Assurance	Control narratives, evidence indexes, internal reviews	Does not replace CCM auditing guidelines, CAIQ responses or STAR assessment.

9. Gap Register Summary

Every CCM domain retains a control-specification-level gap because this release maps to domains rather than reproducing the complete CCM control set. Implementers must perform a licensed, control-by-control review of CCM v4.1, allocate responsibilities, document applicability and gather operating evidence.

D9 mappings are additional/conditional. Where Physical AI or cyber-physical actuation is in scope, PAI-SF™ v1.0 may be used alongside GAISSF; CSX-PAISF-004 is mapping only and does not establish equivalence, evidence sufficiency, or automatic conformance.

10. Limitations

- Domain-level mapping is not a substitute for the 207 CCM v4.1 control specifications.
- CAIQ questions and answers are not reproduced or pre-completed.
- The crosswalk does not determine cloud-provider or customer responsibility.
- The crosswalk does not establish STAR Level 1 or Level 2 eligibility.
- No claim of CSA endorsement, certification, attestation or validation is made.

• Cloud-provider-specific services, configurations, regions and evidence require independent assessment.

11. Notably Absent

- CSA endorsement or affiliation
- STAR listing, certification or attestation
- CAIQ submission or validation
- Proof of implementation or operating effectiveness
- Control-specification-level mapping to all 207 CCM controls
- Cloud-provider-specific configuration evidence
- Automatic assignment of shared responsibility

12. Conclusion

GAISSF provides substantial AI-specific security, governance, supply-chain, monitoring and incident-response capabilities that can support cloud-security programs using CCM v4.1. The crosswalk is most useful as a triage and evidence-reuse instrument. It must not be interpreted as complete CCM coverage or cloud assurance without control-specification-level analysis and verified operating evidence.

Annex A — Complete GAISSF-to-CCM Domain Mapping Register

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
GAISSF-CRO-034-MAP-0001	D1-CTL-01	DATASET PROVENANCE & POISONING PREVENTION	DSP	SP	Medium-High	Dataset Provenance & Poisoning Prevention contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0002	D1-CTL-01	DATASET PROVENANCE & POISONING PREVENTION	TVM	P	Medium	Dataset Provenance & Poisoning Prevention contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0003	D1-CTL-01	DATASET PROVENANCE & POISONING PREVENTION	AIS	P	Medium	Dataset Provenance & Poisoning Prevention contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0004	D1-CTL-01	DATASET PROVENANCE & POISONING PREVENTION	LOG	S	Medium	Dataset Provenance & Poisoning Prevention contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						the cloud control environment.	
GAISSF-CRO-034-MAP-0005	D1-CTL-01	DATASET PROVENANCE & POISONING PREVENTION	CCC	S	Medium	Dataset Provenance & Poisoning Prevention contributes to the Change Control & Configuration Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0006	D1-CTL-02	MODEL EXTRACTION RESISTANCE	DSP	SP	Medium-High	Model Extraction Resistance contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0007	D1-CTL-02	MODEL EXTRACTION RESISTANCE	TVM	P	Medium	Model Extraction Resistance contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0008	D1-CTL-02	MODEL EXTRACTION RESISTANCE	AIS	P	Medium	Model Extraction Resistance contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0009	D1-CTL-02	MODEL EXTRACTION RESISTANCE	LOG	S	Medium	Model Extraction Resistance contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0010	D1-CTL-02	MODEL EXTRACTION RESISTANCE	CCC	S	Medium	Model Extraction Resistance contributes to the Change Control & Configuration Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0011	D1-CTL-03	BEHAVIORAL DRIFT DETECTION	DSP	SP	Medium-High	Behavioral Drift Detection contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0012	D1-CTL-03	BEHAVIORAL DRIFT DETECTION	TVM	P	Medium	Behavioral Drift Detection contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						environment.	
GAISSF-CRO-034-MAP-0013	D1-CTL-03	BEHAVIORAL DRIFT DETECTION	AIS	P	Medium	Behavioral Drift Detection contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0014	D1-CTL-03	BEHAVIORAL DRIFT DETECTION	LOG	S	Medium	Behavioral Drift Detection contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0015	D1-CTL-03	BEHAVIORAL DRIFT DETECTION	CCC	S	Medium	Behavioral Drift Detection contributes to the Change Control & Configuration Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0016	D1-CTL-04	FEDERATED LEARNING POISONING PREVENTION	DSP	SP	Medium-High	Federated Learning Poisoning Prevention contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0017	D1-CTL-04	FEDERATED LEARNING POISONING PREVENTION	TVM	P	Medium	Federated Learning Poisoning Prevention contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0018	D1-CTL-04	FEDERATED LEARNING POISONING PREVENTION	AIS	P	Medium	Federated Learning Poisoning Prevention contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0019	D1-CTL-04	FEDERATED LEARNING POISONING PREVENTION	LOG	S	Medium	Federated Learning Poisoning Prevention contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0020	D1-CTL-04	FEDERATED LEARNING POISONING PREVENTION	CCC	S	Medium	Federated Learning Poisoning Prevention contributes to the Change Control & Configuration	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0021	D1-CTL-05	EMBEDDING SPACE ROBUSTNESS	DSP	SP	Medium-High	Embedding Space Robustness contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0022	D1-CTL-05	EMBEDDING SPACE ROBUSTNESS	TVM	P	Medium	Embedding Space Robustness contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0023	D1-CTL-05	EMBEDDING SPACE ROBUSTNESS	AIS	P	Medium	Embedding Space Robustness contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0024	D1-CTL-05	EMBEDDING SPACE ROBUSTNESS	LOG	S	Medium	Embedding Space Robustness contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0025	D1-CTL-05	EMBEDDING SPACE ROBUSTNESS	CCC	S	Medium	Embedding Space Robustness contributes to the Change Control & Configuration Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0026	D1-CTL-06	POST-QUANTUM MODEL SIGNING & CRYPTO HARDENING	DSP	SP	Medium-High	Post-Quantum Model Signing & Crypto Hardening contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0027	D1-CTL-06	POST-QUANTUM MODEL SIGNING & CRYPTO HARDENING	TVM	P	Medium	Post-Quantum Model Signing & Crypto Hardening contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-	D1-CTL-06	POST-QUANTUM	AIS	P	Medium	Post-Quantum	CCM v4.1

