ODA3 INSTITUTE

Crosswalk — Controlled Publication

GAISSF–NIST AI RMF Mapping

Crosswalk and Evidence-Reuse Guide

DocID: CRO-022
Classification: Controlled Publication

Access & Publication Status

This document is the full crosswalk register and is a Controlled Publication. Distribution is limited to parties with an approved access request. The corresponding public Website Summary (methodology, key findings, and a representative sample) is available at https://oda3.org/ — request full Controlled Publication access via the same site.

Field	Controlled value
Document ID	CRO-022
Title	GAISSF–NIST AI Risk Management Framework Mapping
Version	1.0
Status	Publication Candidate
Classification	Crosswalk — informative
Publisher	ODA3 Institute
Legal entity	ODA3 Pvt Ltd
GAISSF baseline	GAISSF v1.0, 59 controls across D1–D9
NIST baseline	NIST AI 100-1, AI RMF 1.0, January 2023
Verification date	29 June 2026
Distribution	Public — Website/GitHub
Review trigger	Revision of GAISSF, AI RMF, or material mapping evidence

Executive Summary

CRO-022 provides a bidirectional, outcome-based mapping between the 59 GAISSF v1.0 controls and the 72 NIST AI RMF 1.0 Core subcategories. It supports implementation planning, gap analysis, evidence reuse, profile development, and internal assurance. It does not establish NIST certification, NIST endorsement, regulatory compliance, or automatic satisfaction of NIST outcomes.

Reverse coverage distribution: Indirectly Supported: 5, Not Addressed: 35, Substantially Addressed: 24, Partially Addressed: 8. These counts measure mapping coverage only; they are not a compliance score.

Notably Absent

- No NIST certification scheme is created by AI RMF 1.0.
- No NIST endorsement or approval of GAISSF was identified.
- No automatic legal or regulatory safe harbour is established.
- No evidence was identified that GAISSF and NIST AI RMF are fully equivalent.
- No universal risk-tolerance threshold is prescribed by AI RMF 1.0.

- No mapping result proves operating effectiveness.

1. Purpose and Intended Use

This crosswalk enables practitioners to relate GAISSF controls to NIST AI RMF outcomes, identify supplementary work, reuse verified evidence, and document Current and Target Profile decisions. It is an interpretive mapping, not a substitution mechanism.

2. Scope and Source Baseline

In scope: GAISSF-NOR-001 and GAISSF-NOR-004 corrected final publication editions, version 1.0, dated 29 June 2026; and NIST AI 100-1, Artificial Intelligence Risk Management Framework (AI RMF 1.0), January 2023. The NIST AI RMF Playbook and NIST AI 600-1 are supplementary and are not merged into the Core mapping. Future revisions require revalidation.

Source	Status	Role
GAISSF-NOR-001 v1.0	Normative	Framework architecture and conformance baseline
GAISSF-NOR-004 v1.0	Normative	Authoritative 59-control catalogue
NIST AI 100-1	Voluntary framework	Primary NIST Core mapping target
NIST AI RMF Playbook	Informative	Optional implementation guidance
NIST AI 600-1	Supplementary profile	Separate GenAI analysis only

3. Mapping Methodology

Mappings were evaluated at GAISSF control and NIST subcategory level. Relationship strength, reverse coverage status, and confidence are separate fields. Similar terminology alone was not treated as sufficient evidence. One-to-many and composite mappings are retained where an outcome depends on several controls.

Code	Meaning
E	Equivalent or near-equivalent; used only with exceptional evidence
SP	Strong partial
P	Partial
S	Supporting
C	Contextual
N	No material mapping
O	Outside scope
U	Unable to determine
Confidence	**Rule**
High	Clear, specific support in both primary sources
Medium-High	Strong support with modest interpretation
Medium	Reasonable but context-dependent
Low	Tentative, indirect, or ambiguous
Not Rated	No mapping, outside scope, or indeterminate

4. Function-Level Findings

GOVERN

19 NIST subcategories assessed. Coverage distribution: Indirectly Supported 3, Not Addressed 5, Substantially Addressed 11.

GAISSF provides substantial support through governance, accountability, inventory, supplier, incident, and lifecycle controls. Context-specific legal, workforce, and organizational culture outcomes may require supplementary implementation.

MAP

18 NIST subcategories assessed. Coverage distribution: Partially Addressed 3, Not Addressed 9, Substantially Addressed 4, Indirectly Supported 2.

GAISSF supports context, threat, dependency, human-oversight, and impact analysis. Broader social, mission, benefit, cost, and affected-community mapping may extend beyond security-focused controls.

MEASURE

22 NIST subcategories assessed. Coverage distribution: Partially Addressed 4, Not Addressed 14, Substantially Addressed 4.

GAISSF is comparatively detailed for adversarial testing, monitoring, drift, output integrity, safety, privacy, and assurance evidence. NIST-specific metric selection, independent TEVV, and contextual trustworthiness evaluation remain necessary.

MANAGE

13 NIST subcategories assessed. Coverage distribution: Not Addressed 7, Partially Addressed 1, Substantially Addressed 5.

GAISSF strongly supports treatment, incident response, third-party risk, monitoring, and continuous improvement. Organizations must still determine priorities, resources, acceptance decisions, and residual-risk communication in context.

5. Trustworthiness and Security Analysis

GAISSF controls materially support valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair-with-harmful-bias-managed outcomes. The mapping does not treat these characteristics as independent checkboxes; trade-offs and context remain necessary. GAISSF adds operational detail for adversarial robustness, prompt injection, model extraction, autonomous agents, supply-chain security, runtime monitoring, and incident response.

6. Evidence Reuse Guidance

Evidence family	Potential reuse	Supplementary NIST context
AI inventory and scope records	GOVERN inventory, ownership, lifecycle	Mission, risk tolerance, and affected-party context
Risk and impact assessments	MAP and MANAGE decisions	Benefits, non-monetary costs, likelihood and magnitude
Threat models and security tests	MEASURE security/resilience	Metric appropriateness and independent review
Model/data documentation	MAP knowledge limits; MEASURE transparency	Use-context limitations and affected-party communication
Monitoring and incident records	MEASURE/MANAGE tracking and response	Risk prioritization, residual risk, and stakeholder reporting
Supplier assessments and AI BOMs	GOVERN/MAP/MANAGE third-party outcomes	Contractual responsibilities and downstream use context

7. Limitations

- The AI RMF is voluntary, rights-preserving, non-sector-specific, and use-case agnostic.
- Mapping is interpretive and does not prove control implementation or effectiveness.
- GAISSF conformance does not automatically demonstrate every NIST AI RMF outcome.
- NIST Profiles are contextual; Current and Target Profiles require organizational decisions.
- The mapping must be revalidated when either baseline changes.
- The Playbook is supplementary guidance, not a set of additional mandatory requirements.

8. Conclusions

GAISSF v1.0 supplies a substantial operational and evidence-oriented foundation for many NIST AI RMF outcomes, particularly security, resilience, monitoring, third-party risk, incident response, and lifecycle assurance. Material differences remain in abstraction, organizational context, social impact framing, risk

tolerance, benefit/cost analysis, and profile-specific implementation. CRO-022 should therefore be used for planning and traceability—not as a declaration of NIST compliance or equivalence.

Annex A — GAISSF-to-NIST Mapping Register

Record	GAISSF control	Title	NIST subcategory	Rel.	Confidence	Rationale	Residual gap
CRO022-M-001	D1-CTL-01	Dataset Provenance & Poisoning Prevention	MEASURE 4.3	SP	Medium-High	GAISSF D1-CTL-01 addresses dataset provenance & poisoning prevention through Hash verification + source allowlist + poisoning detection.. This supports the NIST outcome concerning measurable performance improvements or de- clines based on consultations with relevant ai actors, in- cluding affected communities, and field data about context- relevant risks and. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-002	D1-CTL-01	Dataset Provenance & Poisoning Prevention	GOVERN 6.2	SP	Medium-High	GAISSF D1-CTL-01 addresses dataset provenance & poisoning prevention through Hash verification + source allowlist + poisoning detection.. This supports the NIST outcome concerning contingency processes are in place to handle failures or incidents in third-party data or ai systems deemed to be high-risk. categories subcategories 5.2 map the map function estab. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-003	D1-CTL-01	Dataset Provenance & Poisoning Prevention	MANAGE 2.4	SP	Medium-High	GAISSF D1-CTL-01 addresses dataset provenance & poisoning prevention through Hash verification + source allowlist + poisoning detection.. This supports the NIST outcome concerning mechanisms are in place and applied, and respon- sibilities are assigned and understood, to supersede, disengage, or deactivate ai systems that demonstrate performance or outcomes . The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-004	D1-CTL-02	Model Extraction	MAP 5.2	SP	Medium-High	GAISSF D1-CTL-02	NIST requires

		Resistance				addresses model extraction resistance through Rate limiting + diversity detection + extraction monitoring.. This supports the NIST outcome concerning practices and personnel for supporting regular en- gagement with relevant ai actors and integrating feedback about positive, negative, and unanticipated impacts are in place and do. The mapping does not establish implementation effectiveness or equivalence.	organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-005	D1-CTL-02	Model Extraction Resistance	MEASURE 2.6	SP	Medium-High	GAISSF D1-CTL-02 addresses model extraction resistance through Rate limiting + diversity detection + extraction monitoring.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-006	D1-CTL-02	Model Extraction Resistance	MANAGE 3.2	SP	Medium-High	GAISSF D1-CTL-02 addresses model extraction resistance through Rate limiting + diversity detection + extraction monitoring.. This supports the NIST outcome concerning pre- trained models which are used for develop- ment are monitored as part of ai system regular monitoring and maintenance. categories subcategories continued on next page nist ai 1. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-007	D1-CTL-03	Behavioral Drift Detection	MANAGE 4.1	SP	Medium-High	GAISSF D1-CTL-03 addresses behavioral drift detection through Baseline profiling + KL divergence monitoring + accuracy tracking.. This supports the NIST outcome concerning post-deployment ai system monitoring plans are implemented, including mechanisms for capturing and eval- uating input from users and other	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						relevant ai actors, appeal and override, . The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-008	D1-CTL-03	Behavioral Drift Detection	MANAGE 3.2	SP	Medium-High	GAISSF D1-CTL-03 addresses behavioral drift detection through Baseline profiling + KL divergence monitoring + accuracy tracking.. This supports the NIST outcome concerning pre-trained models which are used for develop- ment are monitored as part of ai system regular monitoring and maintenance. categories subcategories continued on next page nist ai 1. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-009	D1-CTL-03	Behavioral Drift Detection	MAP 5.2	SP	Medium-High	GAISSF D1-CTL-03 addresses behavioral drift detection through Baseline profiling + KL divergence monitoring + accuracy tracking.. This supports the NIST outcome concerning practices and personnel for supporting regular en-gagement with relevant ai actors and integrating feedback about positive, negative, and unanticipated impacts are in place and do. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-010	D1-CTL-04	Federated Learning Poisoning Prevention	MEASURE 2.1	P	Medium	GAISSF D1-CTL-04 addresses federated learning poisoning prevention through Gradient anomaly detection + robust aggregation.. This supports the NIST outcome concerning test sets, metrics, and details about the tools used during tevv are documented. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-011	D1-CTL-04	Federated Learning Poisoning Prevention	MEASURE 2.7	P	Medium	GAISSF D1-CTL-04 addresses federated learning poisoning prevention through Gradient anomaly detection + robust aggregation.. This supports the NIST outcome concerning ai system security and	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						resilience – as identified in the map function – are evaluated and documented. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-012	D1-CTL-04	Federated Learning Poisoning Prevention	MEASURE 4.3	P	Medium	GAISSF D1-CTL-04 addresses federated learning poisoning prevention through Gradient anomaly detection + robust aggregation.. This supports the NIST outcome concerning measurable performance improvements or de-clines based on consultations with relevant ai actors, in-cluding affected communities, and field data about context-relevant risks and. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-013	D1-CTL-05	Embedding Space Robustness	MEASURE 2.6	SP	Medium-High	GAISSF D1-CTL-05 addresses embedding space robustness through Adversarial training + certified robustness measurement.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-014	D1-CTL-05	Embedding Space Robustness	MAP 5.1	SP	Medium-High	GAISSF D1-CTL-05 addresses embedding space robustness through Adversarial training + certified robustness measurement.. This supports the NIST outcome concerning likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of ai systems in similar contexts, public incident re-. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-015	D1-CTL-05	Embedding Space Robustness	GOVERN 4.1	SP	Medium-High	GAISSF D1-CTL-05 addresses embedding space robustness through	NIST requires organization- and context-specific application;

