ODA3 INSTITUTE

Crosswalk — Controlled Publication

GAISSF–NIST CSF 2.0 Mapping

Cybersecurity Alignment Crosswalk — NIST CSWP 29

DocID: CRO-023
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.

Document ID	CRO-023
Version	1.0
Status	Publication Candidate
Classification	Crosswalk
Publication date	29 June 2026
Publisher	ODA3 Institute

Document Control and Authority

This publication candidate maps the authoritative GAISSF v1.0 59-control baseline to the NIST Cybersecurity Framework 2.0 Core. GAISSF-NOR-001 governs framework architecture and conformance; GAISSF-NOR-004 is the authoritative control catalogue. NIST CSWP 29 Appendix A is the primary external mapping source.

1. Executive Summary

The analysis assessed all 59 GAISSF controls against all 106 NIST CSF 2.0 Core subcategories and produced 182 forward mapping records plus a complete reverse coverage register. The crosswalk is designed for control rationalization, AI-security integration, evidence reuse, profile development, and gap analysis.

The strongest alignment appears in cybersecurity governance, third-party and supply-chain risk, vulnerability and threat assessment, access control, platform and data security, continuous monitoring, incident analysis and mitigation, and resilience. The principal structural limitation is scope: NIST CSF 2.0 addresses cybersecurity risk across the whole organization and all ICT, whereas GAISSF is an AI-security and safety framework focused on AI systems, their supporting infrastructure, suppliers, data, models, agents, and physical-AI components.

2. Purpose and Intended Use

- Develop an AI-focused overlay for a CSF Current or Target Profile.
- Identify GAISSF evidence that may support selected CSF outcomes.
- Locate organization-wide or non-AI cybersecurity gaps that GAISSF does not address.
- Support internal assurance and control rationalization without asserting equivalence.

3. Source Baseline

Source	Identifier	Status	Role
GAISSF Framework Standard	GAISSF-NOR-001 v1.0	Normative, corrected final publication edition	Framework and conformance baseline
GAISSF Control Catalogue	GAISSF-NOR-004 v1.0	Normative, full final	Authoritative 59-control catalogue
NIST Cybersecurity Framework 2.0	NIST CSWP 29, 26 Feb 2024	Voluntary cybersecurity framework	Primary Core mapping target
CSF Implementation Examples	Online, dynamically maintained	Informative and non-exhaustive	Supplementary interpretation only

4. Methodology

Mappings were assigned at GAISSF-control-to-CSF-subcategory level using shared outcome, scope, lifecycle, actor, evidence, and implementation-effect criteria. Similar terminology alone was insufficient. One-to-many and many-to-one relationships were retained. Each mapping has a relationship classification, coverage status, confidence rating, rationale, and residual gap. Reverse coverage was then assessed for every CSF subcategory.

Code	Meaning
SP	Strong partial: substantial support, but material elements remain unmatched
P	Partial: meaningful overlap with narrower or different scope
S	Supporting: assists implementation but does not directly achieve the complete outcome
N	No material mapping
O	Outside scope
U	Unable to determine

5. Quantitative Overview

Metric	Result
GAISSF controls assessed	59

Metric	Result
NIST CSF Core subcategories assessed	106
Forward mapping records	182
Reverse coverage records	106

6. Function-Level Findings

GOVERN

31 NIST CSF subcategories were assessed. GAISSF evidence can support selected AI-system outcomes; enterprise-wide application, non-AI asset coverage, and organization-specific profile prioritization remain separate implementation responsibilities.

IDENTIFY

21 NIST CSF subcategories were assessed. GAISSF evidence can support selected AI-system outcomes; enterprise-wide application, non-AI asset coverage, and organization-specific profile prioritization remain separate implementation responsibilities.

PROTECT

22 NIST CSF subcategories were assessed. GAISSF evidence can support selected AI-system outcomes; enterprise-wide application, non-AI asset coverage, and organization-specific profile prioritization remain separate implementation responsibilities.

DETECT

11 NIST CSF subcategories were assessed. GAISSF evidence can support selected AI-system outcomes; enterprise-wide application, non-AI asset coverage, and organization-specific profile prioritization remain separate implementation responsibilities.

RESPOND

13 NIST CSF subcategories were assessed. GAISSF evidence can support selected AI-system outcomes; enterprise-wide application, non-AI asset coverage, and organization-specific profile prioritization remain separate implementation responsibilities.

RECOVER

8 NIST CSF subcategories were assessed. GAISSF evidence can support selected AI-system outcomes; enterprise-wide application, non-AI asset coverage, and organization-specific profile prioritization remain separate implementation responsibilities.

7. Reverse Coverage Register

NIST ID	Function	Category	Outcome	Mapped GAISSF controls	Coverage	Confidence	Residual gap
GV.OC-01	GOVERN	Organizational Context	The organizational mission is understood and informs cybersecurity risk management	D2-CTL-06	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
GV.OC-02	GOVERN	Organizational Context	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	D2-CTL-06	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
GV.OC-03	GOVERN	Organizational Context	Legal, regulatory, and contractual	D5-CTL-05, D8-CTL-05	Indirectly Supported	Low	GAISSF is AI-system-focused;

NIST ID	Function	Category	Outcome	Mapped GAISSF controls	Coverage	Confidence	Residual gap
			requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed				organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
GV.OC-04	GOVERN	Organizational Context	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.OC-05	GOVERN	Organizational Context	Outcomes, capabilities, and services that the organization depends on are understood and communicated	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.RM-01	GOVERN	Risk Management Strategy	Risk management objectives are established and agreed to by organizational stakeholders	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.RM-02	GOVERN	Risk Management Strategy	Risk appetite and risk tolerance statements are established, communicated, and maintained	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.RM-03	GOVERN	Risk Management Strategy	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.RM-04	GOVERN	Risk Management Strategy	Strategic direction that describes appropriate risk response options is established and communicated	D7-CTL-H05	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
GV.RM-05	GOVERN	Risk Management Strategy	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.RM-06	GOVERN	Risk Management Strategy	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.RM-07	GOVERN	Risk Management Strategy	Strategic opportunities, or positive risks, are characterized and included in organizational cybersecurity risk discussions	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.RR-01	GOVERN	Roles, Responsibilities, and Authorities	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.