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
CRO-034-MAP-0028		MODEL SIGNING & CRYPTO HARDENING				Model Signing & Crypto Hardening contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0029	D1-CTL-06	POST-QUANTUM MODEL SIGNING & CRYPTO HARDENING	LOG	S	Medium	Post-Quantum Model Signing & Crypto Hardening contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0030	D1-CTL-06	POST-QUANTUM MODEL SIGNING & CRYPTO HARDENING	CCC	S	Medium	Post-Quantum Model Signing & Crypto Hardening contributes to the Change Control & Configuration Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0031	D1-CTL-07	LORA/ADAPTER INTEGRITY VERIFICATION	DSP	SP	Medium-High	Lora/Adapter Integrity Verification contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0032	D1-CTL-07	LORA/ADAPTER INTEGRITY VERIFICATION	TVM	P	Medium	Lora/Adapter Integrity Verification contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0033	D1-CTL-07	LORA/ADAPTER INTEGRITY VERIFICATION	AIS	P	Medium	Lora/Adapter Integrity Verification contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0034	D1-CTL-07	LORA/ADAPTER INTEGRITY VERIFICATION	LOG	S	Medium	Lora/Adapter Integrity Verification contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0035	D1-CTL-07	LORA/ADAPTER INTEGRITY VERIFICATION	CCC	S	Medium	Lora/Adapter Integrity Verification contributes to the Change Control & Configuration Management outcome by providing AI-specific	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						requirements that can operate within the cloud control environment.	
GAISSF-CRO-034-MAP-0036	D1-CTL-08	MODEL MERGE ATTACK DETECTION	DSP	SP	Medium-High	Model Merge Attack Detection contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0037	D1-CTL-08	MODEL MERGE ATTACK DETECTION	TVM	P	Medium	Model Merge Attack Detection contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0038	D1-CTL-08	MODEL MERGE ATTACK DETECTION	AIS	P	Medium	Model Merge Attack Detection contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0039	D1-CTL-08	MODEL MERGE ATTACK DETECTION	LOG	S	Medium	Model Merge Attack Detection contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0040	D1-CTL-08	MODEL MERGE ATTACK DETECTION	CCC	S	Medium	Model Merge Attack Detection contributes to the Change Control & Configuration Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0041	D1-CTL-09	QUANTIZATION BACKDOOR SCREENING	DSP	SP	Medium-High	Quantization Backdoor Screening contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0042	D1-CTL-09	QUANTIZATION BACKDOOR SCREENING	TVM	P	Medium	Quantization Backdoor Screening contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0043	D1-CTL-09	QUANTIZATION BACKDOOR SCREENING	AIS	P	Medium	Quantization Backdoor Screening contributes to the Application & Interface Security outcome by providing AI-specific requirements that	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						can operate within the cloud control environment.	
GAISSF-CRO-034-MAP-0044	D1-CTL-09	QUANTIZATION BACKDOOR SCREENING	LOG	S	Medium	Quantization Backdoor Screening contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0045	D1-CTL-09	QUANTIZATION BACKDOOR SCREENING	CCC	S	Medium	Quantization Backdoor Screening contributes to the Change Control & Configuration Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0046	D2-CTL-01	DIRECT PROMPT INJECTION PREVENTION	AIS	SP	Medium-High	Direct Prompt Injection Prevention contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0047	D2-CTL-01	DIRECT PROMPT INJECTION PREVENTION	IVS	P	Medium	Direct Prompt Injection Prevention contributes to the Infrastructure & Virtualization Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0048	D2-CTL-01	DIRECT PROMPT INJECTION PREVENTION	IAM	P	Medium	Direct Prompt Injection Prevention contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0049	D2-CTL-01	DIRECT PROMPT INJECTION PREVENTION	LOG	S	Medium	Direct Prompt Injection Prevention contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0050	D2-CTL-01	DIRECT PROMPT INJECTION PREVENTION	TVM	S	Medium	Direct Prompt Injection Prevention contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0051	D2-CTL-02	INDIRECT PROMPT INJECTION PREVENTION	AIS	SP	Medium-High	Indirect Prompt Injection Prevention contributes to the Application &	CCM v4.1 includes cloud-provider/customer responsibility allocation and

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0052	D2-CTL-02	INDIRECT PROMPT INJECTION PREVENTION	IVS	P	Medium	Indirect Prompt Injection Prevention contributes to the Infrastructure & Virtualization Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0053	D2-CTL-02	INDIRECT PROMPT INJECTION PREVENTION	IAM	P	Medium	Indirect Prompt Injection Prevention contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0054	D2-CTL-02	INDIRECT PROMPT INJECTION PREVENTION	LOG	S	Medium	Indirect Prompt Injection Prevention contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0055	D2-CTL-02	INDIRECT PROMPT INJECTION PREVENTION	TVM	S	Medium	Indirect Prompt Injection Prevention contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0056	D2-CTL-03	JAILBREAK RESISTANCE TESTING	AIS	SP	Medium-High	Jailbreak Resistance Testing contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0057	D2-CTL-03	JAILBREAK RESISTANCE TESTING	IVS	P	Medium	Jailbreak Resistance Testing contributes to the Infrastructure & Virtualization Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0058	D2-CTL-03	JAILBREAK RESISTANCE TESTING	IAM	P	Medium	Jailbreak Resistance Testing contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-	D2-CTL-03	JAILBREAK	LOG	S	Medium	Jailbreak	CCM v4.1

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
CRO-034-MAP-0059		RESISTANCE TESTING				Resistance Testing contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0060	D2-CTL-03	JAILBREAK RESISTANCE TESTING	TVM	S	Medium	Jailbreak Resistance Testing contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0061	D2-CTL-04	MULTI-MODAL INJECTION DEFENSE	AIS	SP	Medium-High	Multi-Modal Injection Defense contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0062	D2-CTL-04	MULTI-MODAL INJECTION DEFENSE	IVS	P	Medium	Multi-Modal Injection Defense contributes to the Infrastructure & Virtualization Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0063	D2-CTL-04	MULTI-MODAL INJECTION DEFENSE	IAM	P	Medium	Multi-Modal Injection Defense contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0064	D2-CTL-04	MULTI-MODAL INJECTION DEFENSE	LOG	S	Medium	Multi-Modal Injection Defense contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0065	D2-CTL-04	MULTI-MODAL INJECTION DEFENSE	TVM	S	Medium	Multi-Modal Injection Defense contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0066	D2-CTL-05	FUNCTION CALL/TOOL CALL INJECTION PREVENTION	AIS	SP	Medium-High	Function Call/Tool Call Injection Prevention contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-	D2-CTL-05	FUNCTION	IVS	P	Medium	Function Call/Tool	CCM v4.1