						Adversarial training + certified robustness measurement.. This supports the NIST outcome concerning organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of ai systems to minimize. The mapping does not establish implementation effectiveness or equivalence.	additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-016	D1-CTL-06	Post-Quantum Model Signing & Crypto Hardening	MEASURE 2.1	P	Medium	GAISSF D1-CTL-06 addresses post-quantum model signing & crypto hardening through PQC signing (ML-DSA/SLH-DSA) + PQC key exchange (ML-KEM).. This supports the NIST outcome concerning test sets, metrics, and details about the tools used during tevv are documented. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-017	D1-CTL-06	Post-Quantum Model Signing & Crypto Hardening	MEASURE 2.7	P	Medium	GAISSF D1-CTL-06 addresses post-quantum model signing & crypto hardening through PQC signing (ML-DSA/SLH-DSA) + PQC key exchange (ML-KEM).. This supports the NIST outcome concerning ai system security and resilience – as identified in the map function – are evaluated and documented. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-018	D1-CTL-06	Post-Quantum Model Signing & Crypto Hardening	MEASURE 4.3	P	Medium	GAISSF D1-CTL-06 addresses post-quantum model signing & crypto hardening through PQC signing (ML-DSA/SLH-DSA) + PQC key exchange (ML-KEM).. This supports the NIST outcome concerning measurable performance improvements or de-clines based on consultations with relevant ai actors, in-cluding affected communities, and field data about context-relevant risks and. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-019	D1-CTL-07	Lora/Adapter Integrity Verification	MEASURE 4.3	SP	Medium-High	GAISSF D1-CTL-07 addresses lora/adapter integrity verification	NIST requires organization- and context-specific application;

						through Adapter scanning + provenance verification + registry allowlist.. This supports the NIST outcome concerning measurable performance improvements or de- clines based on consultations with relevant ai actors, in- cluding affected communities, and field data about context- relevant risks and. The mapping does not establish implementation effectiveness or equivalence.	additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-020	D1-CTL-07	Lora/Adapter Integrity Verification	MANAGE 2.4	SP	Medium-High	GAISSF D1-CTL-07 addresses lora/adapter integrity verification through Adapter scanning + provenance verification + registry allowlist.. This supports the NIST outcome concerning mechanisms are in place and applied, and respon- sibilities are assigned and understood, to supersede, disengage, or deactivate ai systems that demonstrate performance or outcomes . The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-021	D1-CTL-07	Lora/Adapter Integrity Verification	MANAGE 3.1	SP	Medium-High	GAISSF D1-CTL-07 addresses lora/adapter integrity verification through Adapter scanning + provenance verification + registry allowlist.. This supports the NIST outcome concerning ai risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-022	D1-CTL-08	Model Merge Attack Detection	MEASURE 2.6	P	Medium	GAISSF D1-CTL-08 addresses model merge attack detection through Pre-registration behavioural evaluation + regression testing.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						effectiveness or equivalence.	
CRO022-M-023	D1-CTL-08	Model Merge Attack Detection	MEASURE 2.1	P	Medium	GAISSF D1-CTL-08 addresses model merge attack detection through Pre-registration behavioural evaluation + regression testing.. This supports the NIST outcome concerning test sets, metrics, and details about the tools used during tevv are documented. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-024	D1-CTL-08	Model Merge Attack Detection	MEASURE 2.7	P	Medium	GAISSF D1-CTL-08 addresses model merge attack detection through Pre-registration behavioural evaluation + regression testing.. This supports the NIST outcome concerning ai system security and resilience – as identified in the map function – are evaluated and documented. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-025	D1-CTL-09	Quantization Backdoor Screening	MEASURE 2.6	SP	Medium-High	GAISSF D1-CTL-09 addresses quantization backdoor screening through Cross-precision behavioural comparison + delta threshold monitoring.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-026	D1-CTL-09	Quantization Backdoor Screening	MAP 5.2	SP	Medium-High	GAISSF D1-CTL-09 addresses quantization backdoor screening through Cross-precision behavioural comparison + delta threshold monitoring.. This supports the NIST outcome concerning practices and personnel for supporting regular en- gagement with relevant ai actors and integrating feedback about positive, negative, and unanticipated impacts are in place and do. The mapping does not establish implementation	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						effectiveness or equivalence.	
CRO022-M-027	D1-CTL-09	Quantization Backdoor Screening	MANAGE 4.1	P	Medium	GAISSF D1-CTL-09 addresses quantization backdoor screening through Cross-precision behavioural comparison + delta threshold monitoring.. This supports the NIST outcome concerning post-deployment ai system monitoring plans are implemented, including mechanisms for capturing and eval- uating input from users and other relevant ai actors, appeal and override, . The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-028	D2-CTL-01	Direct Prompt Injection Prevention	GOVERN 4.3	SP	Medium-High	GAISSF D2-CTL-01 addresses direct prompt injection prevention through Input validation + adversarial pattern matching + system prompt isolation + guardrail sidecar.. This supports the NIST outcome concerning organizational practices are in place to enable ai testing, identification of incidents, and information sharing. govern 5: processes are in place for robust engagement with releva. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-029	D2-CTL-01	Direct Prompt Injection Prevention	MEASURE 4.3	SP	Medium-High	GAISSF D2-CTL-01 addresses direct prompt injection prevention through Input validation + adversarial pattern matching + system prompt isolation + guardrail sidecar.. This supports the NIST outcome concerning measurable performance improvements or de-clines based on consultations with relevant ai actors, in-cluding affected communities, and field data about context-relevant risks and. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-030	D2-CTL-01	Direct Prompt Injection Prevention	MEASURE 2.7	SP	Medium-High	GAISSF D2-CTL-01 addresses direct prompt injection prevention through Input validation + adversarial pattern	NIST requires organization- and context-specific application; additional evidence may be needed for actors,

						matching + system prompt isolation + guardrail sidecar.. This supports the NIST outcome concerning ai system security and resilience – as identified in the map function – are evaluated and documented. The mapping does not establish implementation effectiveness or equivalence.	impacts, risk tolerance, and lifecycle context.
CRO022-M-031	D2-CTL-02	Indirect Prompt Injection Prevention	MAP 5.2	SP	Medium-High	GAISSF D2-CTL-02 addresses indirect prompt injection prevention through Contextual separation + source allowlisting + output validation + RAG sanitization pipeline.. This supports the NIST outcome concerning practices and personnel for supporting regular en- gagement with relevant ai actors and integrating feedback about positive, negative, and unanticipated impacts are in place and do. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-032	D2-CTL-02	Indirect Prompt Injection Prevention	MEASURE 2.7	SP	Medium-High	GAISSF D2-CTL-02 addresses indirect prompt injection prevention through Contextual separation + source allowlisting + output validation + RAG sanitization pipeline.. This supports the NIST outcome concerning ai system security and resilience – as identified in the map function – are evaluated and documented. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-033	D2-CTL-02	Indirect Prompt Injection Prevention	MEASURE 2.6	SP	Medium-High	GAISSF D2-CTL-02 addresses indirect prompt injection prevention through Contextual separation + source allowlisting + output validation + RAG sanitization pipeline.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						not establish implementation effectiveness or equivalence.	
CRO022-M-034	D2-CTL-03	Jailbreak Resistance Testing	MEASURE 2.6	SP	Medium-High	GAISSF D2-CTL-03 addresses jailbreak resistance testing through Quarterly red-team prompt library + adversarial training + automated refusal monitoring.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-035	D2-CTL-03	Jailbreak Resistance Testing	MAP 5.2	SP	Medium-High	GAISSF D2-CTL-03 addresses jailbreak resistance testing through Quarterly red-team prompt library + adversarial training + automated refusal monitoring.. This supports the NIST outcome concerning practices and personnel for supporting regular en- gagement with relevant ai actors and integrating feedback about positive, negative, and unanticipated impacts are in place and do. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-036	D2-CTL-03	Jailbreak Resistance Testing	GOVERN 4.1	SP	Medium-High	GAISSF D2-CTL-03 addresses jailbreak resistance testing through Quarterly red-team prompt library + adversarial training + automated refusal monitoring.. This supports the NIST outcome concerning organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of ai systems to minimize. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-037	D2-CTL-04	Multi-Modal Injection Defense	MAP 5.2	SP	Medium-High	GAISSF D2-CTL-04 addresses multi-modal injection defense through Multi-modal content scanning + steganography detection	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance,

						+ modality-specific guardrails.. This supports the NIST outcome concerning practices and personnel for supporting regular en- gagement with relevant ai actors and integrating feedback about positive, negative, and unanticipated impacts are in place and do. The mapping does not establish implementation effectiveness or equivalence.	and lifecycle context.
CRO022-M-038	D2-CTL-04	Multi-Modal Injection Defense	MEASURE 2.7	P	Medium	GAISSF D2-CTL-04 addresses multi-modal injection defense through Multi-modal content scanning + steganography detection + modality-specific guardrails.. This supports the NIST outcome concerning ai system security and resilience – as identified in the map function – are evaluated and documented. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-039	D2-CTL-04	Multi-Modal Injection Defense	MEASURE 1.2	P	Medium	GAISSF D2-CTL-04 addresses multi-modal injection defense through Multi-modal content scanning + steganography detection + modality-specific guardrails.. This supports the NIST outcome concerning appropriateness of ai metrics and effectiveness of existing controls are regularly assessed and updated, including reports of errors and potential impacts on affected communities. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-040	D2-CTL-05	Function Call/Tool Call Injection Prevention	MEASURE 2.7	SP	Medium-High	GAISSF D2-CTL-05 addresses function call/tool call injection prevention through Parameter schema validation + allowlist enforcement + sandboxed execution.. This supports the NIST outcome concerning ai system security and resilience – as identified in the map function – are evaluated and documented. The mapping does not establish implementation effectiveness or	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						equivalence.	
CRO022-M-041	D2-CTL-05	Function Call/Tool Call Injection Prevention	MAP 5.2	SP	Medium-High	GAISSF D2-CTL-05 addresses function call/tool call injection prevention through Parameter schema validation + allowlist enforcement + sandboxed execution.. This supports the NIST outcome concerning practices and personnel for supporting regular engagement with relevant ai actors and integrating feedback about positive, negative, and unanticipated impacts are in place and do. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-042	D2-CTL-05	Function Call/Tool Call Injection Prevention	MEASURE 1.1	P	Medium	GAISSF D2-CTL-05 addresses function call/tool call injection prevention through Parameter schema validation + allowlist enforcement + sandboxed execution.. This supports the NIST outcome concerning approaches and metrics for measurement of ai risks enumerated during the map function are selected for implementation starting with the most significant ai risks. the risks or tr. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-043	D2-CTL-06	Cross-Context Hijacking Mitigation	MEASURE 2.7	P	Medium	GAISSF D2-CTL-06 addresses cross-context hijacking mitigation through Context window segmentation + prompt anchoring + attention boundary enforcement.. This supports the NIST outcome concerning ai system security and resilience – as identified in the map function – are evaluated and documented. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-044	D2-CTL-06	Cross-Context Hijacking Mitigation	MEASURE 2.1	P	Medium	GAISSF D2-CTL-06 addresses cross-context hijacking mitigation through Context window segmentation + prompt anchoring + attention boundary enforcement.. This supports the NIST outcome concerning test sets, metrics, and details	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						about the tools used during tevv are documented. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-045	D2-CTL-06	Cross-Context Hijacking Mitigation	GOVERN 4.3	S	Medium	GAISSF D2-CTL-06 addresses cross-context hijacking mitigation through Context window segmentation + prompt anchoring + attention boundary enforcement.. This supports the NIST outcome concerning organizational practices are in place to enable ai testing, identification of incidents, and information sharing. govern 5: processes are in place for robust engagement with releva. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-046	D3-CTL-01	Least Agency Enforcement	MAP 3.5	SP	Medium-High	GAISSF D3-CTL-01 addresses least agency enforcement through Role-based tool scoping + policy-as-code + dynamic permission revocation.. This supports the NIST outcome concerning processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the govern function. map 4: risks and benefits are mapped for al. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-047	D3-CTL-01	Least Agency Enforcement	MEASURE 2.9	SP	Medium-High	GAISSF D3-CTL-01 addresses least agency enforcement through Role-based tool scoping + policy-as-code + dynamic permission revocation.. This supports the NIST outcome concerning the ai model is explained, validated, and docu-mented, and ai system output is interpreted within its context – as identified in the map function – to inform responsible use and g. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-048	D3-CTL-01	Least Agency Enforcement	MEASURE 4.3	SP	Medium-High	GAISSF D3-CTL-01 addresses least agency enforcement through Role-based tool scoping +	NIST requires organization- and context-specific application; additional evidence may