NIST ID	Function	Category	Outcome	Mapped GAISSF controls	Coverage	Confidence	Residual gap
			continually improving				
GV.RR-02	GOVERN	Roles, Responsibilities, and Authorities	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.RR-03	GOVERN	Roles, Responsibilities, and Authorities	Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.RR-04	GOVERN	Roles, Responsibilities, and Authorities	Cybersecurity is included in human resources practices	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.PO-01	GOVERN	Policy	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.PO-02	GOVERN	Policy	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	D6-CTL-03	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
GV.OV-01	GOVERN	Oversight	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.OV-02	GOVERN	Oversight	The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	D8-CTL-01	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
GV.OV-03	GOVERN	Oversight	Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.SC-01	GOVERN	Cybersecurity Supply Chain Risk Management	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
GV.SC-02	GOVERN	Cybersecurity Supply Chain Risk Management	Cybersecurity roles and responsibilities for suppliers, customers, and	D6-CTL-06, D1-CTL-01, D1-CTL-06, D1-CTL-07, D4-CTL-02, D4-CTL-03, D4-CTL-	Partially Addressed	Medium	GAISSF is AI-system-focused; organization-wide cybersecurity

NIST ID	Function	Category	Outcome	Mapped GAISSF controls	Coverage	Confidence	Residual gap
			partners are established, communicated, and coordinated internally and externally	04, D4-CTL-05			outcomes and non-AI ICT assets require additional controls.
GV.SC-03	GOVERN	Cybersecurity Supply Chain Risk Management	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	D8-CTL-01	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
GV.SC-04	GOVERN	Cybersecurity Supply Chain Risk Management	Suppliers are known and prioritized by criticality	D1-CTL-06, D1-CTL-07	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
GV.SC-05	GOVERN	Cybersecurity Supply Chain Risk Management	Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and agreements with suppliers and other relevant third parties	D4-CTL-03, D6-CTL-06, D1-CTL-06, D1-CTL-07, D4-CTL-02, D4-CTL-04, D4-CTL-05, D4-CTL-06	Partially Addressed	Medium	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
GV.SC-06	GOVERN	Cybersecurity Supply Chain Risk Management	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	D4-CTL-03, D6-CTL-06, D1-CTL-06, D1-CTL-07, D3-CTL-05, D4-CTL-02, D4-CTL-04, D4-CTL-05	Partially Addressed	Medium	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
GV.SC-07	GOVERN	Cybersecurity Supply Chain Risk Management	The risks posed by suppliers, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the relationship	D1-CTL-01, D4-CTL-03, D6-CTL-06, D1-CTL-06, D1-CTL-07, D4-CTL-02, D4-CTL-04, D4-CTL-05	Partially Addressed	Medium	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
GV.SC-08	GOVERN	Cybersecurity Supply Chain Risk Management	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	D1-CTL-01, D4-CTL-01, D6-CTL-06, D4-CTL-03, D9-CTL-04, D1-CTL-03, D1-CTL-05, D3-CTL-07	Substantially Addressed	Medium-High	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
GV.SC-09	GOVERN	Cybersecurity Supply Chain Risk Management	Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and performance is monitored throughout the technology product and service life cycle	D2-CTL-04, D3-CTL-03	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
GV.SC-10	GOVERN	Cybersecurity Supply Chain Risk Management	Cybersecurity supply chain risk management plans include provisions for activities after	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.

NIST ID	Function	Category	Outcome	Mapped GAISSF controls	Coverage	Confidence	Residual gap
			the conclusion of a partnership or service agreement				
ID.AM-01	IDENTIFY	Asset Management	Inventories of hardware managed by the organization are maintained	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.AM-02	IDENTIFY	Asset Management	Inventories of software, services, and systems managed by the organization are maintained	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.AM-03	IDENTIFY	Asset Management	Representations of the organization's authorized network communication and internal and external network data flows are maintained	D2-CTL-02	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
ID.AM-04	IDENTIFY	Asset Management	Inventories of services provided by suppliers are maintained	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.AM-05	IDENTIFY	Asset Management	Assets are prioritized based on classification, criticality, resources, and impact on the mission	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.AM-07	IDENTIFY	Asset Management	Inventories of data and corresponding metadata for designated data types are maintained	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.AM-08	IDENTIFY	Asset Management	Systems, hardware, software, services, and data are managed throughout their life cycles	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.RA-01	IDENTIFY	Risk Assessment	Vulnerabilities in assets are identified, validated, and recorded	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.RA-02	IDENTIFY	Risk Assessment	Cyber threat intelligence is received from information sharing forums and sources	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.RA-03	IDENTIFY	Risk Assessment	Internal and external threats to the organization are identified and recorded	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.RA-04	IDENTIFY	Risk Assessment	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.RA-05	IDENTIFY	Risk Assessment	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.RA-06	IDENTIFY	Risk Assessment	Risk responses are chosen, prioritized, planned, tracked, and communicated	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.RA-07	IDENTIFY	Risk Assessment	Changes and exceptions are managed, assessed for risk impact,	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.

NIST ID	Function	Category	Outcome	Mapped GAISSF controls	Coverage	Confidence	Residual gap
			recorded, and tracked				
ID.RA-08	IDENTIFY	Risk Assessment	Processes for receiving, analyzing, and responding to vulnerability disclosures are established	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.RA-09	IDENTIFY	Risk Assessment	The authenticity and integrity of hardware and software are assessed prior to acquisition and use	D1-CTL-04, D1-CTL-08, D1-CTL-09, D2-CTL-02, D3-CTL-04, D3-CTL-06, D5-CTL-01	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
ID.RA-10	IDENTIFY	Risk Assessment	Critical suppliers are assessed prior to acquisition	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.IM-01	IDENTIFY	Improvement	Improvements are identified from evaluations	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.IM-02	IDENTIFY	Improvement	Improvements are identified from security tests and exercises, including those coordinated with suppliers and relevant third parties	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.IM-03	IDENTIFY	Improvement	Improvements are identified from execution of operational processes, procedures, and activities	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
ID.IM-04	IDENTIFY	Improvement	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
PR.AA-01	PROTECT	Identity Management, Authentication, and Access Control	Identities and credentials for authorized users, services, and hardware are managed by the organization	D7-CTL-H03	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
PR.AA-02	PROTECT	Identity Management, Authentication, and Access Control	Identities are proofed and bound to credentials based on the context of interactions	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
PR.AA-03	PROTECT	Identity Management, Authentication, and Access Control	Users, services, and hardware are authenticated	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
PR.AA-04	PROTECT	Identity Management, Authentication, and Access Control	Identity assertions are protected, conveyed, and verified	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
PR.AA-05	PROTECT	Identity Management, Authentication, and Access Control	Access permissions, entitlements, and authorizations are defined in policy, managed, enforced, and reviewed, incorporating least privilege and separation of duties	D3-CTL-01, D6-CTL-05, D7-CTL-H03	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
PR.AA-06	PROTECT	Identity	Physical access	D9-CTL-01, D9-	Partially	Medium	GAISSF is AI-