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
CRO-034-MAP-0067		CALL/TOOL CALL INJECTION PREVENTION				Call Injection Prevention contributes to the Infrastructure & Virtualization Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0068	D2-CTL-05	FUNCTION CALL/TOOL CALL INJECTION PREVENTION	IAM	P	Medium	Function Call/Tool Call Injection Prevention contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0069	D2-CTL-05	FUNCTION CALL/TOOL CALL INJECTION PREVENTION	LOG	S	Medium	Function Call/Tool Call Injection Prevention contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0070	D2-CTL-05	FUNCTION CALL/TOOL CALL INJECTION PREVENTION	TVM	S	Medium	Function Call/Tool Call Injection Prevention contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0071	D2-CTL-06	CROSS- CONTEXT HIJACKING MITIGATION	AIS	SP	Medium-High	Cross-Context Hijacking Mitigation contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0072	D2-CTL-06	CROSS- CONTEXT HIJACKING MITIGATION	IVS	P	Medium	Cross-Context Hijacking Mitigation contributes to the Infrastructure & Virtualization Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0073	D2-CTL-06	CROSS- CONTEXT HIJACKING MITIGATION	IAM	P	Medium	Cross-Context Hijacking Mitigation contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0074	D2-CTL-06	CROSS- CONTEXT HIJACKING MITIGATION	LOG	S	Medium	Cross-Context Hijacking Mitigation contributes to the Logging & Monitoring outcome by providing AI-specific requirements that	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						can operate within the cloud control environment.	
GAISSF-CRO-034-MAP-0075	D2-CTL-06	CROSS-CONTEXT HIJACKING MITIGATION	TVM	S	Medium	Cross-Context Hijacking Mitigation contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0076	D3-CTL-01	LEAST AGENCY ENFORCEMENT	AIS	SP	Medium-High	Least Agency Enforcement contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0077	D3-CTL-01	LEAST AGENCY ENFORCEMENT	IAM	P	Medium	Least Agency Enforcement contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0078	D3-CTL-01	LEAST AGENCY ENFORCEMENT	GRC	P	Medium	Least Agency Enforcement contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0079	D3-CTL-01	LEAST AGENCY ENFORCEMENT	LOG	S	Medium	Least Agency Enforcement contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0080	D3-CTL-01	LEAST AGENCY ENFORCEMENT	SEF	S	Medium	Least Agency Enforcement contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0081	D3-CTL-02	INTER-AGENT COMMUNICATION SECURITY	AIS	SP	Medium-High	Inter-Agent Communication Security contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0082	D3-CTL-02	INTER-AGENT COMMUNICATION SECURITY	IAM	P	Medium	Inter-Agent Communication Security contributes to the Identity & Access Management outcome by providing AI-	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						specific requirements that can operate within the cloud control environment.	this GAISSF control alone.
GAISSF-CRO-034-MAP-0083	D3-CTL-02	INTER-AGENT COMMUNICATION SECURITY	GRC	P	Medium	Inter-Agent Communication Security contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0084	D3-CTL-02	INTER-AGENT COMMUNICATION SECURITY	LOG	S	Medium	Inter-Agent Communication Security contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0085	D3-CTL-02	INTER-AGENT COMMUNICATION SECURITY	SEF	S	Medium	Inter-Agent Communication Security contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0086	D3-CTL-03	AGENTIC PROMPT CHAINING DETECTION	AIS	SP	Medium-High	Agentic Prompt Chaining Detection contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0087	D3-CTL-03	AGENTIC PROMPT CHAINING DETECTION	IAM	P	Medium	Agentic Prompt Chaining Detection contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0088	D3-CTL-03	AGENTIC PROMPT CHAINING DETECTION	GRC	P	Medium	Agentic Prompt Chaining Detection contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0089	D3-CTL-03	AGENTIC PROMPT CHAINING DETECTION	LOG	S	Medium	Agentic Prompt Chaining Detection contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-	D3-CTL-03	AGENTIC	SEF	S	Medium	Agentic Prompt	CCM v4.1

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
CRO-034-MAP-0090		PROMPT CHAINING DETECTION				Chaining Detection contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0091	D3-CTL-04	EMBODIED AI SAFETY CONTROLS	AIS	SP	Medium-High	Embodied Ai Safety Controls contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0092	D3-CTL-04	EMBODIED AI SAFETY CONTROLS	IAM	P	Medium	Embodied Ai Safety Controls contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0093	D3-CTL-04	EMBODIED AI SAFETY CONTROLS	GRC	P	Medium	Embodied Ai Safety Controls contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0094	D3-CTL-04	EMBODIED AI SAFETY CONTROLS	LOG	S	Medium	Embodied Ai Safety Controls contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0095	D3-CTL-04	EMBODIED AI SAFETY CONTROLS	SEF	S	Medium	Embodied Ai Safety Controls contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0096	D3-CTL-05	MULTI-AGENT TRUST CHAIN ATTESTATION	AIS	SP	Medium-High	Multi-Agent Trust Chain Attestation contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0097	D3-CTL-05	MULTI-AGENT TRUST CHAIN ATTESTATION	IAM	P	Medium	Multi-Agent Trust Chain Attestation contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
GAISSF-CRO-034-MAP-0098	D3-CTL-05	MULTI-AGENT TRUST CHAIN ATTESTATION	GRC	P	Medium	Multi-Agent Trust Chain Attestation contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0099	D3-CTL-05	MULTI-AGENT TRUST CHAIN ATTESTATION	LOG	S	Medium	Multi-Agent Trust Chain Attestation contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0100	D3-CTL-05	MULTI-AGENT TRUST CHAIN ATTESTATION	SEF	S	Medium	Multi-Agent Trust Chain Attestation contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0101	D3-CTL-06	PERSISTENT MEMORY EXFILTRATION PREVENTION	AIS	SP	Medium-High	Persistent Memory Exfiltration Prevention contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0102	D3-CTL-06	PERSISTENT MEMORY EXFILTRATION PREVENTION	IAM	P	Medium	Persistent Memory Exfiltration Prevention contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0103	D3-CTL-06	PERSISTENT MEMORY EXFILTRATION PREVENTION	GRC	P	Medium	Persistent Memory Exfiltration Prevention contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0104	D3-CTL-06	PERSISTENT MEMORY EXFILTRATION PREVENTION	LOG	S	Medium	Persistent Memory Exfiltration Prevention contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0105	D3-CTL-06	PERSISTENT MEMORY EXFILTRATION PREVENTION	SEF	S	Medium	Persistent Memory Exfiltration Prevention contributes to the	CCM v4.1 includes cloud-provider/customer responsibility allocation and