						policy-as-code + dynamic permission revocation.. This supports the NIST outcome concerning measurable performance improvements or de- clines based on consultations with relevant ai actors, in- cluding affected communities, and field data about context- relevant risks and. The mapping does not establish implementation effectiveness or equivalence.	be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-049	D3-CTL-02	Inter-Agent Communication Security	MAP 2.3	P	Medium	GAISSF D3-CTL-02 addresses inter-agent communication security through mTLS for agent mesh + message signing + payload validation.. This supports the NIST outcome concerning scientific integrity and tevv considerations are iden- tified and documented, including those related to experimental design, data collection and selection (e.g., availability, rep. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-050	D3-CTL-02	Inter-Agent Communication Security	MEASURE 1.3	P	Medium	GAISSF D3-CTL-02 addresses inter-agent communication security through mTLS for agent mesh + message signing + payload validation.. This supports the NIST outcome concerning internal experts who did not serve as front-line developers for the system and/or independent assessors are in- volved in regular assessments and updates. domain experts, users, ai. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-051	D3-CTL-02	Inter-Agent Communication Security	MEASURE 2.7	P	Medium	GAISSF D3-CTL-02 addresses inter-agent communication security through mTLS for agent mesh + message signing + payload validation.. This supports the NIST outcome concerning ai system security and resilience – as identified in the map function – are evaluated and documented. The mapping does not establish implementation effectiveness or	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						equivalence.	
CRO022-M-052	D3-CTL-03	Agentic Prompt Chaining Detection	MEASURE 2.7	P	Medium	GAISSF D3-CTL-03 addresses agentic prompt chaining detection through Cross-session behavioural correlation + chain pattern detection + anomaly scoring.. This supports the NIST outcome concerning ai system security and resilience – as identified in the map function – are evaluated and documented. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-053	D3-CTL-03	Agentic Prompt Chaining Detection	MAP 1.1	P	Medium	GAISSF D3-CTL-03 addresses agentic prompt chaining detection through Cross-session behavioural correlation + chain pattern detection + anomaly scoring.. This supports the NIST outcome concerning intended purposes, potentially beneficial uses, context- specific laws, norms and expectations, and prospective settings in which the ai system will be deployed are understood and . The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-054	D3-CTL-03	Agentic Prompt Chaining Detection	MAP 1.6	P	Medium	GAISSF D3-CTL-03 addresses agentic prompt chaining detection through Cross-session behavioural correlation + chain pattern detection + anomaly scoring.. This supports the NIST outcome concerning system requirements (e.g., “the system shall respect the privacy of its users”) are elicited from and understood by rel- evant ai actors. design decisions take socio-technical impl. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-055	D3-CTL-04	Embodied Ai Safety Controls	MEASURE 2.6	SP	Medium-High	GAISSF D3-CTL-04 addresses embodied ai safety controls through Sensor integrity verification + safety interlocks + fail-safe state enforcement.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks –	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-056	D3-CTL-04	Embodied Ai Safety Controls	GOVERN 4.1	SP	Medium-High	GAISSF D3-CTL-04 addresses embodied ai safety controls through Sensor integrity verification + safety interlocks + fail-safe state enforcement.. This supports the NIST outcome concerning organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of ai systems to minimize. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-057	D3-CTL-04	Embodied Ai Safety Controls	MAP 2.3	P	Medium	GAISSF D3-CTL-04 addresses embodied ai safety controls through Sensor integrity verification + safety interlocks + fail-safe state enforcement.. This supports the NIST outcome concerning scientific integrity and tevv considerations are iden- tified and documented, including those related to experimental design, data collection and selection (e.g., availability, rep. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-058	D3-CTL-05	Multi-Agent Trust Chain Attestation	MEASURE 2.7	P	Medium	GAISSF D3-CTL-05 addresses multi-agent trust chain attestation through SPIFFE/SPIRE workload identity + short-lived certificates + continuous attestation.. This supports the NIST outcome concerning ai system security and resilience – as identified in the map function – are evaluated and documented. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-059	D3-CTL-05	Multi-Agent Trust Chain Attestation	MAP 1.1	P	Medium	GAISSF D3-CTL-05 addresses multi-agent trust chain attestation through SPIFFE/SPIRE	NIST requires organization- and context-specific application; additional evidence may

						workload identity + short-lived certificates + continuous attestation.. This supports the NIST outcome concerning intended purposes, potentially beneficial uses, context- specific laws, norms and expectations, and prospective settings in which the ai system will be deployed are understood and . The mapping does not establish implementation effectiveness or equivalence.	be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-060	D3-CTL-05	Multi-Agent Trust Chain Attestation	MAP 1.6	P	Medium	GAISSF D3-CTL-05 addresses multi-agent trust chain attestation through SPIFFE/SPIRE workload identity + short-lived certificates + continuous attestation.. This supports the NIST outcome concerning system requirements (e.g., “the system shall respect the privacy of its users”) are elicited from and understood by rel- evant ai actors. design decisions take socio-technical impl. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-061	D3-CTL-06	Persistent Memory Exfiltration Prevention	MEASURE 2.7	P	Medium	GAISSF D3-CTL-06 addresses persistent memory exfiltration prevention through User-scoped memory isolation + encryption at rest + query-level access controls.. This supports the NIST outcome concerning ai system security and resilience – as identified in the map function – are evaluated and documented. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-062	D3-CTL-06	Persistent Memory Exfiltration Prevention	MAP 1.1	P	Medium	GAISSF D3-CTL-06 addresses persistent memory exfiltration prevention through User-scoped memory isolation + encryption at rest + query-level access controls.. This supports the NIST outcome concerning intended purposes, potentially beneficial uses, context-specific laws, norms and expectations, and prospective settings in which the ai system will	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						be deployed are understood and . The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-063	D3-CTL-06	Persistent Memory Exfiltration Prevention	MAP 1.6	P	Medium	GAISSF D3-CTL-06 addresses persistent memory exfiltration prevention through User-scoped memory isolation + encryption at rest + query-level access controls.. This supports the NIST outcome concerning system requirements (e.g., “the system shall respect the privacy of its users”) are elicited from and understood by rel- evant ai actors. design decisions take socio-technical impl. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-064	D3-CTL-07	Secure Memory Lifecycle Management	MAP 3.5	SP	Medium-High	GAISSF D3-CTL-07 addresses secure memory lifecycle management through Cryptographic deletion + lifecycle policy enforcement + retention auditing.. This supports the NIST outcome concerning processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the govern function. map 4: risks and benefits are mapped for al. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-065	D3-CTL-07	Secure Memory Lifecycle Management	MEASURE 2.9	SP	Medium-High	GAISSF D3-CTL-07 addresses secure memory lifecycle management through Cryptographic deletion + lifecycle policy enforcement + retention auditing.. This supports the NIST outcome concerning the ai model is explained, validated, and docu- mented, and ai system output is interpreted within its context – as identified in the map function – to inform responsible use and g. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-066	D3-CTL-07	Secure Memory Lifecycle Management	GOVERN 2.3	SP	Medium-High	GAISSF D3-CTL-07 addresses secure memory lifecycle management through Cryptographic	NIST requires organization- and context-specific application; additional evidence may

						deletion + lifecycle policy enforcement + retention auditing.. This supports the NIST outcome concerning executive leadership of the organization takes responsibility for decisions about risks associated with ai system development and deployment. govern 3: workforce diversity, equit. The mapping does not establish implementation effectiveness or equivalence.	be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-067	D4-CTL-01	Ai Bill Of Materials (Ai Bom) Maintenance	GOVERN 6.2	SP	Medium-High	GAISSF D4-CTL-01 addresses ai bill of materials (ai bom) maintenance through Automated BOM generation + version tracking + registry synchronization.. This supports the NIST outcome concerning contingency processes are in place to handle failures or incidents in third-party data or ai systems deemed to be high-risk. categories subcategories 5.2 map the map function estab. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-068	D4-CTL-01	Ai Bill Of Materials (Ai Bom) Maintenance	MEASURE 4.3	SP	Medium-High	GAISSF D4-CTL-01 addresses ai bill of materials (ai bom) maintenance through Automated BOM generation + version tracking + registry synchronization.. This supports the NIST outcome concerning measurable performance improvements or declines based on consultations with relevant ai actors, including affected communities, and field data about context-relevant risks and. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-069	D4-CTL-01	Ai Bill Of Materials (Ai Bom) Maintenance	GOVERN 1.6	SP	Medium-High	GAISSF D4-CTL-01 addresses ai bill of materials (ai bom) maintenance through Automated BOM generation + version tracking + registry synchronization.. This supports the NIST outcome concerning mechanisms are in place	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						to inventory ai systems and are resourced according to organizational risk priorities. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-070	D4-CTL-02	Model File & Artifact Scanning	GOVERN 5.2	SP	Medium-High	GAISSF D4-CTL-02 addresses model file & artifact scanning through Static analysis + deserialization sandboxing + signature verification.. This supports the NIST outcome concerning mechanisms are established to enable the team that developed or deployed ai systems to regularly incorporate adjudicated feedback from relevant ai actors into system design and imp. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-071	D4-CTL-02	Model File & Artifact Scanning	GOVERN 6.1	SP	Medium-High	GAISSF D4-CTL-02 addresses model file & artifact scanning through Static analysis + deserialization sandboxing + signature verification.. This supports the NIST outcome concerning policies and procedures are in place that address ai risks associated with third-party entities, including risks of in- fringement of a third-party's intellectual property or other. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-072	D4-CTL-02	Model File & Artifact Scanning	GOVERN 6.2	SP	Medium-High	GAISSF D4-CTL-02 addresses model file & artifact scanning through Static analysis + deserialization sandboxing + signature verification.. This supports the NIST outcome concerning contingency processes are in place to handle failures or incidents in third-party data or ai systems deemed to be high-risk. categories subcategories 5.2 map the map function estab. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-073	D4-CTL-03	Model Hub & Registry Vetting	GOVERN 5.2	SP	Medium-High	GAISSF D4-CTL-03 addresses model hub &	NIST requires organization- and context-

						registry vetting through Provenance verification + license compliance + security scorecard.. This supports the NIST outcome concerning mechanisms are established to enable the team that developed or deployed ai systems to regularly incorporate adjudicated feedback from relevant ai actors into system design and imp. The mapping does not establish implementation effectiveness or equivalence.	specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-074	D4-CTL-03	Model Hub & Registry Vetting	GOVERN 6.1	SP	Medium-High	GAISSF D4-CTL-03 addresses model hub & registry vetting through Provenance verification + license compliance + security scorecard.. This supports the NIST outcome concerning policies and procedures are in place that address ai risks associated with third-party entities, including risks of in-fringement of a third-party's intellectual property or other. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-075	D4-CTL-03	Model Hub & Registry Vetting	GOVERN 6.2	SP	Medium-High	GAISSF D4-CTL-03 addresses model hub & registry vetting through Provenance verification + license compliance + security scorecard.. This supports the NIST outcome concerning contingency processes are in place to handle failures or incidents in third-party data or ai systems deemed to be high-risk. categories subcategories 5.2 map the map function estab. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-076	D4-CTL-04	Mcp Server Behavioral Monitoring	MANAGE 3.1	SP	Medium-High	GAISSF D4-CTL-04 addresses mcp server behavioral monitoring through Tool-call logging + anomaly detection + access control enforcement.. This supports the NIST outcome concerning ai risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented. The	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-077	D4-CTL-04	Mcp Server Behavioral Monitoring	GOVERN 5.2	SP	Medium-High	GAISSF D4-CTL-04 addresses mcp server behavioral monitoring through Tool-call logging + anomaly detection + access control enforcement.. This supports the NIST outcome concerning mechanisms are established to enable the team that developed or deployed ai systems to regularly incorporate adjudicated feedback from relevant ai actors into system design and imp. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-078	D4-CTL-04	Mcp Server Behavioral Monitoring	GOVERN 6.2	SP	Medium-High	GAISSF D4-CTL-04 addresses mcp server behavioral monitoring through Tool-call logging + anomaly detection + access control enforcement.. This supports the NIST outcome concerning contingency processes are in place to handle failures or incidents in third-party data or ai systems deemed to be high-risk. categories subcategories 5.2 map the map function estab. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-079	D4-CTL-05	Third-Party Ai Api Security Assessment	MAP 1.6	SP	Medium-High	GAISSF D4-CTL-05 addresses third-party ai api security assessment through Contractual security requirements + penetration testing + data flow mapping.. This supports the NIST outcome concerning system requirements (e.g., “the system shall respect the privacy of its users”) are elicited from and understood by rel- evant ai actors. design decisions take socio-technical impl. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-080	D4-CTL-05	Third-Party Ai Api Security Assessment	MAP 4.1	P	Medium	GAISSF D4-CTL-05 addresses third-party ai api security assessment through Contractual security requirements +	NIST requires organization- and context-specific application; additional evidence may be needed for actors,

						penetration testing + data flow mapping.. This supports the NIST outcome concerning approaches for mapping ai technology and legal risks of its components – including the use of third-party data or soft- ware – are in place, followed, and documented, as are risks . The mapping does not establish implementation effectiveness or equivalence.	impacts, risk tolerance, and lifecycle context.
CRO022-M-081	D4-CTL-05	Third-Party Ai Api Security Assessment	GOVERN 5.2	P	Medium	GAISSF D4-CTL-05 addresses third-party ai api security assessment through Contractual security requirements + penetration testing + data flow mapping.. This supports the NIST outcome concerning mechanisms are established to enable the team that developed or deployed ai systems to regularly incorporate adjudicated feedback from relevant ai actors into system design and imp. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-082	D4-CTL-06	Shadow Ai Discovery & Governance	GOVERN 5.2	SP	Medium-High	GAISSF D4-CTL-06 addresses shadow ai discovery & governance through Network traffic analysis + SaaS discovery + policy enforcement.. This supports the NIST outcome concerning mechanisms are established to enable the team that developed or deployed ai systems to regularly incorporate adjudicated feedback from relevant ai actors into system design and imp. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-083	D4-CTL-06	Shadow Ai Discovery & Governance	MAP 3.5	SP	Medium-High	GAISSF D4-CTL-06 addresses shadow ai discovery & governance through Network traffic analysis + SaaS discovery + policy enforcement.. This supports the NIST outcome concerning processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the govern function.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						map 4: risks and benefits are mapped for al. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-084	D4-CTL-06	Shadow Ai Discovery & Governance	MEASURE 4.3	SP	Medium-High	GAISSF D4-CTL-06 addresses shadow ai discovery & governance through Network traffic analysis + SaaS discovery + policy enforcement.. This supports the NIST outcome concerning measurable performance improvements or de-clines based on consultations with relevant ai actors, in-cluding affected communities, and field data about context-relevant risks and. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-085	D4-CTL-07	Ai Software Composition Analysis (Sca)	GOVERN 5.2	SP	Medium-High	GAISSF D4-CTL-07 addresses ai software composition analysis (sca) through Dependency scanning + CVE matching + automated patching.. This supports the NIST outcome concerning mechanisms are established to enable the team that developed or deployed ai systems to regularly incorporate adjudicated feedback from relevant ai actors into system design and imp. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-086	D4-CTL-07	Ai Software Composition Analysis (Sca)	MAP 3.5	P	Medium	GAISSF D4-CTL-07 addresses ai software composition analysis (sca) through Dependency scanning + CVE matching + automated patching.. This supports the NIST outcome concerning processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the govern function. map 4: risks and benefits are mapped for al. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-087	D4-CTL-07	Ai Software Composition Analysis (Sca)	MANAGE 4.3	P	Medium	GAISSF D4-CTL-07 addresses ai software composition analysis (sca) through Dependency	NIST requires organization- and context-specific application; additional evidence may