NIST ID	Function	Category	Outcome	Mapped GAISSF controls	Coverage	Confidence	Residual gap
		Management, Authentication, and Access Control	to assets is managed, monitored, and enforced commensurate with risk	CTL-02, D9-CTL-03, D9-CTL-04, D9-CTL-05, D9-CTL-07, D1-CTL-04, D1-CTL-08	Addressed		system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
PR.AT-01	PROTECT	Awareness and Training	Personnel receive awareness and training to possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	D1-CTL-02, D2-CTL-03, D5-CTL-06, D7-CTL-H01, D8-CTL-03	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
PR.AT-02	PROTECT	Awareness and Training	Individuals in specialized roles receive awareness and training to possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	D1-CTL-02, D2-CTL-03, D5-CTL-06, D7-CTL-H01, D8-CTL-03	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
PR.DS-01	PROTECT	Data Security	The confidentiality, integrity, and availability of data at rest are protected	D2-CTL-05, D5-CTL-05, D6-CTL-07	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
PR.DS-02	PROTECT	Data Security	The confidentiality, integrity, and availability of data in transit are protected	D2-CTL-05	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
PR.DS-10	PROTECT	Data Security	The confidentiality, integrity, and availability of data in use are protected	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
PR.DS-11	PROTECT	Data Security	Backups of data are created, protected, maintained, and tested	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
PR.PS-01	PROTECT	Platform Security	Configuration management practices are established and applied	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
PR.PS-02	PROTECT	Platform Security	Software is maintained, replaced, and removed commensurate with risk	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
PR.PS-03	PROTECT	Platform Security	Hardware is maintained, replaced, and removed commensurate with risk	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
PR.PS-04	PROTECT	Platform Security	Log records are generated and made available for continuous monitoring	D2-CTL-04	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
PR.PS-05	PROTECT	Platform Security	Installation and execution of unauthorized software are prevented	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.

NIST ID	Function	Category	Outcome	Mapped GAISSF controls	Coverage	Confidence	Residual gap
PR.PS-06	PROTECT	Platform Security	Secure software development practices are integrated, and performance is monitored throughout the software development life cycle	D8-CTL-05	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
PR.IR-01	PROTECT	Technology Infrastructure Resilience	Networks and environments are protected from unauthorized logical access and usage	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
PR.IR-02	PROTECT	Technology Infrastructure Resilience	Technology assets are protected from environmental threats	D3-CTL-02	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
PR.IR-03	PROTECT	Technology Infrastructure Resilience	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
PR.IR-04	PROTECT	Technology Infrastructure Resilience	Adequate resource capacity to ensure availability is maintained	D6-CTL-07	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
DE.CM-01	DETECT	Continuous Monitoring	Networks and network services are monitored to find potentially adverse events	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
DE.CM-02	DETECT	Continuous Monitoring	The physical environment is monitored to find potentially adverse events	D9-CTL-05, D9-CTL-07, D5-CTL-02, D5-CTL-03, D9-CTL-01, D9-CTL-02, D9-CTL-03, D9-CTL-04	Partially Addressed	Medium	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
DE.CM-03	DETECT	Continuous Monitoring	Personnel activity and technology usage are monitored to find potentially adverse events	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
DE.CM-06	DETECT	Continuous Monitoring	External service provider activities and services are monitored to find potentially adverse events	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
DE.CM-09	DETECT	Continuous Monitoring	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
DE.AE-02	DETECT	Adverse Event Analysis	Potentially adverse events are analyzed to better understand associated activities	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
DE.AE-03	DETECT	Adverse Event Analysis	Information is correlated from multiple sources	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
DE.AE-04	DETECT	Adverse Event	The estimated	None	Not Addressed	Not Rated	No sufficiently

NIST ID	Function	Category	Outcome	Mapped GAISSF controls	Coverage	Confidence	Residual gap
		Analysis	impact and scope of adverse events are understood				direct GAISSF control was identified.
DE.AE-06	DETECT	Adverse Event Analysis	Information on adverse events is provided to authorized staff and tools	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
DE.AE-07	DETECT	Adverse Event Analysis	Cyber threat intelligence and other contextual information are integrated into analysis	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
DE.AE-08	DETECT	Adverse Event Analysis	Incidents are declared when adverse events meet defined incident criteria	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
RS.MA-01	RESPOND	Incident Management	The incident response plan is executed in coordination with relevant third parties once an incident is declared	D7-CTL-H04	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
RS.MA-02	RESPOND	Incident Management	Incident reports are triaged and validated	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
RS.MA-03	RESPOND	Incident Management	Incidents are categorized and prioritized	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
RS.MA-04	RESPOND	Incident Management	Incidents are escalated or elevated as needed	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
RS.MA-05	RESPOND	Incident Management	Criteria for initiating incident recovery are applied	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
RS.AN-03	RESPOND	Incident Analysis	Analysis is performed to establish what occurred during an incident and its root cause	D9-CTL-04	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
RS.AN-06	RESPOND	Incident Analysis	Actions performed during an investigation are recorded, and record integrity and provenance are preserved	D1-CTL-01, D4-CTL-01, D9-CTL-07, D1-CTL-03, D1-CTL-05, D2-CTL-01, D5-CTL-04, D6-CTL-01	Partially Addressed	Medium	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
RS.AN-07	RESPOND	Incident Analysis	Incident data and metadata are collected, and their integrity and provenance are preserved	D1-CTL-01, D4-CTL-01, D1-CTL-03, D1-CTL-05, D2-CTL-01, D5-CTL-04, D6-CTL-01, D6-CTL-04	Partially Addressed	Medium	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
RS.AN-08	RESPOND	Incident Analysis	An incident's magnitude is estimated and validated	D2-CTL-01, D5-CTL-04	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
RS.CO-02	RESPOND	Incident Response Reporting and Communication	Internal and external stakeholders are notified of incidents	D8-CTL-04	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional