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0106	D3-CTL-07	SECURE MEMORY LIFECYCLE MANAGEMENT	AIS	SP	Medium-High	Secure Memory Lifecycle Management contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0107	D3-CTL-07	SECURE MEMORY LIFECYCLE MANAGEMENT	IAM	P	Medium	Secure Memory Lifecycle Management contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0108	D3-CTL-07	SECURE MEMORY LIFECYCLE MANAGEMENT	GRC	P	Medium	Secure Memory Lifecycle Management contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0109	D3-CTL-07	SECURE MEMORY LIFECYCLE MANAGEMENT	LOG	S	Medium	Secure Memory Lifecycle Management contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0110	D3-CTL-07	SECURE MEMORY LIFECYCLE MANAGEMENT	SEF	S	Medium	Secure Memory Lifecycle Management contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0111	D4-CTL-01	AI BILL OF MATERIALS (AI BOM) MAINTENANCE	STA	SP	Medium-High	AI Bill Of Materials (Ai Bom) Maintenance contributes to the Supply Chain Management, Transparency & Accountability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0112	D4-CTL-01	AI BILL OF MATERIALS (AI BOM) MAINTENANCE	GRC	P	Medium	AI Bill Of Materials (Ai Bom) Maintenance contributes to the Governance, Risk Management & Compliance	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						outcome by providing AI-specific requirements that can operate within the cloud control environment.	established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0113	D4-CTL-01	AI BILL OF MATERIALS (AI BOM) MAINTENANCE	DSP	P	Medium	AI Bill Of Materials (Ai Bom) Maintenance contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0114	D4-CTL-01	AI BILL OF MATERIALS (AI BOM) MAINTENANCE	TVM	S	Medium	AI Bill Of Materials (Ai Bom) Maintenance contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0115	D4-CTL-01	AI BILL OF MATERIALS (AI BOM) MAINTENANCE	IPY	S	Medium	AI Bill Of Materials (Ai Bom) Maintenance contributes to the Interoperability & Portability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0116	D4-CTL-02	MODEL FILE & ARTIFACT SCANNING	STA	SP	Medium-High	Model File & Artifact Scanning contributes to the Supply Chain Management, Transparency & Accountability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0117	D4-CTL-02	MODEL FILE & ARTIFACT SCANNING	GRC	P	Medium	Model File & Artifact Scanning contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0118	D4-CTL-02	MODEL FILE & ARTIFACT SCANNING	DSP	P	Medium	Model File & Artifact Scanning contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0119	D4-CTL-02	MODEL FILE & ARTIFACT SCANNING	TVM	S	Medium	Model File & Artifact Scanning contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0120	D4-CTL-02	MODEL FILE & ARTIFACT SCANNING	IPY	S	Medium	Model File & Artifact Scanning contributes to the Interoperability &	CCM v4.1 includes cloud-provider/customer responsibility

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						Portability outcome by providing AI-specific requirements that can operate within the cloud control environment.	allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0121	D4-CTL-03	MODEL HUB & REGISTRY VETTING	STA	SP	Medium-High	Model Hub & Registry Vetting contributes to the Supply Chain Management, Transparency & Accountability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0122	D4-CTL-03	MODEL HUB & REGISTRY VETTING	GRC	P	Medium	Model Hub & Registry Vetting contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0123	D4-CTL-03	MODEL HUB & REGISTRY VETTING	DSP	P	Medium	Model Hub & Registry Vetting contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0124	D4-CTL-03	MODEL HUB & REGISTRY VETTING	TVM	S	Medium	Model Hub & Registry Vetting contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0125	D4-CTL-03	MODEL HUB & REGISTRY VETTING	IPY	S	Medium	Model Hub & Registry Vetting contributes to the Interoperability & Portability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0126	D4-CTL-04	MCP SERVER BEHAVIORAL MONITORING	STA	SP	Medium-High	Mcp Server Behavioral Monitoring contributes to the Supply Chain Management, Transparency & Accountability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0127	D4-CTL-04	MCP SERVER BEHAVIORAL MONITORING	GRC	P	Medium	Mcp Server Behavioral Monitoring contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-	D4-CTL-04	MCP SERVER	DSP	P	Medium	Mcp Server	CCM v4.1

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
CRO-034-MAP-0128		BEHAVIORAL MONITORING				Behavioral Monitoring contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0129	D4-CTL-04	MCP SERVER BEHAVIORAL MONITORING	TVM	S	Medium	Mcp Server Behavioral Monitoring contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0130	D4-CTL-04	MCP SERVER BEHAVIORAL MONITORING	IPY	S	Medium	Mcp Server Behavioral Monitoring contributes to the Interoperability & Portability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0131	D4-CTL-05	THIRD-PARTY AI API SECURITY ASSESSMENT	STA	SP	Medium-High	Third-Party Ai Api Security Assessment contributes to the Supply Chain Management, Transparency & Accountability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0132	D4-CTL-05	THIRD-PARTY AI API SECURITY ASSESSMENT	GRC	P	Medium	Third-Party Ai Api Security Assessment contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0133	D4-CTL-05	THIRD-PARTY AI API SECURITY ASSESSMENT	DSP	P	Medium	Third-Party Ai Api Security Assessment contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0134	D4-CTL-05	THIRD-PARTY AI API SECURITY ASSESSMENT	TVM	S	Medium	Third-Party Ai Api Security Assessment contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0135	D4-CTL-05	THIRD-PARTY AI API SECURITY ASSESSMENT	IPY	S	Medium	Third-Party Ai Api Security Assessment contributes to the Interoperability & Portability outcome by providing AI-	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						specific requirements that can operate within the cloud control environment.	this GAISSF control alone.
GAISSF-CRO-034-MAP-0136	D4-CTL-06	SHADOW AI DISCOVERY & GOVERNANCE	STA	SP	Medium-High	Shadow Ai Discovery & Governance contributes to the Supply Chain Management, Transparency & Accountability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0137	D4-CTL-06	SHADOW AI DISCOVERY & GOVERNANCE	GRC	P	Medium	Shadow Ai Discovery & Governance contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0138	D4-CTL-06	SHADOW AI DISCOVERY & GOVERNANCE	DSP	P	Medium	Shadow Ai Discovery & Governance contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0139	D4-CTL-06	SHADOW AI DISCOVERY & GOVERNANCE	TVM	S	Medium	Shadow Ai Discovery & Governance contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0140	D4-CTL-06	SHADOW AI DISCOVERY & GOVERNANCE	IPY	S	Medium	Shadow Ai Discovery & Governance contributes to the Interoperability & Portability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0141	D4-CTL-07	AI SOFTWARE COMPOSITION ANALYSIS (SCA)	STA	SP	Medium-High	AI Software Composition Analysis (Sca) contributes to the Supply Chain Management, Transparency & Accountability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0142	D4-CTL-07	AI SOFTWARE COMPOSITION ANALYSIS (SCA)	GRC	P	Medium	AI Software Composition Analysis (Sca) contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						environment.	
GAISSF-CRO-034-MAP-0143	D4-CTL-07	AI SOFTWARE COMPOSITION ANALYSIS (SCA)	DSP	P	Medium	AI Software Composition Analysis (Sca) contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0144	D4-CTL-07	AI SOFTWARE COMPOSITION ANALYSIS (SCA)	TVM	S	Medium	AI Software Composition Analysis (Sca) contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0145	D4-CTL-07	AI SOFTWARE COMPOSITION ANALYSIS (SCA)	IPY	S	Medium	AI Software Composition Analysis (Sca) contributes to the Interoperability & Portability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0146	D5-CTL-01	HARMFUL CONTENT BLOCKING	DSP	SP	Medium-High	Harmful Content Blocking contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0147	D5-CTL-01	HARMFUL CONTENT BLOCKING	AIS	P	Medium	Harmful Content Blocking contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0148	D5-CTL-01	HARMFUL CONTENT BLOCKING	GRC	P	Medium	Harmful Content Blocking contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0149	D5-CTL-01	HARMFUL CONTENT BLOCKING	LOG	S	Medium	Harmful Content Blocking contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0150	D5-CTL-02	PII LEAKAGE PREVENTION	DSP	SP	Medium-High	Pii Leakage Prevention contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-	D5-CTL-02	PII LEAKAGE PREVENTION	AIS	P	Medium	Pii Leakage Prevention	CCM v4.1 includes cloud-