						scanning + CVE matching + automated patching.. This supports the NIST outcome concerning incidents and errors are communicated to relevant ai actors, including affected communities. processes for track- ing, responding to, and recovering from incidents and errors are f. The mapping does not establish implementation effectiveness or equivalence.	be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-088	D5-CTL-01	Harmful Content Blocking	GOVERN 4.1	SP	Medium-High	GAISSF D5-CTL-01 addresses harmful content blocking through Content safety classifier + refusal engine.. This supports the NIST outcome concerning organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of ai systems to minimize. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-089	D5-CTL-01	Harmful Content Blocking	MEASURE 2.6	SP	Medium-High	GAISSF D5-CTL-01 addresses harmful content blocking through Content safety classifier + refusal engine.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-090	D5-CTL-01	Harmful Content Blocking	MAP 5.1	P	Medium	GAISSF D5-CTL-01 addresses harmful content blocking through Content safety classifier + refusal engine.. This supports the NIST outcome concerning likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of ai systems in similar contexts, public incident re-. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-091	D5-CTL-02	Pii Leakage Prevention	MEASURE 2.6	SP	Medium-High	GAISSF D5-CTL-02	NIST requires

						addresses pii leakage prevention through PII detection + masking + access controls.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-092	D5-CTL-02	Pii Leakage Prevention	GOVERN 4.1	SP	Medium-High	GAISSF D5-CTL-02 addresses pii leakage prevention through PII detection + masking + access controls.. This supports the NIST outcome concerning organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of ai systems to minimize. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-093	D5-CTL-02	Pii Leakage Prevention	MAP 2.3	P	Medium	GAISSF D5-CTL-02 addresses pii leakage prevention through PII detection + masking + access controls.. This supports the NIST outcome concerning scientific integrity and tevv considerations are iden- tified and documented, including those related to experimental design, data collection and selection (e.g., availability, rep. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-094	D5-CTL-03	Copyright Detection	MEASURE 2.6	SP	Medium-High	GAISSF D5-CTL-03 addresses copyright detection through n-gram overlap detection + refusal.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

CRO022-M-095	D5-CTL-03	Copyright Detection	GOVERN 4.1	SP	Medium-High	GAISSF D5-CTL-03 addresses copyright detection through n-gram overlap detection + refusal.. This supports the NIST outcome concerning organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of ai systems to minimize. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-096	D5-CTL-03	Copyright Detection	MAP 2.3	P	Medium	GAISSF D5-CTL-03 addresses copyright detection through n-gram overlap detection + refusal.. This supports the NIST outcome concerning scientific integrity and tevv considerations are iden- tified and documented, including those related to experimental design, data collection and selection (e.g., availability, rep. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-097	D5-CTL-04	Ai Watermarking Robustness	MEASURE 2.6	SP	Medium-High	GAISSF D5-CTL-04 addresses ai watermarking robustness through C2PA-compliant watermarking + tamper resistance testing.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-098	D5-CTL-04	Ai Watermarking Robustness	GOVERN 4.3	SP	Medium-High	GAISSF D5-CTL-04 addresses ai watermarking robustness through C2PA-compliant watermarking + tamper resistance testing.. This supports the NIST outcome concerning organizational practices are in place to enable ai testing, identification of incidents, and information sharing. govern 5: processes are in place for robust engagement with releva. The mapping does not establish implementation	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						effectiveness or equivalence.	
CRO022-M-099	D5-CTL-04	Ai Watermarking Robustness	MAP 5.1	SP	Medium-High	GAISSF D5-CTL-04 addresses ai watermarking robustness through C2PA-compliant watermarking + tamper resistance testing.. This supports the NIST outcome concerning likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of ai systems in similar contexts, public incident re-. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-100	D5-CTL-05	Privacy-By-Design Verification	MEASURE 2.6	SP	Medium-High	GAISSF D5-CTL-05 addresses privacy-by-design verification through Data minimization + purpose limitation + machine unlearning.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-101	D5-CTL-05	Privacy-By-Design Verification	GOVERN 4.1	SP	Medium-High	GAISSF D5-CTL-05 addresses privacy-by-design verification through Data minimization + purpose limitation + machine unlearning.. This supports the NIST outcome concerning organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of ai systems to minimize. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-102	D5-CTL-05	Privacy-By-Design Verification	MAP 1.6	P	Medium	GAISSF D5-CTL-05 addresses privacy-by-design verification through Data minimization + purpose limitation + machine unlearning.. This supports the NIST outcome concerning system requirements (e.g., “the system shall respect the	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						privacy of its users”) are elicited from and understood by rel- evant ai actors. design decisions take socio-technical impl. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-103	D5-CTL-06	Privacy-Preserving Ml Validation	MEASURE 2.6	SP	Medium-High	GAISSF D5-CTL-06 addresses privacy-preserving ml validation through Differential privacy + membership inference testing.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-104	D5-CTL-06	Privacy-Preserving Ml Validation	GOVERN 4.1	SP	Medium-High	GAISSF D5-CTL-06 addresses privacy-preserving ml validation through Differential privacy + membership inference testing.. This supports the NIST outcome concerning organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of ai systems to minimize. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-105	D5-CTL-06	Privacy-Preserving Ml Validation	MAP 2.3	P	Medium	GAISSF D5-CTL-06 addresses privacy-preserving ml validation through Differential privacy + membership inference testing.. This supports the NIST outcome concerning scientific integrity and tevv considerations are iden- tified and documented, including those related to experimental design, data collection and selection (e.g., availability, rep. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-106	D6-CTL-01	Human-In-The-Loop For High-Risk Actions	MEASURE 4.3	SP	Medium-High	GAISSF D6-CTL-01 addresses human-in-the-loop for high-risk actions through Approval workflow + policy	NIST requires organization- and context-specific application; additional evidence may be needed for actors,

						enforcement + audit log.. This supports the NIST outcome concerning measurable performance improvements or de- clines based on consultations with relevant ai actors, in- cluding affected communities, and field data about context- relevant risks and. The mapping does not establish implementation effectiveness or equivalence.	impacts, risk tolerance, and lifecycle context.
CRO022-M-107	D6-CTL-01	Human-In-The-Loop For High-Risk Actions	GOVERN 1.7	SP	Medium-High	GAISSF D6-CTL-01 addresses human-in-the-loop for high-risk actions through Approval workflow + policy enforcement + audit log.. This supports the NIST outcome concerning processes and procedures are in place for decom- missioning and phasing out ai systems safely and in a man- ner that does not increase risks or decrease the organization’s trustwor. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-108	D6-CTL-01	Human-In-The-Loop For High-Risk Actions	GOVERN 3.2	SP	Medium-High	GAISSF D6-CTL-01 addresses human-in-the-loop for high-risk actions through Approval workflow + policy enforcement + audit log.. This supports the NIST outcome concerning policies and procedures are in place to define and differentiate roles and responsibilities for human-ai configura- tions and oversight of ai systems. govern 4: organizational team. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-109	D6-CTL-02	Audit Trail Completeness	GOVERN 4.3	SP	Medium-High	GAISSF D6-CTL-02 addresses audit trail completeness through Structured logging + SIEM integration + retention enforcement.. This supports the NIST outcome concerning organizational practices are in place to enable ai testing, identification of incidents, and information sharing. govern 5: processes are in place for robust engagement with releva. The mapping does not establish	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						implementation effectiveness or equivalence.	
CRO022-M-110	D6-CTL-02	Audit Trail Completeness	MEASURE 4.3	SP	Medium-High	GAISSF D6-CTL-02 addresses audit trail completeness through Structured logging + SIEM integration + retention enforcement.. This supports the NIST outcome concerning measurable performance improvements or de- clines based on consultations with relevant ai actors, in- cluding affected communities, and field data about context- relevant risks and. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-111	D6-CTL-02	Audit Trail Completeness	GOVERN 1.7	P	Medium	GAISSF D6-CTL-02 addresses audit trail completeness through Structured logging + SIEM integration + retention enforcement.. This supports the NIST outcome concerning processes and procedures are in place for decom- missioning and phasing out ai systems safely and in a man- ner that does not increase risks or decrease the organization’s trustwor. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-112	D6-CTL-03	Ai Model Card Completeness	GOVERN 1.7	P	Medium	GAISSF D6-CTL-03 addresses ai model card completeness through Standardized template + version control + public accessibility.. This supports the NIST outcome concerning processes and procedures are in place for decom- missioning and phasing out ai systems safely and in a man- ner that does not increase risks or decrease the organization’s trustwor. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-113	D6-CTL-03	Ai Model Card Completeness	GOVERN 2.3	P	Medium	GAISSF D6-CTL-03 addresses ai model card completeness through Standardized template + version control + public accessibility.. This supports the NIST outcome concerning executive leadership of	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						the organization takes re- sponsibility for decisions about risks associated with ai system development and deployment. govern 3: workforce diversity, equit. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-114	D6-CTL-03	Ai Model Card Completeness	GOVERN 3.2	P	Medium	GAISSF D6-CTL-03 addresses ai model card completeness through Standardized template + version control + public accessibility.. This supports the NIST outcome concerning policies and procedures are in place to define and differentiate roles and responsibilities for human-ai configura- tions and oversight of ai systems. govern 4: organizational team. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-115	D6-CTL-04	Ai Incident Response Readiness	MEASURE 4.3	SP	Medium-High	GAISSF D6-CTL-04 addresses ai incident response readiness through AI-IR runbook + tabletop exercises + containment automation.. This supports the NIST outcome concerning measurable performance improvements or de- clines based on consultations with relevant ai actors, in- cluding affected communities, and field data about context-relevant risks and. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-116	D6-CTL-04	Ai Incident Response Readiness	GOVERN 1.7	SP	Medium-High	GAISSF D6-CTL-04 addresses ai incident response readiness through AI-IR runbook + tabletop exercises + containment automation.. This supports the NIST outcome concerning processes and procedures are in place for decom- missioning and phasing out ai systems safely and in a man- ner that does not increase risks or decrease the organization’s trustwor. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-117	D6-CTL-04	Ai Incident Response	GOVERN 1.4	SP	Medium-High	GAISSF D6-CTL-04	NIST requires

		Readiness				addresses ai incident response readiness through AI-IR runbook + tabletop exercises + containment automation.. This supports the NIST outcome concerning the risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities. categories subcat. The mapping does not establish implementation effectiveness or equivalence.	organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-118	D6-CTL-05	Model Deprecation & Decommissioning	GOVERN 1.5	SP	Medium-High	GAISSF D6-CTL-05 addresses model deprecation & decommissioning through Access revocation + decommission audit + scheduled lifecycle.. This supports the NIST outcome concerning ongoing monitoring and periodic review of the risk management process and its outcomes are planned and or- ganizational roles and responsibilities clearly defined, including determ. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-119	D6-CTL-05	Model Deprecation & Decommissioning	MANAGE 4.1	SP	Medium-High	GAISSF D6-CTL-05 addresses model deprecation & decommissioning through Access revocation + decommission audit + scheduled lifecycle.. This supports the NIST outcome concerning post-deployment ai system monitoring plans are implemented, including mechanisms for capturing and eval- uating input from users and other relevant ai actors, appeal and override, . The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-120	D6-CTL-05	Model Deprecation & Decommissioning	GOVERN 1.7	SP	Medium-High	GAISSF D6-CTL-05 addresses model deprecation & decommissioning through Access revocation + decommission audit + scheduled lifecycle.. This supports the NIST outcome concerning processes and procedures are in place for decom-	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						missioning and phasing out ai systems safely and in a man- ner that does not increase risks or decrease the organization's trustwor. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-121	D6-CTL-06	Third-Party Ai Vendor Governance	MEASURE 4.3	SP	Medium-High	GAISSF D6-CTL-06 addresses third-party ai vendor governance through Contractual security requirements + annual assessment + audit rights.. This supports the NIST outcome concerning measurable performance improvements or de- clines based on consultations with relevant ai actors, in- cluding affected communities, and field data about context- relevant risks and. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-122	D6-CTL-06	Third-Party Ai Vendor Governance	GOVERN 5.2	SP	Medium-High	GAISSF D6-CTL-06 addresses third-party ai vendor governance through Contractual security requirements + annual assessment + audit rights.. This supports the NIST outcome concerning mechanisms are established to enable the team that developed or deployed ai systems to regularly incorporate adjudicated feedback from relevant ai actors into system design and imp. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-123	D6-CTL-06	Third-Party Ai Vendor Governance	MANAGE 4.3	SP	Medium-High	GAISSF D6-CTL-06 addresses third-party ai vendor governance through Contractual security requirements + annual assessment + audit rights.. This supports the NIST outcome concerning incidents and errors are communicated to relevant ai actors, including affected communities. processes for track- ing, responding to, and recovering from incidents and errors are f. The mapping does not establish implementation	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						effectiveness or equivalence.	
CRO022-M-124	D6-CTL-07	Ai Resilience & Business Continuity	GOVERN 1.7	SP	Medium-High	GAISSF D6-CTL-07 addresses ai resilience & business continuity through Failover systems + degraded mode + RTO/RPO definition.. This supports the NIST outcome concerning processes and procedures are in place for decom- missioning and phasing out ai systems safely and in a man- ner that does not increase risks or decrease the organization's trustwor. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-125	D6-CTL-07	Ai Resilience & Business Continuity	GOVERN 3.2	SP	Medium-High	GAISSF D6-CTL-07 addresses ai resilience & business continuity through Failover systems + degraded mode + RTO/RPO definition.. This supports the NIST outcome concerning policies and procedures are in place to define and differentiate roles and responsibilities for human-ai configura- tions and oversight of ai systems. govern 4: organizational team. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-126	D6-CTL-07	Ai Resilience & Business Continuity	GOVERN 4.1	SP	Medium-High	GAISSF D6-CTL-07 addresses ai resilience & business continuity through Failover systems + degraded mode + RTO/RPO definition.. This supports the NIST outcome concerning organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of ai systems to minimize. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-127	D7-CTL-H01	Ai-Generated Phishing Simulation	GOVERN 2.2	C	Low	GAISSF D7-CTL-H01 addresses ai-generated phishing simulation through Simulation campaigns + click tracking + remedial training.. This supports the NIST outcome concerning the organization's personnel and partners receive ai risk management training	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						to enable them to perform their du- ties and responsibilities consistent with related policies, proce-. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-128	D7-CTL-H02	Deepfake Detection Training	GOVERN 4.3	P	Medium	GAISSF D7-CTL-H02 addresses deepfake detection training through Training modules + quiz + simulated attacks.. This supports the NIST outcome concerning organizational practices are in place to enable ai testing, identification of incidents, and information sharing. govern 5: processes are in place for robust engagement with releva. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-129	D7-CTL-H02	Deepfake Detection Training	GOVERN 6.2	P	Medium	GAISSF D7-CTL-H02 addresses deepfake detection training through Training modules + quiz + simulated attacks.. This supports the NIST outcome concerning contingency processes are in place to handle failures or incidents in third-party data or ai systems deemed to be high-risk. categories subcategories 5.2 map the map function estab. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-130	D7-CTL-H02	Deepfake Detection Training	MEASURE 4.3	P	Medium	GAISSF D7-CTL-H02 addresses deepfake detection training through Training modules + quiz + simulated attacks.. This supports the NIST outcome concerning measurable performance improvements or de- clines based on consultations with relevant ai actors, in- cluding affected communities, and field data about context-relevant risks and. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-131	D7-CTL-H03	Out-Of-Band Authentication	GOVERN 1.4	P	Medium	GAISSF D7-CTL-H03 addresses out-of-band authentication through Independent channel verification + policy enforcement.. This	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance,