NIST ID	Function	Category	Outcome	Mapped GAISSF controls	Coverage	Confidence	Residual gap
							controls.
RS.CO-03	RESPOND	Incident Response Reporting and Communication	Information is shared with designated internal and external stakeholders	D8-CTL-04	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
RS.MI-01	RESPOND	Incident Mitigation	Incidents are contained	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
RS.MI-02	RESPOND	Incident Mitigation	Incidents are eradicated	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
RC.RP-01	RECOVER	Incident Recovery Plan Execution	The recovery portion of the incident response plan is executed once initiated from the incident response process	D7-CTL-H04	Indirectly Supported	Low	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
RC.RP-02	RECOVER	Incident Recovery Plan Execution	Recovery actions are selected, scoped, prioritized, and performed	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
RC.RP-03	RECOVER	Incident Recovery Plan Execution	The integrity of backups and other restoration assets is verified before use	D4-CTL-01, D1-CTL-03, D1-CTL-05, D2-CTL-01, D5-CTL-04, D6-CTL-01, D6-CTL-04, D7-CTL-H02	Partially Addressed	Medium	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
RC.RP-04	RECOVER	Incident Recovery Plan Execution	Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	D9-CTL-04, D9-CTL-07, D1-CTL-03, D3-CTL-07, D6-CTL-01, D6-CTL-04, D9-CTL-01	Partially Addressed	Medium	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
RC.RP-05	RECOVER	Incident Recovery Plan Execution	The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	D4-CTL-01, D1-CTL-05, D2-CTL-01, D5-CTL-04, D7-CTL-H02, D9-CTL-01, D9-CTL-05	Partially Addressed	Medium	GAISSF is AI-system-focused; organization-wide cybersecurity outcomes and non-AI ICT assets require additional controls.
RC.RP-06	RECOVER	Incident Recovery Plan Execution	The end of incident recovery is declared based on criteria, and incident-related documentation is completed	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
RC.CO-03	RECOVER	Incident Recovery Communication	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.
RC.CO-04	RECOVER	Incident Recovery Communication	Public updates on incident recovery are shared using approved methods and messaging	None	Not Addressed	Not Rated	No sufficiently direct GAISSF control was identified.

8. GAISSF-to-NIST Mapping Register

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
CRO023-MAP-0001	D1-CTL-01	Dataset Provenance & Poisoning Prevention	GV.SC-08	GOVERN	SP	Medium-High	GAISSF D1-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0002	D1-CTL-01	Dataset Provenance & Poisoning Prevention	RS.AN-07	RESPOND	P	Medium	GAISSF D1-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0003	D1-CTL-01	Dataset Provenance & Poisoning Prevention	GV.SC-07	GOVERN	P	Medium	GAISSF D1-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0004	D1-CTL-01	Dataset Provenance & Poisoning Prevention	RS.AN-06	RESPOND	P	Medium	GAISSF D1-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0005	D1-CTL-01	Dataset Provenance & Poisoning Prevention	GV.SC-02	GOVERN	S	Low	GAISSF D1-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							neutral.	
CRO023-MAP-0006	D1-CTL-02	Model Extraction Resistance	PR.AT-01	PROTECT	S	Low	GAISSF D1-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AT-01. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0007	D1-CTL-02	Model Extraction Resistance	PR.AT-02	PROTECT	S	Low	GAISSF D1-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AT-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0008	D1-CTL-03	Behavioral Drift Detection	RS.AN-07	RESPOND	S	Low	GAISSF D1-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0009	D1-CTL-03	Behavioral Drift Detection	GV.SC-08	GOVERN	S	Low	GAISSF D1-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0010	D1-CTL-03	Behavioral Drift Detection	RS.AN-06	RESPOND	S	Low	GAISSF D1-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-	D1-CTL-03	Behavioral	RC.RP-03	RECOVER	S	Low	GAISSF D1-	Organization-

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
0011		Drift Detection					CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-03. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0012	D1-CTL-03	Behavioral Drift Detection	RC.RP-04	RECOVER	S	Low	GAISSF D1-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-04. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0013	D1-CTL-04	Federated Learning Poisoning Prevention	ID.RA-09	IDENTIFY	S	Low	GAISSF D1-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in ID.RA-09. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0014	D1-CTL-04	Federated Learning Poisoning Prevention	PR.AA-06	PROTECT	S	Low	GAISSF D1-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0015	D1-CTL-05	Embedding Space Robustness	RC.RP-05	RECOVER	S	Low	GAISSF D1-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0016	D1-CTL-05	Embedding Space Robustness	GV.SC-08	GOVERN	S	Low	GAISSF D1-CTL-05 provides AI-	Organization-wide ICT scope,

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0017	D1-CTL-05	Embedding Space Robustness	RS.AN-06	RESPOND	S	Low	GAISSF D1-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0018	D1-CTL-05	Embedding Space Robustness	RS.AN-07	RESPOND	S	Low	GAISSF D1-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0019	D1-CTL-05	Embedding Space Robustness	RC.RP-03	RECOVER	S	Low	GAISSF D1-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-03. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0020	D1-CTL-06	Post-Quantum Model Signing & Crypto Hardening	GV.SC-02	GOVERN	S	Low	GAISSF D1-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0021	D1-CTL-06	Post-Quantum Model Signing & Crypto Hardening	GV.SC-04	GOVERN	S	Low	GAISSF D1-CTL-06 provides AI-system-specific	Organization-wide ICT scope, enterprise context, and