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
MAP-0151						contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0152	D5-CTL-02	PII LEAKAGE PREVENTION	GRC	P	Medium	Pii Leakage Prevention contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0153	D5-CTL-02	PII LEAKAGE PREVENTION	LOG	S	Medium	Pii Leakage Prevention contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0154	D5-CTL-03	COPYRIGHT DETECTION	DSP	SP	Medium-High	Copyright Detection contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0155	D5-CTL-03	COPYRIGHT DETECTION	AIS	P	Medium	Copyright Detection contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0156	D5-CTL-03	COPYRIGHT DETECTION	GRC	P	Medium	Copyright Detection contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0157	D5-CTL-03	COPYRIGHT DETECTION	LOG	S	Medium	Copyright Detection contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0158	D5-CTL-04	AI WATERMARKING ROBUSTNESS	DSP	SP	Medium-High	Ai Watermarking Robustness contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0159	D5-CTL-04	AI WATERMARKING ROBUSTNESS	AIS	P	Medium	Ai Watermarking Robustness contributes to the Application & Interface Security outcome by providing AI-	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						specific requirements that can operate within the cloud control environment.	established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0160	D5-CTL-04	AI WATERMARKING ROBUSTNESS	GRC	P	Medium	AI Watermarking Robustness contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0161	D5-CTL-04	AI WATERMARKING ROBUSTNESS	LOG	S	Medium	AI Watermarking Robustness contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0162	D5-CTL-05	PRIVACY-BY-DESIGN VERIFICATION	DSP	SP	Medium-High	Privacy-By-Design Verification contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0163	D5-CTL-05	PRIVACY-BY-DESIGN VERIFICATION	AIS	P	Medium	Privacy-By-Design Verification contributes to the Application & Interface Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0164	D5-CTL-05	PRIVACY-BY-DESIGN VERIFICATION	GRC	P	Medium	Privacy-By-Design Verification contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0165	D5-CTL-05	PRIVACY-BY-DESIGN VERIFICATION	LOG	S	Medium	Privacy-By-Design Verification contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0166	D5-CTL-06	PRIVACY-PRESERVING ML VALIDATION	DSP	SP	Medium-High	Privacy-Preserving ML Validation contributes to the Data Security & Privacy outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0167	D5-CTL-06	PRIVACY-PRESERVING ML VALIDATION	AIS	P	Medium	Privacy-Preserving ML Validation contributes to the Application & Interface Security outcome by	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						providing AI-specific requirements that can operate within the cloud control environment.	established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0168	D5-CTL-06	PRIVACY-PRESERVING ML VALIDATION	GRC	P	Medium	Privacy-Preserving ML Validation contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0169	D5-CTL-06	PRIVACY-PRESERVING ML VALIDATION	LOG	S	Medium	Privacy-Preserving ML Validation contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0170	D6-CTL-01	HUMAN-IN-THE-LOOP FOR HIGH-RISK ACTIONS	GRC	SP	Medium-High	Human-In-The-Loop For High-Risk Actions contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0171	D6-CTL-01	HUMAN-IN-THE-LOOP FOR HIGH-RISK ACTIONS	A&A	P	Medium	Human-In-The-Loop For High-Risk Actions contributes to the Audit & Assurance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0172	D6-CTL-01	HUMAN-IN-THE-LOOP FOR HIGH-RISK ACTIONS	LOG	P	Medium	Human-In-The-Loop For High-Risk Actions contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0173	D6-CTL-01	HUMAN-IN-THE-LOOP FOR HIGH-RISK ACTIONS	SEF	S	Medium	Human-In-The-Loop For High-Risk Actions contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0174	D6-CTL-01	HUMAN-IN-THE-LOOP FOR HIGH-RISK ACTIONS	BCR	S	Medium	Human-In-The-Loop For High-Risk Actions contributes to the Business Continuity Management & Operational Resilience outcome by providing AI-specific requirements that	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						can operate within the cloud control environment.	
GAISSF-CRO-034-MAP-0175	D6-CTL-02	AUDIT TRAIL COMPLETENESS	GRC	SP	Medium-High	Audit Trail Completeness contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0176	D6-CTL-02	AUDIT TRAIL COMPLETENESS	A&A	P	Medium	Audit Trail Completeness contributes to the Audit & Assurance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0177	D6-CTL-02	AUDIT TRAIL COMPLETENESS	LOG	P	Medium	Audit Trail Completeness contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0178	D6-CTL-02	AUDIT TRAIL COMPLETENESS	SEF	S	Medium	Audit Trail Completeness contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0179	D6-CTL-02	AUDIT TRAIL COMPLETENESS	BCR	S	Medium	Audit Trail Completeness contributes to the Business Continuity Management & Operational Resilience outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0180	D6-CTL-03	AI MODEL CARD COMPLETENESS	GRC	SP	Medium-High	AI Model Card Completeness contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0181	D6-CTL-03	AI MODEL CARD COMPLETENESS	A&A	P	Medium	AI Model Card Completeness contributes to the Audit & Assurance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0182	D6-CTL-03	AI MODEL CARD COMPLETENESS	LOG	P	Medium	AI Model Card Completeness contributes to the Logging & Monitoring outcome by providing AI-	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						specific requirements that can operate within the cloud control environment.	established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0183	D6-CTL-03	AI MODEL CARD COMPLETENESS	SEF	S	Medium	Ai Model Card Completeness contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0184	D6-CTL-03	AI MODEL CARD COMPLETENESS	BCR	S	Medium	Ai Model Card Completeness contributes to the Business Continuity Management & Operational Resilience outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0185	D6-CTL-04	AI INCIDENT RESPONSE READINESS	GRC	SP	Medium-High	Ai Incident Response Readiness contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0186	D6-CTL-04	AI INCIDENT RESPONSE READINESS	A&A	P	Medium	Ai Incident Response Readiness contributes to the Audit & Assurance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0187	D6-CTL-04	AI INCIDENT RESPONSE READINESS	LOG	P	Medium	Ai Incident Response Readiness contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0188	D6-CTL-04	AI INCIDENT RESPONSE READINESS	SEF	S	Medium	Ai Incident Response Readiness contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0189	D6-CTL-04	AI INCIDENT RESPONSE READINESS	BCR	S	Medium	Ai Incident Response Readiness contributes to the Business Continuity Management & Operational Resilience outcome by providing AI-specific	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						requirements that can operate within the cloud control environment.	
GAISSF-CRO-034-MAP-0190	D6-CTL-05	MODEL DEPRECATION & DECOMMISSIONING	GRC	SP	Medium-High	Model Deprecation & Decommissioning contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0191	D6-CTL-05	MODEL DEPRECATION & DECOMMISSIONING	A&A	P	Medium	Model Deprecation & Decommissioning contributes to the Audit & Assurance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0192	D6-CTL-05	MODEL DEPRECATION & DECOMMISSIONING	LOG	P	Medium	Model Deprecation & Decommissioning contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0193	D6-CTL-05	MODEL DEPRECATION & DECOMMISSIONING	SEF	S	Medium	Model Deprecation & Decommissioning contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0194	D6-CTL-05	MODEL DEPRECATION & DECOMMISSIONING	BCR	S	Medium	Model Deprecation & Decommissioning contributes to the Business Continuity Management & Operational Resilience outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0195	D6-CTL-06	THIRD-PARTY AI VENDOR GOVERNANCE	GRC	SP	Medium-High	Third-Party Ai Vendor Governance contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0196	D6-CTL-06	THIRD-PARTY AI VENDOR GOVERNANCE	A&A	P	Medium	Third-Party Ai Vendor Governance contributes to the Audit & Assurance outcome by providing AI-specific requirements that can operate within the cloud control	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						environment.	
GAISSF-CRO-034-MAP-0197	D6-CTL-06	THIRD-PARTY AI VENDOR GOVERNANCE	LOG	P	Medium	Third-Party Ai Vendor Governance contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0198	D6-CTL-06	THIRD-PARTY AI VENDOR GOVERNANCE	SEF	S	Medium	Third-Party Ai Vendor Governance contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0199	D6-CTL-06	THIRD-PARTY AI VENDOR GOVERNANCE	BCR	S	Medium	Third-Party Ai Vendor Governance contributes to the Business Continuity Management & Operational Resilience outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0200	D6-CTL-07	AI RESILIENCE & BUSINESS CONTINUITY	GRC	SP	Medium-High	AI Resilience & Business Continuity contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0201	D6-CTL-07	AI RESILIENCE & BUSINESS CONTINUITY	A&A	P	Medium	AI Resilience & Business Continuity contributes to the Audit & Assurance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0202	D6-CTL-07	AI RESILIENCE & BUSINESS CONTINUITY	LOG	P	Medium	AI Resilience & Business Continuity contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0203	D6-CTL-07	AI RESILIENCE & BUSINESS CONTINUITY	SEF	S	Medium	AI Resilience & Business Continuity contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-	D6-CTL-07	AI RESILIENCE &	BCR	S	Medium	AI Resilience &	CCM v4.1