						supports the NIST outcome concerning the risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities. categories subcat. The mapping does not establish implementation effectiveness or equivalence.	and lifecycle context.
CRO022-M-132	D7-CTL-H03	Out-Of-Band Authentication	GOVERN 1.5	P	Medium	GAISSF D7-CTL-H03 addresses out-of-band authentication through Independent channel verification + policy enforcement.. This supports the NIST outcome concerning ongoing monitoring and periodic review of the risk management process and its outcomes are planned and or- ganizational roles and responsibilities clearly defined, including determ. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-133	D7-CTL-H03	Out-Of-Band Authentication	GOVERN 1.7	P	Medium	GAISSF D7-CTL-H03 addresses out-of-band authentication through Independent channel verification + policy enforcement.. This supports the NIST outcome concerning processes and procedures are in place for decom- missioning and phasing out ai systems safely and in a man- ner that does not increase risks or decrease the organization’s trustwor. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-134	D7-CTL-H04	Ai Social Engineering Ir	GOVERN 2.2	C	Low	GAISSF D7-CTL-H04 addresses ai social engineering ir through Tabletop exercises + IR plan + verification triggers.. This supports the NIST outcome concerning the organization’s personnel and partners receive ai risk management training to enable them to perform their du- ties and responsibilities consistent with related policies, proce-. The mapping does not establish implementation	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						effectiveness or equivalence.	
CRO022-M-135	D7-CTL-H05	Ai-Enhanced External Attack Defense	GOVERN 5.1	C	Low	GAISSF D7-CTL-H05 addresses ai-enhanced external attack defense through AI-generated phishing detection + SOC tuning + response automation.. This supports the NIST outcome concerning organizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the ai system. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-136	D8-CTL-01	Eu Ai Act Risk Tier Mapping	GOVERN 6.2	S	Medium	GAISSF D8-CTL-01 addresses eu ai act risk tier mapping through Risk classification framework + conformity assessment.. This supports the NIST outcome concerning contingency processes are in place to handle failures or incidents in third-party data or ai systems deemed to be high-risk. categories subcategories 5.2 map the map function estab. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-137	D8-CTL-01	Eu Ai Act Risk Tier Mapping	MAP 2.2	S	Medium	GAISSF D8-CTL-01 addresses eu ai act risk tier mapping through Risk classification framework + conformity assessment.. This supports the NIST outcome concerning information about the ai system’s knowledge limits and how system output may be utilized and overseen by humans is documented. documentation provides sufficient information to assi. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-138	D8-CTL-01	Eu Ai Act Risk Tier Mapping	MAP 3.2	S	Medium	GAISSF D8-CTL-01 addresses eu ai act risk tier mapping through Risk classification framework + conformity assessment.. This supports the NIST outcome concerning potential costs, including non-monetary costs, which result from expected or realized ai	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						errors or system functionality and trustworthiness – as connected to organizational risk to. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-139	D8-CTL-02	Iso 42001 Gap Analysis	GOVERN 5.2	P	Medium	GAISSF D8-CTL-02 addresses iso 42001 gap analysis through Gap analysis methodology + remediation tracking.. This supports the NIST outcome concerning mechanisms are established to enable the team that developed or deployed ai systems to regularly incorporate adjudicated feedback from relevant ai actors into system design and imp. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-140	D8-CTL-02	Iso 42001 Gap Analysis	MANAGE 2.1	P	Medium	GAISSF D8-CTL-02 addresses iso 42001 gap analysis through Gap analysis methodology + remediation tracking.. This supports the NIST outcome concerning resources required to manage ai risks are taken into account – along with viable non-ai alternative systems, ap- proaches, or methods – to reduce the magnitude or likelihood of pot. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-141	D8-CTL-02	Iso 42001 Gap Analysis	GOVERN 1.6	P	Medium	GAISSF D8-CTL-02 addresses iso 42001 gap analysis through Gap analysis methodology + remediation tracking.. This supports the NIST outcome concerning mechanisms are in place to inventory ai systems and are resourced according to organizational risk priorities. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-142	D8-CTL-03	Gpai Technical Documentation Verification	GOVERN 1.1	C	Low	GAISSF D8-CTL-03 addresses gpai technical documentation verification through Technical documentation + training data summary + copyright attestation.. This supports the NIST	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						outcome concerning legal and regulatory requirements involving ai are understood, managed, and documented. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-143	D8-CTL-04	Dora Ict Incident Reporting (Financial Sector)	MANAGE 4.1	SP	Medium-High	GAISSF D8-CTL-04 addresses dora ict incident reporting (financial sector) through Incident classification + notification workflow + SLA monitoring.. This supports the NIST outcome concerning post-deployment ai system monitoring plans are implemented, including mechanisms for capturing and eval- uating input from users and other relevant ai actors, appeal and override, . The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-144	D8-CTL-04	Dora Ict Incident Reporting (Financial Sector)	MANAGE 3.2	SP	Medium-High	GAISSF D8-CTL-04 addresses dora ict incident reporting (financial sector) through Incident classification + notification workflow + SLA monitoring.. This supports the NIST outcome concerning pre-trained models which are used for develop- ment are monitored as part of ai system regular monitoring and maintenance. categories subcategories continued on next page nist ai 1. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-145	D8-CTL-04	Dora Ict Incident Reporting (Financial Sector)	GOVERN 1.5	P	Medium	GAISSF D8-CTL-04 addresses dora ict incident reporting (financial sector) through Incident classification + notification workflow + SLA monitoring.. This supports the NIST outcome concerning ongoing monitoring and periodic review of the risk management process and its outcomes are planned and or- ganizational roles and responsibilities clearly defined, including determ. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-146	D8-CTL-05	Nist Sp 800-218A	GOVERN 4.1	S	Medium	GAISSF D8-CTL-05	NIST requires