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							controls and evidence that support the cybersecurity outcome in GV.SC-04. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0022	D1-CTL-06	Post-Quantum Model Signing & Crypto Hardening	GV.SC-05	GOVERN	S	Low	GAISSF D1-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0023	D1-CTL-06	Post-Quantum Model Signing & Crypto Hardening	GV.SC-06	GOVERN	S	Low	GAISSF D1-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0024	D1-CTL-06	Post-Quantum Model Signing & Crypto Hardening	GV.SC-07	GOVERN	S	Low	GAISSF D1-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0025	D1-CTL-07	Lora/Adapter Integrity Verification	GV.SC-02	GOVERN	S	Low	GAISSF D1-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0026	D1-CTL-07	Lora/Adapter Integrity Verification	GV.SC-04	GOVERN	S	Low	GAISSF D1-CTL-07 provides AI-system-specific controls and evidence that	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							support the cybersecurity outcome in GV.SC-04. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0027	D1-CTL-07	Lora/Adapter Integrity Verification	GV.SC-05	GOVERN	S	Low	GAISSF D1-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0028	D1-CTL-07	Lora/Adapter Integrity Verification	GV.SC-06	GOVERN	S	Low	GAISSF D1-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0029	D1-CTL-07	Lora/Adapter Integrity Verification	GV.SC-07	GOVERN	S	Low	GAISSF D1-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0030	D1-CTL-08	Model Merge Attack Detection	PR.AA-06	PROTECT	S	Low	GAISSF D1-CTL-08 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0031	D1-CTL-08	Model Merge Attack Detection	ID.RA-09	IDENTIFY	S	Low	GAISSF D1-CTL-08 provides AI-system-specific controls and evidence that support the cybersecurity	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							outcome in ID.RA-09. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	scope and require separate implementation evidence.
CRO023-MAP-0032	D1-CTL-09	Quantization Backdoor Screening	PR.AA-06	PROTECT	S	Low	GAISSF D1-CTL-09 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0033	D1-CTL-09	Quantization Backdoor Screening	ID.RA-09	IDENTIFY	S	Low	GAISSF D1-CTL-09 provides AI-system-specific controls and evidence that support the cybersecurity outcome in ID.RA-09. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0034	D2-CTL-01	Direct Prompt Injection Prevention	RS.AN-07	RESPOND	S	Low	GAISSF D2-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0035	D2-CTL-01	Direct Prompt Injection Prevention	RS.AN-06	RESPOND	S	Low	GAISSF D2-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0036	D2-CTL-01	Direct Prompt Injection Prevention	RC.RP-03	RECOVER	S	Low	GAISSF D2-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-03. The	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	separate implementation evidence.
CRO023-MAP-0037	D2-CTL-01	Direct Prompt Injection Prevention	RC.RP-05	RECOVER	S	Low	GAISSF D2-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0038	D2-CTL-01	Direct Prompt Injection Prevention	RS.AN-08	RESPOND	S	Low	GAISSF D2-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0039	D2-CTL-02	Indirect Prompt Injection Prevention	ID.RA-09	IDENTIFY	S	Low	GAISSF D2-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in ID.RA-09. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0040	D2-CTL-02	Indirect Prompt Injection Prevention	ID.AM-03	IDENTIFY	S	Low	GAISSF D2-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in ID.AM-03. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0041	D2-CTL-03	Jailbreak Resistance Testing	PR.AT-01	PROTECT	S	Low	GAISSF D2-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AT-01. The relationship is outcome-	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementatio

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							based; NIST CSF 2.0 remains broader and technology-neutral.	n evidence.
CRO023-MAP-0042	D2-CTL-03	Jailbreak Resistance Testing	PR.AT-02	PROTECT	S	Low	GAISSF D2-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AT-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0043	D2-CTL-04	Multi-Modal Injection Defense	GV.SC-09	GOVERN	S	Low	GAISSF D2-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-09. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0044	D2-CTL-04	Multi-Modal Injection Defense	PR.PS-04	PROTECT	S	Low	GAISSF D2-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.PS-04. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0045	D2-CTL-05	Function Call/Tool Call Injection Prevention	PR.DS-01	PROTECT	S	Low	GAISSF D2-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.DS-01. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0046	D2-CTL-05	Function Call/Tool Call Injection Prevention	PR.DS-02	PROTECT	S	Low	GAISSF D2-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.DS-02. The relationship is outcome-based; NIST CSF 2.0	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							remains broader and technology-neutral.	
CRO023-MAP-0047	D2-CTL-06	Cross-Context Hijacking Mitigation	GV.OC-01	GOVERN	S	Low	GAISSF D2-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.OC-01. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0048	D2-CTL-06	Cross-Context Hijacking Mitigation	GV.OC-02	GOVERN	S	Low	GAISSF D2-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.OC-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0049	D3-CTL-01	Least Agency Enforcement	PR.AA-06	PROTECT	S	Low	GAISSF D3-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0050	D3-CTL-01	Least Agency Enforcement	PR.AA-05	PROTECT	S	Low	GAISSF D3-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0051	D3-CTL-02	Inter-Agent Communication Security	PR.AA-06	PROTECT	S	Low	GAISSF D3-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							technology-neutral.	
CRO023-MAP-0052	D3-CTL-02	Inter-Agent Communication Security	PR.IR-02	PROTECT	S	Low	GAISSF D3-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.IR-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0053	D3-CTL-03	Agentic Prompt Chaining Detection	PR.AA-06	PROTECT	S	Low	GAISSF D3-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0054	D3-CTL-03	Agentic Prompt Chaining Detection	GV.SC-09	GOVERN	S	Low	GAISSF D3-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-09. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0055	D3-CTL-04	Embodied Ai Safety Controls	ID.RA-09	IDENTIFY	S	Low	GAISSF D3-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in ID.RA-09. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0056	D3-CTL-04	Embodied Ai Safety Controls	PR.AA-06	PROTECT	S	Low	GAISSF D3-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
CRO023-MAP-0057	D3-CTL-05	Multi-Agent Trust Chain Attestation	PR.AA-06	PROTECT	S	Low	GAISSF D3-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0058	D3-CTL-05	Multi-Agent Trust Chain Attestation	GV.SC-06	GOVERN	S	Low	GAISSF D3-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0059	D3-CTL-06	Persistent Memory Exfiltration Prevention	PR.AA-06	PROTECT	S	Low	GAISSF D3-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0060	D3-CTL-06	Persistent Memory Exfiltration Prevention	ID.RA-09	IDENTIFY	S	Low	GAISSF D3-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in ID.RA-09. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0061	D3-CTL-07	Secure Memory Lifecycle Management	GV.SC-08	GOVERN	S	Low	GAISSF D3-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0062	D3-CTL-07	Secure Memory	RC.RP-04	RECOVER	S	Low	GAISSF D3-CTL-07	Organization-wide ICT