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
CRO-034-MAP-0204		BUSINESS CONTINUITY				Business Continuity contributes to the Business Continuity Management & Operational Resilience outcome by providing AI-specific requirements that can operate within the cloud control environment.	includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0205	D7-CTL-H01	AI-GENERATED PHISHING SIMULATION	HRS	SP	Medium-High	AI-Generated Phishing Simulation contributes to the Human Resources Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0206	D7-CTL-H01	AI-GENERATED PHISHING SIMULATION	IAM	P	Medium	AI-Generated Phishing Simulation contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0207	D7-CTL-H01	AI-GENERATED PHISHING SIMULATION	SEF	P	Medium	AI-Generated Phishing Simulation contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0208	D7-CTL-H01	AI-GENERATED PHISHING SIMULATION	TVM	S	Medium	AI-Generated Phishing Simulation contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0209	D7-CTL-H01	AI-GENERATED PHISHING SIMULATION	GRC	S	Medium	AI-Generated Phishing Simulation contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0210	D7-CTL-H02	DEEPPAKE DETECTION TRAINING	HRS	SP	Medium-High	Deepfake Detection Training contributes to the Human Resources Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0211	D7-CTL-H02	DEEPPAKE DETECTION TRAINING	IAM	P	Medium	Deepfake Detection Training contributes to the Identity & Access Management	CCM v4.1 includes cloud-provider/customer responsibility allocation and

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						outcome by providing AI-specific requirements that can operate within the cloud control environment.	detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0212	D7-CTL-H02	DEEPPFAKE DETECTION TRAINING	SEF	P	Medium	Deepfake Detection Training contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0213	D7-CTL-H02	DEEPPFAKE DETECTION TRAINING	TVM	S	Medium	Deepfake Detection Training contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0214	D7-CTL-H02	DEEPPFAKE DETECTION TRAINING	GRC	S	Medium	Deepfake Detection Training contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0215	D7-CTL-H03	OUT-OF-BAND AUTHENTICATIO N	HRS	SP	Medium-High	Out-Of-Band Authentication contributes to the Human Resources Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0216	D7-CTL-H03	OUT-OF-BAND AUTHENTICATIO N	IAM	P	Medium	Out-Of-Band Authentication contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0217	D7-CTL-H03	OUT-OF-BAND AUTHENTICATIO N	SEF	P	Medium	Out-Of-Band Authentication contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0218	D7-CTL-H03	OUT-OF-BAND AUTHENTICATIO N	TVM	S	Medium	Out-Of-Band Authentication contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0219	D7-CTL-H03	OUT-OF-BAND AUTHENTICATIO N	GRC	S	Medium	Out-Of-Band Authentication contributes to the	CCM v4.1 includes cloud-provider/customer