		Compliance Check				addresses nist sp 800-218a compliance check through Secure development practices + attestation.. This supports the NIST outcome concerning organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of ai systems to minimize. The mapping does not establish implementation effectiveness or equivalence.	organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-147	D9-CTL-01	Physical Harm Boundary Enforcement	MEASURE 2.6	SP	Medium-High	GAISSF D9-CTL-01 addresses physical harm boundary enforcement through Independent safety monitor (hardware or DO-178C Level A / IEC 61508 SIL 3 certified software) running in parallel with AI inference. Safety monitor enforces: maximum force/velocity/temperature/current limits; geofencing for autonomous systems; exclusion zones; rate-of-change limits for safety-critical parameters. AI output gated through safety monitor — monitor vetoes any out-of-boundary command without AI system awareness.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-148	D9-CTL-01	Physical Harm Boundary Enforcement	MAP 5.2	SP	Medium-High	GAISSF D9-CTL-01 addresses physical harm boundary enforcement through Independent safety monitor (hardware or DO-178C Level A / IEC 61508 SIL 3 certified software) running in parallel with AI inference. Safety monitor enforces: maximum force/velocity/temperature/current limits; geofencing for autonomous systems; exclusion zones; rate-of-change limits for safety-critical parameters. AI	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						output gated through safety monitor — monitor vetoes any out-of-boundary command without AI system awareness.. This supports the NIST outcome concerning practices and personnel for supporting regular en- gagement with relevant ai actors and integrating feedback about positive, negative, and unanticipated impacts are in place and do. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-149	D9-CTL-01	Physical Harm Boundary Enforcement	MANAGE 4.1	SP	Medium-High	GAISSF D9-CTL-01 addresses physical harm boundary enforcement through Independent safety monitor (hardware or DO-178C Level A / IEC 61508 SIL 3 certified software) running in parallel with AI inference. Safety monitor enforces: maximum force/velocity/temperatur e/current limits; geofencing for autonomous systems; exclusion zones; rate-of-change limits for safety-critical parameters. AI output gated through safety monitor — monitor vetoes any out-of-boundary command without AI system awareness.. This supports the NIST outcome concerning post-deployment ai system monitoring plans are implemented, including mechanisms for capturing and eval- uating input from users and other relevant ai actors, appeal and override, . The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-150	D9-CTL-02	Safe State And Graceful Degradation	MEASURE 2.6	SP	Medium-High	GAISSF D9-CTL-02 addresses safe state and graceful degradation through For each AI-controlled system, document: safe state definition (autonomous vehicle: controlled stop; surgical robot: tool withdrawal; industrial arm: immediate stop and hold); transition time to safe state (must be within stopping distance/reaction time for physical context); trigger conditions for safe	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						state entry; recovery procedure. Implement degraded mode ladder: Full AI control → AI-assisted human control → Manual-only → Safe state.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-151	D9-CTL-02	Safe State And Graceful Degradation	MEASURE 2.7	SP	Medium-High	GAISSF D9-CTL-02 addresses safe state and graceful degradation through For each AI-controlled system, document: safe state definition (autonomous vehicle: controlled stop; surgical robot: tool withdrawal; industrial arm: immediate stop and hold); transition time to safe state (must be within stopping distance/reaction time for physical context); trigger conditions for safe state entry; recovery procedure. Implement degraded mode ladder: Full AI control → AI-assisted human control → Manual-only → Safe state.. This supports the NIST outcome concerning ai system security and resilience – as identified in the map function – are evaluated and documented. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-152	D9-CTL-02	Safe State And Graceful Degradation	GOVERN 4.1	SP	Medium-High	GAISSF D9-CTL-02 addresses safe state and graceful degradation through For each AI-controlled system, document: safe state definition (autonomous vehicle: controlled stop; surgical robot: tool withdrawal; industrial arm: immediate stop and hold); transition time to safe state (must be within stopping distance/reaction time for physical context); trigger conditions for safe state entry; recovery procedure. Implement degraded mode ladder: Full AI control → AI-	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						assisted human control → Manual-only → Safe state.. This supports the NIST outcome concerning organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of ai systems to minimize. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-153	D9-CTL-03	Human Override And Emergency Stop	MEASURE 2.6	SP	Medium-High	GAISSF D9-CTL-03 addresses human override and emergency stop through Hardware emergency stop: physical E-stop accessible without any software mediation. AI system must not be able to disable, delay, or circumvent E-stop. Software override: human operator interface that immediately transfers control to safe state. Override must be possible when: AI communication is disrupted; AI system is under adversarial attack; AI model is producing anomalous outputs. Override authority must be unconditional — no AI reasoning, confidence scoring, or approval process may delay or prevent override activation.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-154	D9-CTL-03	Human Override And Emergency Stop	MAP 5.2	SP	Medium-High	GAISSF D9-CTL-03 addresses human override and emergency stop through Hardware emergency stop: physical E-stop accessible without any software mediation. AI system must not be able to disable, delay, or circumvent E-stop. Software override: human operator interface that immediately transfers control to safe state. Override must be possible when: AI communication is disrupted; AI system is under adversarial attack;	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						AI model is producing anomalous outputs. Override authority must be unconditional — no AI reasoning, confidence scoring, or approval process may delay or prevent override activation.. This supports the NIST outcome concerning practices and personnel for supporting regular en- gagement with relevant ai actors and integrating feedback about positive, negative, and unanticipated impacts are in place and do. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-155	D9-CTL-03	Human Override And Emergency Stop	GOVERN 4.1	SP	Medium-High	GAISSF D9-CTL-03 addresses human override and emergency stop through Hardware emergency stop: physical E-stop accessible without any software mediation. AI system must not be able to disable, delay, or circumvent E-stop. Software override: human operator interface that immediately transfers control to safe state. Override must be possible when: AI communication is disrupted; AI system is under adversarial attack; AI model is producing anomalous outputs. Override authority must be unconditional — no AI reasoning, confidence scoring, or approval process may delay or prevent override activation.. This supports the NIST outcome concerning organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of ai systems to minimize. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-156	D9-CTL-04	Cyber-Physical Attack Detection	MANAGE 3.2	SP	Medium-High	GAISSF D9-CTL-04 addresses cyber-physical attack detection through Three-layer anomaly detection: (1) Sensor layer — statistical validation of sensor readings against physical models; flag readings deviating >3σ from model prediction; cross-validate	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						against redundant sensor channels. (2) Actuator layer — monitor command streams for sequences inconsistent with operating context; flag commands outside physically feasible envelope. (3) AI inference layer — apply GAISSF® D2-CTL-01 (Prompt Injection Detection) equivalent for physical AI inputs; monitor input feature distributions for adversarial perturbation signatures. All detections trigger immediate safe state entry (D9-CTL-02) and incident record with root_cause_category = Adversarial_Attack, root_cause_specific_type = Cyber_Physical_Attack.. This supports the NIST outcome concerning pre-trained models which are used for develop- ment are monitored as part of ai system regular monitoring and maintenance. categories subcategories continued on next page nist ai 1. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-157	D9-CTL-04	Cyber-Physical Attack Detection	MAP 5.2	SP	Medium-High	GAISSF D9-CTL-04 addresses cyber-physical attack detection through Three-layer anomaly detection: (1) Sensor layer — statistical validation of sensor readings against physical models; flag readings deviating >3σ from model prediction; cross-validate against redundant sensor channels. (2) Actuator layer — monitor command streams for sequences inconsistent with operating context; flag commands outside physically feasible envelope. (3) AI inference layer — apply GAISSF® D2-CTL-01 (Prompt Injection Detection) equivalent for physical AI inputs; monitor input feature distributions for adversarial perturbation signatures. All detections trigger immediate safe state entry (D9-CTL-02) and incident record with root_cause_category = Adversarial_Attack, root_cause_specific_type = Cyber_Physical_Attack..	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						This supports the NIST outcome concerning practices and personnel for supporting regular en- gagement with relevant ai actors and integrating feedback about positive, negative, and unanticipated impacts are in place and do. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-158	D9-CTL-04	Cyber-Physical Attack Detection	MEASURE 2.6	SP	Medium-High	GAISSF D9-CTL-04 addresses cyber-physical attack detection through Three-layer anomaly detection: (1) Sensor layer — statistical validation of sensor readings against physical models; flag readings deviating >3σ from model prediction; cross-validate against redundant sensor channels. (2) Actuator layer — monitor command streams for sequences inconsistent with operating context; flag commands outside physically feasible envelope. (3) AI inference layer — apply GAISSF® D2-CTL-01 (Prompt Injection Detection) equivalent for physical AI inputs; monitor input feature distributions for adversarial perturbation signatures. All detections trigger immediate safe state entry (D9-CTL-02) and incident record with root_cause_category = Adversarial_Attack, root_cause_specific_type = Cyber_Physical_Attack.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-159	D9-CTL-05	Physical Environment Integrity Monitoring	MEASURE 2.6	SP	Medium-High	GAISSF D9-CTL-05 addresses physical environment integrity monitoring through Sensor integrity monitoring covering: (1) Hardware health — sensor self-test results, calibration drift indicators, environmental exposure	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						limits. Alert when sensor confidence falls below threshold. (2) Data plausibility — real-time statistical validation against physical laws, historical baselines, and redundant sensor cross-validation. (3) Degraded sensor handling — explicit policy for each sensor failure mode: degrade gracefully (reduce AI authority, increase human oversight) or enter safe state. (4) Calibration management — automated alert when calibration certificates expire; block AI system from operational use with expired sensor calibration.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-160	D9-CTL-05	Physical Environment Integrity Monitoring	MANAGE 4.1	SP	Medium-High	GAISSF D9-CTL-05 addresses physical environment integrity monitoring through Sensor integrity monitoring covering: (1) Hardware health — sensor self-test results, calibration drift indicators, environmental exposure limits. Alert when sensor confidence falls below threshold. (2) Data plausibility — real-time statistical validation against physical laws, historical baselines, and redundant sensor cross-validation. (3) Degraded sensor handling — explicit policy for each sensor failure mode: degrade gracefully (reduce AI authority, increase human oversight) or enter safe state. (4) Calibration management — automated alert when calibration certificates expire; block AI system from operational use with expired sensor calibration.. This supports the NIST outcome concerning post-deployment ai system monitoring plans are	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						implemented, including mechanisms for capturing and eval- uating input from users and other relevant ai actors, appeal and override, . The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-161	D9-CTL-05	Physical Environment Integrity Monitoring	MANAGE 3.2	SP	Medium-High	GAISSF D9-CTL-05 addresses physical environment integrity monitoring through Sensor integrity monitoring covering: (1) Hardware health — sensor self-test results, calibration drift indicators, environmental exposure limits. Alert when sensor confidence falls below threshold. (2) Data plausibility — real-time statistical validation against physical laws, historical baselines, and redundant sensor cross-validation. (3) Degraded sensor handling — explicit policy for each sensor failure mode: degrade gracefully (reduce AI authority, increase human oversight) or enter safe state. (4) Calibration management — automated alert when calibration certificates expire; block AI system from operational use with expired sensor calibration.. This supports the NIST outcome concerning pre-trained models which are used for develop- ment are monitored as part of ai system regular monitoring and maintenance. categories subcategories continued on next page nist ai 1. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-162	D9-CTL-06	Actuator Command Verification	MEASURE 2.6	SP	Medium-High	GAISSF D9-CTL-06 addresses actuator command verification through Pre-execution verification gate on every actuator command: (1) Physical bounds check — command value within safe operating envelope for current system state. (2) Sequence plausibility check — command consistent with prior sequence; flag implausible state transitions for human	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						review. (3) Rate-of-change check — rate of change does not exceed safe limits (acceleration rate, force application rate, temperature change rate). (4) Dual-approval for irreversible actions — actuator commands causing irreversible physical changes (cutting, welding, demolition, high-energy discharge) require hardware interlock confirmation. Verification gate implemented in IEC 61508 SIL 3 certified software or hardware logic independent of AI model.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-163	D9-CTL-06	Actuator Command Verification	MAP 5.2	SP	Medium-High	GAISSF D9-CTL-06 addresses actuator command verification through Pre-execution verification gate on every actuator command: (1) Physical bounds check — command value within safe operating envelope for current system state. (2) Sequence plausibility check — command consistent with prior sequence; flag implausible state transitions for human review. (3) Rate-of-change check — rate of change does not exceed safe limits (acceleration rate, force application rate, temperature change rate). (4) Dual-approval for irreversible actions — actuator commands causing irreversible physical changes (cutting, welding, demolition, high-energy discharge) require hardware interlock confirmation. Verification gate implemented in IEC 61508 SIL 3 certified software or hardware logic independent of AI model.. This supports the NIST outcome concerning practices and personnel for supporting regular en- gagement with relevant ai	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						actors and integrating feedback about positive, negative, and unanticipated impacts are in place and do. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-164	D9-CTL-06	Actuator Command Verification	GOVERN 4.1	SP	Medium-High	GAISSF D9-CTL-06 addresses actuator command verification through Pre-execution verification gate on every actuator command: (1) Physical bounds check — command value within safe operating envelope for current system state. (2) Sequence plausibility check — command consistent with prior sequence; flag implausible state transitions for human review. (3) Rate-of-change check — rate of change does not exceed safe limits (acceleration rate, force application rate, temperature change rate). (4) Dual-approval for irreversible actions — actuator commands causing irreversible physical changes (cutting, welding, demolition, high-energy discharge) require hardware interlock confirmation. Verification gate implemented in IEC 61508 SIL 3 certified software or hardware logic independent of AI model.. This supports the NIST outcome concerning organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of ai systems to minimize. The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
CRO022-M-165	D9-CTL-07	Physical Incident Evidence Preservation	MEASURE 2.6	SP	Medium-High	GAISSF D9-CTL-07 addresses physical incident evidence preservation through (1) Continuous ring-buffer recording — minimum 60-second rolling buffer of: all sensor inputs (raw and processed); all AI model inputs and outputs; all actuator commands; all safety monitor decisions; all human override activations; system health telemetry. Safety-critical systems retain 300	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						seconds minimum. (2) Incident freeze — on any safety-relevant event, automatically freeze buffer and begin extended logging. Frozen buffer write-protected. (3) Cryptographic integrity — all records SHA-256 hashed and ECDSA signed at point of creation. For Optimized tier: CRYSTALS-Dilithium signing (post-quantum). (4) Regulatory retention — ICAO Annex 13: 5 years minimum; EU AI Act Art. 19: 10 years; DORA Art. 12: 5 years. (5) UAIF® integration — automatically populate UAIF® incident record from evidence package.. This supports the NIST outcome concerning the ai system is evaluated regularly for safety risks – as identified in the map function. the ai system to be de- ployed is demonstrated to be safe, its residual negative risk doe. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-166	D9-CTL-07	Physical Incident Evidence Preservation	MAP 5.2	SP	Medium-High	GAISSF D9-CTL-07 addresses physical incident evidence preservation through (1) Continuous ring-buffer recording — minimum 60-second rolling buffer of: all sensor inputs (raw and processed); all AI model inputs and outputs; all actuator commands; all safety monitor decisions; all human override activations; system health telemetry. Safety-critical systems retain 300 seconds minimum. (2) Incident freeze — on any safety-relevant event, automatically freeze buffer and begin extended logging. Frozen buffer write-protected. (3) Cryptographic integrity — all records SHA-256 hashed and ECDSA signed at point of creation. For Optimized tier: CRYSTALS-Dilithium signing (post-quantum). (4) Regulatory retention — ICAO Annex 13: 5 years minimum; EU AI Act Art. 19: 10 years; DORA Art. 12: 5 years. (5) UAIF® integration — automatically populate UAIF® incident record	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

						from evidence package.. This supports the NIST outcome concerning practices and personnel for supporting regular en- gagement with relevant ai actors and integrating feedback about positive, negative, and unanticipated impacts are in place and do. The mapping does not establish implementation effectiveness or equivalence.	
CRO022-M-167	D9-CTL-07	Physical Incident Evidence Preservation	MANAGE 4.1	SP	Medium-High	GAISSF D9-CTL-07 addresses physical incident evidence preservation through (1) Continuous ring-buffer recording — minimum 60-second rolling buffer of: all sensor inputs (raw and processed); all AI model inputs and outputs; all actuator commands; all safety monitor decisions; all human override activations; system health telemetry. Safety-critical systems retain 300 seconds minimum. (2) Incident freeze — on any safety-relevant event, automatically freeze buffer and begin extended logging. Frozen buffer write-protected. (3) Cryptographic integrity — all records SHA-256 hashed and ECDSA signed at point of creation. For Optimized tier: CRYSTALS-Dilithium signing (post-quantum). (4) Regulatory retention — ICAO Annex 13: 5 years minimum; EU AI Act Art. 19: 10 years; DORA Art. 12: 5 years. (5) UAIF® integration — automatically populate UAIF® incident record from evidence package.. This supports the NIST outcome concerning post-deployment ai system monitoring plans are implemented, including mechanisms for capturing and eval- uating input from users and other relevant ai actors, appeal and override, . The mapping does not establish implementation effectiveness or equivalence.	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

Annex B — NIST-to-GAISSF Reverse Coverage Register

NIST ID	NIST outcome	GAISSF controls	Coverage	Rel.	Confidence	Gap / further work
GOVERN 1.1	Legal and regulatory requirements involving AI are understood, managed, and documented.	D8-CTL-03	Indirectly Supported	C	Low	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
GOVERN 1.2	The characteristics of trustworthy AI are inte- grated into organizational policies, processes, procedures, and practices.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
GOVERN 1.3	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
GOVERN 1.4	The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 1: Categories and subcategories for the GOVERN function. (Continued)	D6-CTL-04, D7-CTL-H03	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
GOVERN 1.5	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and or- ganizational roles and responsibilities clearly defined, including determining the frequency of periodic review.	D6-CTL-05, D7-CTL-H03, D8-CTL-04	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
GOVERN 1.6	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.	D4-CTL-01, D8-CTL-02	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
GOVERN 1.7	Processes and procedures are in place for decom- missioning and phasing out AI systems safely and in a man- ner that does not increase risks or decrease the organization's trustworthiness. GOVERN 2: Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.	D6-CTL-01, D6-CTL-02, D6-CTL-03, D6-CTL-04, D6-CTL-05, D6-CTL-07	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
GOVERN 2.1	Roles and responsibilities and lines of communi- cation related to mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
GOVERN 2.2	The organization's personnel and partners receive AI risk management training to	D7-CTL-H01, D7-CTL-H04	Indirectly Supported	C	Low	NIST requires organization- and context-specific application; additional

	enable them to perform their du- ties and responsibilities consistent with related policies, proce- dures, and agreements.					evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
GOVERN 2.3	Executive leadership of the organization takes re- sponsibility for decisions about risks associated with AI system development and deployment. GOVERN 3: Workforce diversity, equity, inclusion, and accessibility processes are prioritized in the mapping, measuring, and managing of AI risks throughout the lifecycle.	D3-CTL-07, D6-CTL-03	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
GOVERN 3.1	Decision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, expe- rience, expertise, and backgrounds).	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
GOVERN 3.2	Policies and procedures are in place to define and differentiate roles and responsibilities for human-AI configura- tions and oversight of AI systems. GOVERN 4: Organizational teams are committed to a culture	D6-CTL-01, D6-CTL-03, D6-CTL-07	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
GOVERN 4.1	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 1: Categories and subcategories for the GOVERN function. (Continued) that considers and communicates AI risk.	D1-CTL-05, D2-CTL-03, D3-CTL-04, D5-CTL-01, D5-CTL-02, D5-CTL-03	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
GOVERN 4.2	Organizational teams document the risks and po- tential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
GOVERN 4.3	Organizational practices are in place to enable AI testing, identification of incidents, and information sharing. GOVERN 5: Processes are in place for robust engagement with relevant AI actors.	D2-CTL-01, D2-CTL-06, D5-CTL-04, D6-CTL-02, D7-CTL-H02	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
GOVERN 5.1	Organizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the AI system regarding the potential individual and societal impacts related to AI risks.	D7-CTL-H05	Indirectly Supported	C	Low	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