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
		Lifecycle Management					provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-04. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0063	D4-CTL-01	Ai Bill Of Materials (Ai Bom) Maintenance	GV.SC-08	GOVERN	SP	Medium-High	GAISSF D4-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0064	D4-CTL-01	Ai Bill Of Materials (Ai Bom) Maintenance	RS.AN-06	RESPOND	P	Medium	GAISSF D4-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0065	D4-CTL-01	Ai Bill Of Materials (Ai Bom) Maintenance	RS.AN-07	RESPOND	P	Medium	GAISSF D4-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0066	D4-CTL-01	Ai Bill Of Materials (Ai Bom) Maintenance	RC.RP-03	RECOVER	P	Medium	GAISSF D4-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-03. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0067	D4-CTL-01	Ai Bill Of Materials (Ai Bom) Maintenance	RC.RP-05	RECOVER	P	Medium	GAISSF D4-CTL-01 provides AI-system-	Organization-wide ICT scope, enterprise

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							specific controls and evidence that support the cybersecurity outcome in RC.RP-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0068	D4-CTL-02	Model File & Artifact Scanning	GV.SC-07	GOVERN	S	Low	GAISSF D4-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0069	D4-CTL-02	Model File & Artifact Scanning	GV.SC-06	GOVERN	S	Low	GAISSF D4-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0070	D4-CTL-02	Model File & Artifact Scanning	GV.SC-05	GOVERN	S	Low	GAISSF D4-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0071	D4-CTL-02	Model File & Artifact Scanning	GV.SC-08	GOVERN	S	Low	GAISSF D4-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0072	D4-CTL-02	Model File & Artifact Scanning	GV.SC-02	GOVERN	S	Low	GAISSF D4-CTL-02 provides AI-system-specific controls and	Organization-wide ICT scope, enterprise context, and non-AI assets

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							evidence that support the cybersecurity outcome in GV.SC-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0073	D4-CTL-03	Model Hub & Registry Vetting	GV.SC-06	GOVERN	P	Medium	GAISSF D4-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0074	D4-CTL-03	Model Hub & Registry Vetting	GV.SC-05	GOVERN	P	Medium	GAISSF D4-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0075	D4-CTL-03	Model Hub & Registry Vetting	GV.SC-07	GOVERN	P	Medium	GAISSF D4-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0076	D4-CTL-03	Model Hub & Registry Vetting	GV.SC-08	GOVERN	P	Medium	GAISSF D4-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0077	D4-CTL-03	Model Hub & Registry Vetting	GV.SC-02	GOVERN	S	Low	GAISSF D4-CTL-03 provides AI-system-specific controls and evidence that support the	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							cybersecurity outcome in GV.SC-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0078	D4-CTL-04	Mcp Server Behavioral Monitoring	GV.SC-07	GOVERN	S	Low	GAISSF D4-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0079	D4-CTL-04	Mcp Server Behavioral Monitoring	GV.SC-06	GOVERN	S	Low	GAISSF D4-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0080	D4-CTL-04	Mcp Server Behavioral Monitoring	GV.SC-05	GOVERN	S	Low	GAISSF D4-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0081	D4-CTL-04	Mcp Server Behavioral Monitoring	GV.SC-08	GOVERN	S	Low	GAISSF D4-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0082	D4-CTL-04	Mcp Server Behavioral Monitoring	GV.SC-02	GOVERN	S	Low	GAISSF D4-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							GV.SC-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	require separate implementation evidence.
CRO023-MAP-0083	D4-CTL-05	Third-Party Ai Api Security Assessment	GV.SC-05	GOVERN	S	Low	GAISSF D4-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0084	D4-CTL-05	Third-Party Ai Api Security Assessment	GV.SC-06	GOVERN	S	Low	GAISSF D4-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0085	D4-CTL-05	Third-Party Ai Api Security Assessment	GV.SC-07	GOVERN	S	Low	GAISSF D4-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0086	D4-CTL-05	Third-Party Ai Api Security Assessment	GV.SC-08	GOVERN	S	Low	GAISSF D4-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0087	D4-CTL-05	Third-Party Ai Api Security Assessment	GV.SC-02	GOVERN	S	Low	GAISSF D4-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-02. The relationship is	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	implementation evidence.
CRO023-MAP-0088	D4-CTL-06	Shadow Ai Discovery & Governance	GV.SC-07	GOVERN	S	Low	GAISSF D4-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0089	D4-CTL-06	Shadow Ai Discovery & Governance	GV.SC-02	GOVERN	S	Low	GAISSF D4-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0090	D4-CTL-06	Shadow Ai Discovery & Governance	GV.SC-06	GOVERN	S	Low	GAISSF D4-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0091	D4-CTL-06	Shadow Ai Discovery & Governance	GV.SC-05	GOVERN	S	Low	GAISSF D4-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0092	D4-CTL-06	Shadow Ai Discovery & Governance	GV.SC-08	GOVERN	S	Low	GAISSF D4-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							CSF 2.0 remains broader and technology-neutral.	
CRO023-MAP-0093	D4-CTL-07	Ai Software Composition Analysis (Sca)	GV.SC-06	GOVERN	S	Low	GAISSF D4-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0094	D4-CTL-07	Ai Software Composition Analysis (Sca)	GV.SC-05	GOVERN	S	Low	GAISSF D4-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0095	D4-CTL-07	Ai Software Composition Analysis (Sca)	GV.SC-07	GOVERN	S	Low	GAISSF D4-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0096	D4-CTL-07	Ai Software Composition Analysis (Sca)	GV.SC-08	GOVERN	S	Low	GAISSF D4-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0097	D4-CTL-07	Ai Software Composition Analysis (Sca)	GV.SC-02	GOVERN	S	Low	GAISSF D4-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-02. The relationship is outcome-based; NIST CSF 2.0 remains	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							broader and technology-neutral.	
CRO023-MAP-0098	D5-CTL-01	Harmful Content Blocking	ID.RA-09	IDENTIFY	S	Low	GAISSF D5-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in ID.RA-09. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0099	D5-CTL-01	Harmful Content Blocking	PR.AA-06	PROTECT	S	Low	GAISSF D5-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0100	D5-CTL-02	Pii Leakage Prevention	PR.AA-06	PROTECT	S	Low	GAISSF D5-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0101	D5-CTL-02	Pii Leakage Prevention	DE.CM-02	DETECT	S	Low	GAISSF D5-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in DE.CM-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0102	D5-CTL-03	Copyright Detection	PR.AA-06	PROTECT	S	Low	GAISSF D5-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							neutral.	
CRO023-MAP-0103	D5-CTL-03	Copyright Detection	DE.CM-02	DETECT	S	Low	GAISSF D5-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in DE.CM-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0104	D5-CTL-04	Ai Watermarking Robustness	RS.AN-06	RESPOND	S	Low	GAISSF D5-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0105	D5-CTL-04	Ai Watermarking Robustness	RS.AN-07	RESPOND	S	Low	GAISSF D5-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0106	D5-CTL-04	Ai Watermarking Robustness	RC.RP-03	RECOVER	S	Low	GAISSF D5-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-03. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0107	D5-CTL-04	Ai Watermarking Robustness	RC.RP-05	RECOVER	S	Low	GAISSF D5-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-	D5-CTL-04	Ai	RS.AN-08	RESPOND	S	Low	GAISSF D5-	Organization-