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0220	D7-CTL-H04	AI SOCIAL ENGINEERING IR	HRS	SP	Medium-High	AI Social Engineering Ir contributes to the Human Resources Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0221	D7-CTL-H04	AI SOCIAL ENGINEERING IR	IAM	P	Medium	AI Social Engineering Ir contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0222	D7-CTL-H04	AI SOCIAL ENGINEERING IR	SEF	P	Medium	AI Social Engineering Ir contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0223	D7-CTL-H04	AI SOCIAL ENGINEERING IR	TVM	S	Medium	AI Social Engineering Ir contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0224	D7-CTL-H04	AI SOCIAL ENGINEERING IR	GRC	S	Medium	AI Social Engineering Ir contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0225	D7-CTL-H05	AI-ENHANCED EXTERNAL ATTACK DEFENSE	HRS	SP	Medium-High	AI-Enhanced External Attack Defense contributes to the Human Resources Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0226	D7-CTL-H05	AI-ENHANCED EXTERNAL ATTACK DEFENSE	IAM	P	Medium	AI-Enhanced External Attack Defense contributes to the Identity & Access Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-	D7-CTL-H05	AI-ENHANCED	SEF	P	Medium	AI-Enhanced	CCM v4.1

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
CRO-034-MAP-0227		EXTERNAL ATTACK DEFENSE				External Attack Defense contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0228	D7-CTL-H05	AI-ENHANCED EXTERNAL ATTACK DEFENSE	TVM	S	Medium	AI-Enhanced External Attack Defense contributes to the Threat & Vulnerability Management outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0229	D7-CTL-H05	AI-ENHANCED EXTERNAL ATTACK DEFENSE	GRC	S	Medium	AI-Enhanced External Attack Defense contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0230	D8-CTL-01	EU AI ACT RISK TIER MAPPING	GRC	SP	Medium-High	Eu Ai Act Risk Tier Mapping contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0231	D8-CTL-01	EU AI ACT RISK TIER MAPPING	A&A	P	Medium	Eu Ai Act Risk Tier Mapping contributes to the Audit & Assurance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0232	D8-CTL-01	EU AI ACT RISK TIER MAPPING	STA	P	Medium	Eu Ai Act Risk Tier Mapping contributes to the Supply Chain Management, Transparency & Accountability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0233	D8-CTL-02	ISO 42001 GAP ANALYSIS	GRC	SP	Medium-High	Iso 42001 Gap Analysis contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0234	D8-CTL-02	ISO 42001 GAP ANALYSIS	A&A	P	Medium	Iso 42001 Gap Analysis contributes to the Audit & Assurance outcome by providing AI-	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						specific requirements that can operate within the cloud control environment.	established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0235	D8-CTL-02	ISO 42001 GAP ANALYSIS	STA	P	Medium	Iso 42001 Gap Analysis contributes to the Supply Chain Management, Transparency & Accountability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0236	D8-CTL-03	GPAI TECHNICAL DOCUMENTATION VERIFICATION	GRC	SP	Medium-High	Gpai Technical Documentation Verification contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0237	D8-CTL-03	GPAI TECHNICAL DOCUMENTATION VERIFICATION	A&A	P	Medium	Gpai Technical Documentation Verification contributes to the Audit & Assurance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0238	D8-CTL-03	GPAI TECHNICAL DOCUMENTATION VERIFICATION	STA	P	Medium	Gpai Technical Documentation Verification contributes to the Supply Chain Management, Transparency & Accountability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0239	D8-CTL-04	DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)	GRC	SP	Medium-High	Dora Ict Incident Reporting (Financial Sector) contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0240	D8-CTL-04	DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)	A&A	P	Medium	Dora Ict Incident Reporting (Financial Sector) contributes to the Audit & Assurance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0241	D8-CTL-04	DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)	STA	P	Medium	Dora Ict Incident Reporting (Financial Sector) contributes to the Supply Chain Management, Transparency & Accountability outcome by providing AI-specific requirements that can operate within	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						the cloud control environment.	
GAISSF-CRO-034-MAP-0242	D8-CTL-04	DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)	SEF	S	Medium	Dora Ict Incident Reporting (Financial Sector) contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0243	D8-CTL-04	DORA ICT INCIDENT REPORTING (FINANCIAL SECTOR)	LOG	S	Medium	Dora Ict Incident Reporting (Financial Sector) contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0244	D8-CTL-05	NIST SP 800-218A COMPLIANCE CHECK	GRC	SP	Medium-High	Nist Sp 800-218A Compliance Check contributes to the Governance, Risk Management & Compliance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0245	D8-CTL-05	NIST SP 800-218A COMPLIANCE CHECK	A&A	P	Medium	Nist Sp 800-218A Compliance Check contributes to the Audit & Assurance outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0246	D8-CTL-05	NIST SP 800-218A COMPLIANCE CHECK	STA	P	Medium	Nist Sp 800-218A Compliance Check contributes to the Supply Chain Management, Transparency & Accountability outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0247	D9-CTL-01	PHYSICAL HARM BOUNDARY ENFORCEMENT	DCS	SP	Medium-High	Physical Harm Boundary Enforcement contributes to the Datacenter Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0248	D9-CTL-01	PHYSICAL HARM BOUNDARY ENFORCEMENT	IVS	P	Medium	Physical Harm Boundary Enforcement contributes to the Infrastructure & Virtualization Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0249	D9-CTL-01	PHYSICAL HARM BOUNDARY ENFORCEMENT	BCR	P	Medium	Physical Harm Boundary Enforcement contributes to the Business	CCM v4.1 includes cloud-provider/customer responsibility allocation and