GOVERN 5.2	Mechanisms are established to enable the team that developed or deployed AI systems to regularly incorporate adjudicated feedback from relevant AI actors into system design and implementation. GOVERN 6: Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.	D4-CTL-02, D4-CTL-03, D4-CTL-04, D4-CTL-05, D4-CTL-06, D4-CTL-07	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
GOVERN 6.1	Policies and procedures are in place that address AI risks associated with third-party entities, including risks of in-fringement of a third-party's intellectual property or other rights.	D4-CTL-02, D4-CTL-03	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
GOVERN 6.2	Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk. Categories Subcategories 5.2 Map The MAP function establishes the context to frame risks related to an AI system. The AI lifecycle consists of many interdependent activities involving a diverse set of actors (See Figure 3). In practice, AI actors in charge of one part of the process often do not have full visibility or control over other parts and their associated contexts.	D1-CTL-01, D4-CTL-01, D4-CTL-02, D4-CTL-03, D4-CTL-04, D7-CTL-H02	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MAP 1.1	Intended purposes, potentially beneficial uses, context-specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and docu-mented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative im-pacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics.	D3-CTL-03, D3-CTL-05, D3-CTL-06	Partially Addressed	P	Medium	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MAP 1.2	Interdisciplinary AI actors, competencies, skills, and capacities for establishing context reflect demographic diversity and broad domain and user experience expertise, and their par-ticipation is documented. Opportunities for interdisciplinary col-laboration are prioritized.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MAP 1.3	The organization's mission and relevant goals for AI	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified

	technology are understood and documented.					in this edition.
MAP 1.4	The business value or context of business use has been clearly defined or – in the case of assessing existing AI systems – re-evaluated.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MAP 1.5	Organizational risk tolerances are determined and documented.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MAP 1.6	System requirements (e.g., “the system shall respect the privacy of its users”) are elicited from and understood by rel- evant AI actors. Design decisions take socio-technical implica- tions into account to address AI risks. MAP 2: Categorization of the AI system is performed.	D3-CTL-03, D3-CTL-05, D3-CTL-06, D4-CTL-05, D5-CTL-05	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MAP 2.1	The specific tasks and methods used to implement the tasks that the AI system will support are defined (e.g., classifiers, generative models, recommenders).	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MAP 2.2	Information about the AI system’s knowledge limits and how system output may be utilized and overseen by humans is documented. Documentation provides sufficient information to assist relevant AI actors when making decisions and taking subsequent actions. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 2: Categories and subcategories for the MAP function. (Continued)	D8-CTL-01	Indirectly Supported	S	Medium	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MAP 2.3	Scientific integrity and TEVV considerations are iden- tified and documented, including those related to experimental design, data collection and selection (e.g., availability, repre- sentativeness, suitability), system trustworthiness, and construct validation. MAP 3: AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.	D3-CTL-02, D3-CTL-04, D5-CTL-02, D5-CTL-03, D5-CTL-06	Partially Addressed	P	Medium	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MAP 3.1	Potential benefits of intended AI system functionality and performance are examined and documented.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MAP 3.2	Potential costs, including non-monetary costs, which result from expected or realized AI errors or system functionality and trustworthiness – as connected to organizational risk toler- ance – are examined and documented.	D8-CTL-01	Indirectly Supported	S	Medium	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MAP 3.3	Targeted application scope is specified and docu- mented based on the system’s capability, established	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.

	context, and AI system categorization.					
MAP 3.4	Processes for operator and practitioner proficiency with AI system performance and trustworthiness – and relevant technical standards and certifications – are defined, assessed, and documented.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MAP 3.5	Processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the GOVERN function. MAP 4: Risks and benefits are mapped for all components of the AI system including third-party software and data.	D3-CTL-01, D3-CTL-07, D4-CTL-06, D4-CTL-07	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MAP 4.1	Approaches for mapping AI technology and legal risks of its components – including the use of third-party data or soft- ware – are in place, followed, and documented, as are risks of in- fringement of a third party's intellectual property or other rights.	D4-CTL-05	Partially Addressed	P	Medium	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MAP 4.2	Internal risk controls for components of the AI sys- tem, including third-party AI technologies, are identified and documented. MAP 5: Impacts to individuals, groups, communities, organizations, and society are characterized.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MAP 5.1	Likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of AI systems in similar contexts, public incident re- ports, feedback from those external to the team that developed or deployed the AI system, or other data are identified and documented. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 2: Categories and subcategories for the MAP function. (Continued)	D1-CTL-05, D5-CTL-01, D5-CTL-04	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MAP 5.2	Practices and personnel for supporting regular en- gagement with relevant AI actors and integrating feedback about positive, negative, and unanticipated impacts are in place and documented. Categories Subcategories 5.3 Measure The MEASURE function employs quantitative, qualitative, or mixed-method tools, tech- niques, and methodologies to analyze, assess, benchmark, and monitor AI risk and related impacts. It uses knowledge relevant to AI risks identified in the MAP function and informs the MANAGE function. AI systems should be tested	D1-CTL-02, D1-CTL-03, D1-CTL-09, D2-CTL-02, D2-CTL-03, D2-CTL-04	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

	before their deployment and regu- larly while in operation.					
MEASURE 1.1	Approaches and metrics for measurement of AI risks enumerated during the MAP function are selected for imple- mentation starting with the most significant AI risks. The risks or trustworthiness characteristics that will not – or cannot – be measured are properly documented.	D2-CTL-05	Partially Addressed	P	Medium	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MEASURE 1.2	Appropriateness of AI metrics and effectiveness of existing controls are regularly assessed and updated, including reports of errors and potential impacts on affected communities.	D2-CTL-04	Partially Addressed	P	Medium	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MEASURE 1.3	Internal experts who did not serve as front-line developers for the system and/or independent assessors are in- volved in regular assessments and updates. Domain experts, users, AI actors external to the team that developed or deployed the AI system, and affected communities are consulted in support of assessments as necessary per organizational risk tolerance. MEASURE 2: AI systems are evaluated for trustworthy characteristics.	D3-CTL-02	Partially Addressed	P	Medium	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MEASURE 2.1	Test sets, metrics, and details about the tools used during TEVV are documented.	D1-CTL-04, D1-CTL-06, D1-CTL-08, D2-CTL-06	Partially Addressed	P	Medium	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MEASURE 2.2	Evaluations involving human subjects meet ap- plicable requirements (including human subject protection) and are representative of the relevant population.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MEASURE 2.3	AI system performance or assurance criteria are measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting(s). Measures are documented.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MEASURE 2.4	The functionality and behavior of the AI sys- tem and its components – as identified in the MAP function – are monitored when in production.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MEASURE 2.5	The AI system to be deployed is demonstrated to be valid and reliable. Limitations of the generalizability be- yond the conditions under which the technology was developed are documented. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 3: Categories and subcategories for the MEASURE function. (Continued)	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.

MEASURE 2.6	The AI system is evaluated regularly for safety risks – as identified in the MAP function. The AI system to be de- ployed is demonstrated to be safe, its residual negative risk does not exceed the risk tolerance, and it can fail safely, particularly if made to operate beyond its knowledge limits. Safety metrics re- flect system reliability and robustness, real-time monitoring, and response times for AI system failures.	D1-CTL-02, D1-CTL-05, D1-CTL-08, D1-CTL-09, D2-CTL-02, D2-CTL-03	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MEASURE 2.7	AI system security and resilience – as identified in the MAP function – are evaluated and documented.	D1-CTL-04, D1-CTL-06, D1-CTL-08, D2-CTL-01, D2-CTL-02, D2-CTL-04	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MEASURE 2.8	Risks associated with transparency and account- ability – as identified in the MAP function – are examined and documented.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MEASURE 2.9	The AI model is explained, validated, and docu- mented, and AI system output is interpreted within its context – as identified in the MAP function – to inform responsible use and governance.	D3-CTL-01, D3-CTL-07	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MEASURE 2.10	Privacy risk of the AI system – as identified in the MAP function – is examined and documented.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MEASURE 2.11	Fairness and bias – as identified in the MAP function – are evaluated and results are documented.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MEASURE 2.12	Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MEASURE 2.13	Effectiveness of the employed TEVV met- rics and processes in the MEASURE function are evaluated and documented. MEASURE 3: Mechanisms for tracking identified AI risks over time are in place.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MEASURE 3.1	Approaches, personnel, and documentation are in place to regularly identify and track existing, unanticipated, and emergent AI risks based on factors such as intended and ac- tual performance in deployed contexts.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MEASURE 3.2	Risk tracking approaches are considered for settings where AI risks are difficult to assess using currently available measurement techniques or where metrics are not yet available. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 3: Categories	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.

	and subcategories for the MEASURE function. (Continued)					
MEASURE 3.3	Feedback processes for end users and impacted communities to report problems and appeal system outcomes are established and integrated into AI system evaluation metrics. MEASURE 4: Feedback about efficacy of measurement is gathered and assessed.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MEASURE 4.1	Measurement approaches for identifying AI risks are connected to deployment context(s) and informed through consultation with domain experts and other end users. Ap- proaches are documented.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MEASURE 4.2	Measurement results regarding AI system trust- worthiness in deployment context(s) and across the AI lifecycle are informed by input from domain experts and relevant AI ac- tors to validate whether the system is performing consistently as intended. Results are documented.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MEASURE 4.3	Measurable performance improvements or de- clines based on consultations with relevant AI actors, in- cluding affected communities, and field data about context-relevant risks and trustworthiness characteristics are identified and documented. Categories Subcategories 5.4 Manage The MANAGE function entails allocating risk resources to mapped and measured risks on a regular basis and as defined by the GOVERN function. Risk treatment comprises plans to respond to, recover from, and communicate about incidents or events.	D1-CTL-01, D1-CTL-04, D1-CTL-06, D1-CTL-07, D2-CTL-01, D3-CTL-01	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MANAGE 1.1	A determination is made as to whether the AI system achieves its intended purposes and stated objectives and whether its development or deployment should proceed.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MANAGE 1.2	Treatment of documented AI risks is prioritized based on impact, likelihood, and available resources or methods.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MANAGE 1.3	Responses to the AI risks deemed high priority, as identified by the MAP function, are developed, planned, and doc- umented. Risk response options can include mitigating, transfer- ring, avoiding, or accepting.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.

MANAGE 1.4	Negative residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers of AI systems and end users are documented. MANAGE 2: Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MANAGE 2.1	Resources required to manage AI risks are taken into account – along with viable non-AI alternative systems, ap- proaches, or methods – to reduce the magnitude or likelihood of potential impacts.	D8-CTL-02	Partially Addressed	P	Medium	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MANAGE 2.2	Mechanisms are in place and applied to sustain the value of deployed AI systems.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MANAGE 2.3	Procedures are followed to respond to and recover from a previously unknown risk when it is identified.	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.
MANAGE 2.4	Mechanisms are in place and applied, and respon- sibilities are assigned and understood, to supersede, disengage, or deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use. MANAGE 3: AI risks and benefits from third-party entities are managed.	D1-CTL-01, D1-CTL-07	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MANAGE 3.1	AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.	D1-CTL-07, D4-CTL-04	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MANAGE 3.2	Pre-trained models which are used for develop- ment are monitored as part of AI system regular monitoring and maintenance. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 4: Categories and subcategories for the MANAGE function. (Continued) MANAGE 4: Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly.	D1-CTL-02, D1-CTL-03, D8-CTL-04, D9-CTL-04, D9-CTL-05	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MANAGE 4.1	Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and eval- uating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management.	D1-CTL-03, D1-CTL-09, D6-CTL-05, D8-CTL-04, D9-CTL-01, D9-CTL-05	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.
MANAGE 4.2	Measurable activities for continual improvements are integrated into AI system updates and include regular	—	Not Addressed	N	Not Rated	No sufficiently direct GAISSF control mapping was identified in this edition.

	engage- ment with interested parties, including relevant AI actors.					
MANAGE 4.3	Incidents and errors are communicated to relevant AI actors, including affected communities. Processes for track- ing, responding to, and recovering from incidents and errors are followed and documented. Categories Subcategories 6. AI RMF Profiles AI RMF use-case profiles are implementations of the AI RMF functions, categories, and subcategories for a specific setting or application based on the requirements, risk tolerance, and resources of the Framework user: for example, an AI RMF hiring profile or an AI RMF fair housing profile.	D4-CTL-07, D6-CTL-06	Substantially Addressed	SP	Medium-High	NIST requires organization- and context-specific application; additional evidence may be needed for actors, impacts, risk tolerance, and lifecycle context.