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
0108		Watermarking Robustness					CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0109	D5-CTL-05	Privacy-By-Design Verification	GV.OC-03	GOVERN	S	Low	GAISSF D5-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.OC-03. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0110	D5-CTL-05	Privacy-By-Design Verification	PR.DS-01	PROTECT	S	Low	GAISSF D5-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.DS-01. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0111	D5-CTL-06	Privacy-Preserving Ml Validation	PR.AT-01	PROTECT	S	Low	GAISSF D5-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AT-01. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0112	D5-CTL-06	Privacy-Preserving Ml Validation	PR.AT-02	PROTECT	S	Low	GAISSF D5-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AT-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0113	D6-CTL-01	Human-In-The-Loop For High-Risk Actions	RC.RP-04	RECOVER	S	Low	GAISSF D6-CTL-01 provides AI-	Organization-wide ICT scope,

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							system-specific controls and evidence that support the cybersecurity outcome in RC.RP-04. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0114	D6-CTL-01	Human-In-The-Loop For High-Risk Actions	GV.SC-08	GOVERN	S	Low	GAISSF D6-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0115	D6-CTL-01	Human-In-The-Loop For High-Risk Actions	RS.AN-06	RESPOND	S	Low	GAISSF D6-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0116	D6-CTL-01	Human-In-The-Loop For High-Risk Actions	RS.AN-07	RESPOND	S	Low	GAISSF D6-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0117	D6-CTL-01	Human-In-The-Loop For High-Risk Actions	RC.RP-03	RECOVER	S	Low	GAISSF D6-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-03. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0118	D6-CTL-02	Audit Trail Completeness	RS.AN-06	RESPOND	S	Low	GAISSF D6-CTL-02 provides AI-system-specific	Organization-wide ICT scope, enterprise context, and

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							controls and evidence that support the cybersecurity outcome in RS.AN-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0119	D6-CTL-03	Ai Model Card Completeness	GV.PO-02	GOVERN	S	Low	GAISSF D6-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.PO-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0120	D6-CTL-03	Ai Model Card Completeness	GV.SC-02	GOVERN	S	Low	GAISSF D6-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0121	D6-CTL-04	Ai Incident Response Readiness	GV.SC-08	GOVERN	S	Low	GAISSF D6-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0122	D6-CTL-04	Ai Incident Response Readiness	RS.AN-07	RESPOND	S	Low	GAISSF D6-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0123	D6-CTL-04	Ai Incident Response Readiness	RS.AN-06	RESPOND	S	Low	GAISSF D6-CTL-04 provides AI-system-specific controls and evidence that	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							support the cybersecurity outcome in RS.AN-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0124	D6-CTL-04	Ai Incident Response Readiness	RC.RP-03	RECOVER	S	Low	GAISSF D6-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-03. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0125	D6-CTL-04	Ai Incident Response Readiness	RC.RP-04	RECOVER	S	Low	GAISSF D6-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-04. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0126	D6-CTL-05	Model Deprecation & Decommissioning	PR.AA-05	PROTECT	S	Low	GAISSF D6-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0127	D6-CTL-05	Model Deprecation & Decommissioning	PR.AA-06	PROTECT	S	Low	GAISSF D6-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0128	D6-CTL-06	Third-Party Ai Vendor Governance	GV.SC-08	GOVERN	SP	Medium-High	GAISSF D6-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	scope and require separate implementation evidence.
CRO023-MAP-0129	D6-CTL-06	Third-Party Ai Vendor Governance	GV.SC-02	GOVERN	P	Medium	GAISSF D6-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0130	D6-CTL-06	Third-Party Ai Vendor Governance	GV.SC-05	GOVERN	P	Medium	GAISSF D6-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0131	D6-CTL-06	Third-Party Ai Vendor Governance	GV.SC-06	GOVERN	P	Medium	GAISSF D6-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0132	D6-CTL-06	Third-Party Ai Vendor Governance	GV.SC-07	GOVERN	P	Medium	GAISSF D6-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0133	D6-CTL-07	Ai Resilience & Business Continuity	PR.IR-04	PROTECT	S	Low	GAISSF D6-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.IR-04. The	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	separate implementation evidence.
CRO023-MAP-0134	D6-CTL-07	Ai Resilience & Business Continuity	PR.DS-01	PROTECT	S	Low	GAISSF D6-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.DS-01. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0135	D7-CTL-H01	Ai-Generated Phishing Simulation	PR.AT-01	PROTECT	S	Low	GAISSF D7-CTL-H01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AT-01. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0136	D7-CTL-H01	Ai-Generated Phishing Simulation	PR.AT-02	PROTECT	S	Low	GAISSF D7-CTL-H01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AT-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0137	D7-CTL-H02	Deepfake Detection Training	RS.AN-07	RESPOND	S	Low	GAISSF D7-CTL-H02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0138	D7-CTL-H02	Deepfake Detection Training	RS.AN-06	RESPOND	S	Low	GAISSF D7-CTL-H02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-06. The relationship is outcome-	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementatio