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						Continuity Management & Operational Resilience outcome by providing AI-specific requirements that can operate within the cloud control environment.	detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0250	D9-CTL-01	PHYSICAL HARM BOUNDARY ENFORCEMENT	SEF	S	Medium	Physical Harm Boundary Enforcement contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0251	D9-CTL-01	PHYSICAL HARM BOUNDARY ENFORCEMENT	LOG	S	Medium	Physical Harm Boundary Enforcement contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0252	D9-CTL-02	SAFE STATE AND GRACEFUL DEGRADATION	DCS	SP	Medium-High	Safe State And Graceful Degradation contributes to the Datacenter Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0253	D9-CTL-02	SAFE STATE AND GRACEFUL DEGRADATION	IVS	P	Medium	Safe State And Graceful Degradation contributes to the Infrastructure & Virtualization Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0254	D9-CTL-02	SAFE STATE AND GRACEFUL DEGRADATION	BCR	P	Medium	Safe State And Graceful Degradation contributes to the Business Continuity Management & Operational Resilience outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0255	D9-CTL-02	SAFE STATE AND GRACEFUL DEGRADATION	SEF	S	Medium	Safe State And Graceful Degradation contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0256	D9-CTL-02	SAFE STATE AND GRACEFUL DEGRADATION	LOG	S	Medium	Safe State And Graceful Degradation contributes to the Logging & Monitoring	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						outcome by providing AI-specific requirements that can operate within the cloud control environment.	specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0257	D9-CTL-03	HUMAN OVERRIDE AND EMERGENCY STOP	DCS	SP	Medium-High	Human Override And Emergency Stop contributes to the Datacenter Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0258	D9-CTL-03	HUMAN OVERRIDE AND EMERGENCY STOP	IVS	P	Medium	Human Override And Emergency Stop contributes to the Infrastructure & Virtualization Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0259	D9-CTL-03	HUMAN OVERRIDE AND EMERGENCY STOP	BCR	P	Medium	Human Override And Emergency Stop contributes to the Business Continuity Management & Operational Resilience outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0260	D9-CTL-03	HUMAN OVERRIDE AND EMERGENCY STOP	SEF	S	Medium	Human Override And Emergency Stop contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0261	D9-CTL-03	HUMAN OVERRIDE AND EMERGENCY STOP	LOG	S	Medium	Human Override And Emergency Stop contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0262	D9-CTL-04	CYBER-PHYSICAL ATTACK DETECTION	DCS	SP	Medium-High	Cyber-Physical Attack Detection contributes to the Datacenter Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0263	D9-CTL-04	CYBER-PHYSICAL ATTACK DETECTION	IVS	P	Medium	Cyber-Physical Attack Detection contributes to the Infrastructure & Virtualization Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0264	D9-CTL-04	CYBER-PHYSICAL ATTACK DETECTION	BCR	P	Medium	Cyber-Physical Attack Detection contributes to the Business Continuity	CCM v4.1 includes cloud-provider/customer responsibility allocation and

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						Management & Operational Resilience outcome by providing AI-specific requirements that can operate within the cloud control environment.	detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0265	D9-CTL-04	CYBER-PHYSICAL ATTACK DETECTION	SEF	S	Medium	Cyber-Physical Attack Detection contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0266	D9-CTL-04	CYBER-PHYSICAL ATTACK DETECTION	LOG	S	Medium	Cyber-Physical Attack Detection contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0267	D9-CTL-05	PHYSICAL ENVIRONMENT INTEGRITY MONITORING	DCS	SP	Medium-High	Physical Environment Integrity Monitoring contributes to the Datacenter Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0268	D9-CTL-05	PHYSICAL ENVIRONMENT INTEGRITY MONITORING	IVS	P	Medium	Physical Environment Integrity Monitoring contributes to the Infrastructure & Virtualization Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0269	D9-CTL-05	PHYSICAL ENVIRONMENT INTEGRITY MONITORING	BCR	P	Medium	Physical Environment Integrity Monitoring contributes to the Business Continuity Management & Operational Resilience outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0270	D9-CTL-05	PHYSICAL ENVIRONMENT INTEGRITY MONITORING	SEF	S	Medium	Physical Environment Integrity Monitoring contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0271	D9-CTL-05	PHYSICAL ENVIRONMENT INTEGRITY MONITORING	LOG	S	Medium	Physical Environment Integrity Monitoring contributes to the	CCM v4.1 includes cloud-provider/customer responsibility allocation and

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0272	D9-CTL-06	ACTUATOR COMMAND VERIFICATION	DCS	SP	Medium-High	Actuator Command Verification contributes to the Datacenter Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0273	D9-CTL-06	ACTUATOR COMMAND VERIFICATION	IVS	P	Medium	Actuator Command Verification contributes to the Infrastructure & Virtualization Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0274	D9-CTL-06	ACTUATOR COMMAND VERIFICATION	BCR	P	Medium	Actuator Command Verification contributes to the Business Continuity Management & Operational Resilience outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0275	D9-CTL-06	ACTUATOR COMMAND VERIFICATION	SEF	S	Medium	Actuator Command Verification contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0276	D9-CTL-06	ACTUATOR COMMAND VERIFICATION	LOG	S	Medium	Actuator Command Verification contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0277	D9-CTL-07	PHYSICAL INCIDENT EVIDENCE PRESERVATION	DCS	SP	Medium-High	Physical Incident Evidence Preservation contributes to the Datacenter Security outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0278	D9-CTL-07	PHYSICAL INCIDENT EVIDENCE PRESERVATION	IVS	P	Medium	Physical Incident Evidence Preservation contributes to the Infrastructure & Virtualization Security outcome by providing AI-specific requirements that can operate within	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.

Record	GAISSF control	Control title	CCM domain	Relationship	Confidence	Rationale	Residual gap
						the cloud control environment.	
GAISSF-CRO-034-MAP-0279	D9-CTL-07	PHYSICAL INCIDENT EVIDENCE PRESERVATION	BCR	P	Medium	Physical Incident Evidence Preservation contributes to the Business Continuity Management & Operational Resilience outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0280	D9-CTL-07	PHYSICAL INCIDENT EVIDENCE PRESERVATION	SEF	S	Medium	Physical Incident Evidence Preservation contributes to the Security Incident Management, E-Discovery & Cloud Forensics outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.
GAISSF-CRO-034-MAP-0281	D9-CTL-07	PHYSICAL INCIDENT EVIDENCE PRESERVATION	LOG	S	Medium	Physical Incident Evidence Preservation contributes to the Logging & Monitoring outcome by providing AI-specific requirements that can operate within the cloud control environment.	CCM v4.1 includes cloud-provider/customer responsibility allocation and detailed control specifications not established by this GAISSF control alone.

Annex B — Source Register

Source	Version/status	Role	Official location
GAISSF Framework Standard	GAISSF-NOR-001 v1.0; published 1 Jul 2026; updated 4 Oct 2026	Normative framework architecture / conformance baseline	docs.oda3.org / official ODA3 publication channels
GAISSF Control Catalogue	GAISSF-NOR-004 v1.0; published 1 Jul 2026; updated 4 Oct 2026	Authoritative 59-control catalogue; D9 additional / conditional	docs.oda3.org / official ODA3 publication channels
CSA Cloud Controls Matrix and CAIQ	CCM v4.1 / CAIQ v4.1; released 27 Jan 2026	Primary external cloud-security baseline: 207 controls / 17 domains; CAIQ 283 questions	Official CSA CCM v4.1 release
CCM Implementation and Auditing Guidelines	CCM v4.1	Supplementary implementation and auditing guidance	Included with official CCM v4.1 release
STAR Program	Current programme; v4.1 accepted	Separate registry / assurance layer; not established by this mapping	Official CSA STAR programme