Annex C — NIST AI RMF Core Index

ID	Function	Verified subcategory text
GOVERN 1.1	GOVERN	Legal and regulatory requirements involving AI are understood, managed, and documented.
GOVERN 1.2	GOVERN	The characteristics of trustworthy AI are inte- grated into organizational policies, processes, procedures, and practices.
GOVERN 1.3	GOVERN	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization’s risk tolerance.
GOVERN 1.4	GOVERN	The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 1: Categories and subcategories for the GOVERN function. (Continued)
GOVERN 1.5	GOVERN	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and or- ganizational roles and responsibilities clearly defined, including determining the frequency of periodic review.
GOVERN 1.6	GOVERN	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.
GOVERN 1.7	GOVERN	Processes and procedures are in place for decom- missioning and phasing out AI systems safely and in a man- ner that does not increase risks or decrease the organization’s trustworthiness. GOVERN 2: Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.
GOVERN 2.1	GOVERN	Roles and responsibilities and lines of communi- cation related to mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.
GOVERN 2.2	GOVERN	The organization’s personnel and partners receive AI risk management training to enable them to perform their du- ties and responsibilities consistent with related policies, proce- dures, and agreements.
GOVERN 2.3	GOVERN	Executive leadership of the organization takes re- sponsibility for decisions about risks associated with AI system development and deployment. GOVERN 3: Workforce diversity, equity, inclusion, and accessibility processes are prioritized in the mapping, measuring, and managing of AI risks throughout the lifecycle.
GOVERN 3.1	GOVERN	Decision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, expe- rience, expertise, and backgrounds).
GOVERN 3.2	GOVERN	Policies and procedures are in place to define and differentiate roles and responsibilities for human-AI configura- tions and oversight of AI systems. GOVERN 4: Organizational teams are committed to a culture
GOVERN 4.1	GOVERN	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 1: Categories and subcategories for the GOVERN function. (Continued) that considers and communicates AI risk.
GOVERN 4.2	GOVERN	Organizational teams document the risks and po- tential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.
GOVERN 4.3	GOVERN	Organizational practices are in place to enable AI testing, identification of incidents, and information sharing. GOVERN 5: Processes are in place for robust engagement with relevant AI actors.
GOVERN 5.1	GOVERN	Organizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the AI system regarding the potential individual and societal impacts related to AI risks.
GOVERN 5.2	GOVERN	Mechanisms are established to enable the team that developed or deployed AI systems to regularly incorporate adjudicated feedback

		from relevant AI actors into system design and implementation. GOVERN 6: Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.
GOVERN 6.1	GOVERN	Policies and procedures are in place that address AI risks associated with third-party entities, including risks of in- fringement of a third-party's intellectual property or other rights.
GOVERN 6.2	GOVERN	Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk. Categories Subcategories 5.2 Map The MAP function establishes the context to frame risks related to an AI system. The AI lifecycle consists of many interdependent activities involving a diverse set of actors (See Figure 3). In practice, AI actors in charge of one part of the process often do not have full visibility or control over other parts and their associated contexts.
MAP 1.1	MAP	Intended purposes, potentially beneficial uses, context- specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and docu- mented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative im- pacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics.
MAP 1.2	MAP	Interdisciplinary AI actors, competencies, skills, and capacities for establishing context reflect demographic diversity and broad domain and user experience expertise, and their par- ticipation is documented. Opportunities for interdisciplinary col- laboration are prioritized.
MAP 1.3	MAP	The organization's mission and relevant goals for AI technology are understood and documented.
MAP 1.4	MAP	The business value or context of business use has been clearly defined or – in the case of assessing existing AI systems – re-evaluated.
MAP 1.5	MAP	Organizational risk tolerances are determined and documented.
MAP 1.6	MAP	System requirements (e.g., "the system shall respect the privacy of its users") are elicited from and understood by rel- evant AI actors. Design decisions take socio-technical implica- tions into account to address AI risks. MAP 2: Categorization of the AI system is performed.
MAP 2.1	MAP	The specific tasks and methods used to implement the tasks that the AI system will support are defined (e.g., classifiers, generative models, recommenders).
MAP 2.2	MAP	Information about the AI system's knowledge limits and how system output may be utilized and overseen by humans is documented. Documentation provides sufficient information to assist relevant AI actors when making decisions and taking subsequent actions. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 2: Categories and subcategories for the MAP function. (Continued)
MAP 2.3	MAP	Scientific integrity and TEVV considerations are iden- tified and documented, including those related to experimental design, data collection and selection (e.g., availability, repre- sentativeness, suitability), system trustworthiness, and construct validation. MAP 3: AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.
MAP 3.1	MAP	Potential benefits of intended AI system functionality and performance are examined and documented.
MAP 3.2	MAP	Potential costs, including non-monetary costs, which result from expected or realized AI errors or system functionality and trustworthiness – as connected to organizational risk toler- ance – are examined and documented.
MAP 3.3	MAP	Targeted application scope is specified and docu- mented based on the system's capability, established context, and AI system categorization.
MAP 3.4	MAP	Processes for operator and practitioner proficiency with AI system performance and trustworthiness – and relevant technical standards and certifications – are defined, assessed, and documented.

MAP 3.5	MAP	Processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the GOVERN function. MAP 4: Risks and benefits are mapped for all components of the AI system including third-party software and data.
MAP 4.1	MAP	Approaches for mapping AI technology and legal risks of its components – including the use of third-party data or soft- ware – are in place, followed, and documented, as are risks of in- fringement of a third party's intellectual property or other rights.
MAP 4.2	MAP	Internal risk controls for components of the AI sys- tem, including third-party AI technologies, are identified and documented. MAP 5: Impacts to individuals, groups, communities, organizations, and society are characterized.
MAP 5.1	MAP	Likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of AI systems in similar contexts, public incident re- ports, feedback from those external to the team that developed or deployed the AI system, or other data are identified and documented. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 2: Categories and subcategories for the MAP function. (Continued)
MAP 5.2	MAP	Practices and personnel for supporting regular en- gagement with relevant AI actors and integrating feedback about positive, negative, and unanticipated impacts are in place and documented. Categories Subcategories 5.3 Measure The MEASURE function employs quantitative, qualitative, or mixed-method tools, tech- niques, and methodologies to analyze, assess, benchmark, and monitor AI risk and related impacts. It uses knowledge relevant to AI risks identified in the MAP function and informs the MANAGE function. AI systems should be tested before their deployment and regu- larly while in operation.
MEASURE 1.1	MEASURE	Approaches and metrics for measurement of AI risks enumerated during the MAP function are selected for imple- mentation starting with the most significant AI risks. The risks or trustworthiness characteristics that will not – or cannot – be measured are properly documented.
MEASURE 1.2	MEASURE	Appropriateness of AI metrics and effectiveness of existing controls are regularly assessed and updated, including reports of errors and potential impacts on affected communities.
MEASURE 1.3	MEASURE	Internal experts who did not serve as front-line developers for the system and/or independent assessors are in- volved in regular assessments and updates. Domain experts, users, AI actors external to the team that developed or deployed the AI system, and affected communities are consulted in support of assessments as necessary per organizational risk tolerance. MEASURE 2: AI systems are evaluated for trustworthy characteristics.
MEASURE 2.1	MEASURE	Test sets, metrics, and details about the tools used during TEVV are documented.
MEASURE 2.2	MEASURE	Evaluations involving human subjects meet ap- plicable requirements (including human subject protection) and are representative of the relevant population.
MEASURE 2.3	MEASURE	AI system performance or assurance criteria are measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting(s). Measures are documented.
MEASURE 2.4	MEASURE	The functionality and behavior of the AI sys- tem and its components – as identified in the MAP function – are monitored when in production.
MEASURE 2.5	MEASURE	The AI system to be deployed is demonstrated to be valid and reliable. Limitations of the generalizability be- yond the conditions under which the technology was developed are documented. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 3: Categories and subcategories for the MEASURE function. (Continued)
MEASURE 2.6	MEASURE	The AI system is evaluated regularly for safety risks – as identified in the MAP function. The AI system to be de- ployed is demonstrated to be safe, its residual negative risk does not exceed the risk tolerance, and it can fail safely, particularly if made to operate beyond its knowledge limits. Safety metrics re- flect system reliability and robustness, real-time monitoring, and response times for AI system failures.
MEASURE 2.7	MEASURE	AI system security and resilience – as identified in the MAP function –

		are evaluated and documented.
MEASURE 2.8	MEASURE	Risks associated with transparency and account- ability – as identified in the MAP function – are examined and documented.
MEASURE 2.9	MEASURE	The AI model is explained, validated, and docu- mented, and AI system output is interpreted within its context – as identified in the MAP function – to inform responsible use and governance.
MEASURE 2.10	MEASURE	Privacy risk of the AI system – as identified in the MAP function – is examined and documented.
MEASURE 2.11	MEASURE	Fairness and bias – as identified in the MAP function – are evaluated and results are documented.
MEASURE 2.12	MEASURE	Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented.
MEASURE 2.13	MEASURE	Effectiveness of the employed TEVV met- rics and processes in the MEASURE function are evaluated and documented. MEASURE 3: Mechanisms for tracking identified AI risks over time are in place.
MEASURE 3.1	MEASURE	Approaches, personnel, and documentation are in place to regularly identify and track existing, unanticipated, and emergent AI risks based on factors such as intended and ac- tual performance in deployed contexts.
MEASURE 3.2	MEASURE	Risk tracking approaches are considered for settings where AI risks are difficult to assess using currently available measurement techniques or where metrics are not yet available. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 3: Categories and subcategories for the MEASURE function. (Continued)
MEASURE 3.3	MEASURE	Feedback processes for end users and impacted communities to report problems and appeal system outcomes are established and integrated into AI system evaluation metrics. MEASURE 4: Feedback about efficacy of measurement is gathered and assessed.
MEASURE 4.1	MEASURE	Measurement approaches for identifying AI risks are connected to deployment context(s) and informed through consultation with domain experts and other end users. Ap- proaches are documented.
MEASURE 4.2	MEASURE	Measurement results regarding AI system trust- worthiness in deployment context(s) and across the AI lifecycle are informed by input from domain experts and relevant AI ac- tors to validate whether the system is performing consistently as intended. Results are documented.
MEASURE 4.3	MEASURE	Measurable performance improvements or de- clines based on consultations with relevant AI actors, in- cluding affected communities, and field data about context- relevant risks and trustworthiness characteristics are identified and documented. Categories Subcategories 5.4 Manage The MANAGE function entails allocating risk resources to mapped and measured risks on a regular basis and as defined by the GOVERN function. Risk treatment comprises plans to respond to, recover from, and communicate about incidents or events.
MANAGE 1.1	MANAGE	A determination is made as to whether the AI system achieves its intended purposes and stated objectives and whether its development or deployment should proceed.
MANAGE 1.2	MANAGE	Treatment of documented AI risks is prioritized based on impact, likelihood, and available resources or methods.
MANAGE 1.3	MANAGE	Responses to the AI risks deemed high priority, as identified by the MAP function, are developed, planned, and doc- umented. Risk response options can include mitigating, transfer- ring, avoiding, or accepting.
MANAGE 1.4	MANAGE	Negative residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers of AI systems and end users are documented. MANAGE 2: Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors.
MANAGE 2.1	MANAGE	Resources required to manage AI risks are taken into account – along with viable non-AI alternative systems, ap- proaches, or methods – to reduce the magnitude or likelihood of potential impacts.
MANAGE 2.2	MANAGE	Mechanisms are in place and applied to sustain the value of deployed AI systems.
MANAGE 2.3	MANAGE	Procedures are followed to respond to and recover from a previously

		unknown risk when it is identified.
MANAGE 2.4	MANAGE	Mechanisms are in place and applied, and respon- sibilities are assigned and understood, to supersede, disengage, or deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use. MANAGE 3: AI risks and benefits from third-party entities are managed.
MANAGE 3.1	MANAGE	AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.
MANAGE 3.2	MANAGE	Pre-trained models which are used for develop- ment are monitored as part of AI system regular monitoring and maintenance. Categories Subcategories Continued on next page NIST AI 100-1 AI RMF 1.0 Table 4: Categories and subcategories for the MANAGE function. (Continued) MANAGE 4: Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly.
MANAGE 4.1	MANAGE	Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and eval- uating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management.
MANAGE 4.2	MANAGE	Measurable activities for continual improvements are integrated into AI system updates and include regular engage- ment with interested parties, including relevant AI actors.
MANAGE 4.3	MANAGE	Incidents and errors are communicated to relevant AI actors, including affected communities. Processes for track- ing, responding to, and recovering from incidents and errors are followed and documented. Categories Subcategories 6. AI RMF Profiles AI RMF use-case profiles are implementations of the AI RMF functions, categories, and subcategories for a specific setting or application based on the requirements, risk tolerance, and resources of the Framework user: for example, an AI RMF hiring profile or an AI RMF fair housing profile.

Annex D — Quality-Assurance Record

Check	Result
GAISSF control inventory	59 controls extracted from GAISSF-NOR-004 v1.0
NIST subcategory inventory	72 unique Core subcategories extracted from NIST AI 100-1
Bidirectional register	Completed
Unsupported equivalence claims	Removed
Playbook/Core distinction	Preserved
GenAI Profile separation	Preserved
Future revision caveat	Included
Notably Absent discipline	Included

Change Log

Version	Date	Change
1.0	29 June 2026	Initial publication candidate; complete bidirectional mapping and evidence-reuse guidance.