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							based; NIST CSF 2.0 remains broader and technology-neutral.	n evidence.
CRO023-MAP-0139	D7-CTL-H02	Deepfake Detection Training	RC.RP-03	RECOVER	S	Low	GAISSF D7-CTL-H02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-03. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0140	D7-CTL-H02	Deepfake Detection Training	RC.RP-05	RECOVER	S	Low	GAISSF D7-CTL-H02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0141	D7-CTL-H03	Out-Of-Band Authentication	PR.AA-05	PROTECT	S	Low	GAISSF D7-CTL-H03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0142	D7-CTL-H03	Out-Of-Band Authentication	PR.AA-01	PROTECT	S	Low	GAISSF D7-CTL-H03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-01. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0143	D7-CTL-H04	Ai Social Engineering Ir	RS.MA-01	RESPOND	S	Low	GAISSF D7-CTL-H04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.MA-01. The relationship is outcome-based; NIST CSF 2.0	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							remains broader and technology-neutral.	
CRO023-MAP-0144	D7-CTL-H04	Ai Social Engineering Ir	RC.RP-01	RECOVER	S	Low	GAISSF D7-CTL-H04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-01. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0145	D7-CTL-H05	Ai-Enhanced External Attack Defense	GV.RM-04	GOVERN	S	Low	GAISSF D7-CTL-H05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.RM-04. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0146	D7-CTL-H05	Ai-Enhanced External Attack Defense	GV.SC-08	GOVERN	S	Low	GAISSF D7-CTL-H05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0147	D8-CTL-01	Eu Ai Act Risk Tier Mapping	GV.OV-02	GOVERN	S	Low	GAISSF D8-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.OV-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0148	D8-CTL-01	Eu Ai Act Risk Tier Mapping	GV.SC-03	GOVERN	S	Low	GAISSF D8-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-03. The relationship is outcome-based; NIST CSF 2.0 remains broader and	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							technology-neutral.	
CRO023-MAP-0149	D8-CTL-02	Iso 42001 Gap Analysis	GV.SC-06	GOVERN	S	Low	GAISSF D8-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0150	D8-CTL-02	Iso 42001 Gap Analysis	RS.AN-06	RESPOND	S	Low	GAISSF D8-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0151	D8-CTL-03	Gpai Technical Documentation Verification	PR.AT-01	PROTECT	S	Low	GAISSF D8-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AT-01. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0152	D8-CTL-03	Gpai Technical Documentation Verification	PR.AT-02	PROTECT	S	Low	GAISSF D8-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AT-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0153	D8-CTL-04	Dora Ict Incident Reporting (Financial Sector)	RS.CO-02	RESPOND	S	Low	GAISSF D8-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.CO-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
CRO023-MAP-0154	D8-CTL-04	Dora Ict Incident Reporting (Financial Sector)	RS.CO-03	RESPOND	S	Low	GAISSF D8-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.CO-03. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0155	D8-CTL-05	Nist Sp 800-218A Compliance Check	PR.PS-06	PROTECT	S	Low	GAISSF D8-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.PS-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0156	D8-CTL-05	Nist Sp 800-218A Compliance Check	GV.OC-03	GOVERN	S	Low	GAISSF D8-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.OC-03. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0157	D9-CTL-01	Physical Harm Boundary Enforcement	PR.AA-06	PROTECT	P	Medium	GAISSF D9-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0158	D9-CTL-01	Physical Harm Boundary Enforcement	DE.CM-02	DETECT	S	Low	GAISSF D9-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in DE.CM-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0159	D9-CTL-01	Physical Harm Boundary	RC.RP-04	RECOVER	S	Low	GAISSF D9-CTL-01	Organization-wide ICT

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
		Enforcement					provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-04. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0160	D9-CTL-01	Physical Harm Boundary Enforcement	RC.RP-05	RECOVER	S	Low	GAISSF D9-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0161	D9-CTL-01	Physical Harm Boundary Enforcement	GV.SC-08	GOVERN	S	Low	GAISSF D9-CTL-01 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0162	D9-CTL-02	Safe State And Graceful Degradation	PR.AA-06	PROTECT	P	Medium	GAISSF D9-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0163	D9-CTL-02	Safe State And Graceful Degradation	DE.CM-02	DETECT	S	Low	GAISSF D9-CTL-02 provides AI-system-specific controls and evidence that support the cybersecurity outcome in DE.CM-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0164	D9-CTL-03	Human Override And Emergency Stop	PR.AA-06	PROTECT	P	Medium	GAISSF D9-CTL-03 provides AI-system-	Organization-wide ICT scope, enterprise

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0165	D9-CTL-03	Human Override And Emergency Stop	DE.CM-02	DETECT	S	Low	GAISSF D9-CTL-03 provides AI-system-specific controls and evidence that support the cybersecurity outcome in DE.CM-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0166	D9-CTL-04	Cyber-Physical Attack Detection	PR.AA-06	PROTECT	P	Medium	GAISSF D9-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0167	D9-CTL-04	Cyber-Physical Attack Detection	RC.RP-04	RECOVER	P	Medium	GAISSF D9-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-04. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0168	D9-CTL-04	Cyber-Physical Attack Detection	GV.SC-08	GOVERN	P	Medium	GAISSF D9-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0169	D9-CTL-04	Cyber-Physical Attack Detection	DE.CM-02	DETECT	S	Low	GAISSF D9-CTL-04 provides AI-system-specific controls and	Organization-wide ICT scope, enterprise context, and non-AI assets

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							evidence that support the cybersecurity outcome in DE.CM-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0170	D9-CTL-04	Cyber-Physical Attack Detection	RS.AN-03	RESPOND	S	Low	GAISSF D9-CTL-04 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-03. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0171	D9-CTL-05	Physical Environment Integrity Monitoring	DE.CM-02	DETECT	P	Medium	GAISSF D9-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in DE.CM-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0172	D9-CTL-05	Physical Environment Integrity Monitoring	PR.AA-06	PROTECT	P	Medium	GAISSF D9-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0173	D9-CTL-05	Physical Environment Integrity Monitoring	RC.RP-05	RECOVER	S	Low	GAISSF D9-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-05. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0174	D9-CTL-05	Physical Environment Integrity Monitoring	RS.AN-06	RESPOND	S	Low	GAISSF D9-CTL-05 provides AI-system-specific controls and evidence that support the	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							cybersecurity outcome in RS.AN-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0175	D9-CTL-05	Physical Environment Integrity Monitoring	RS.AN-07	RESPOND	S	Low	GAISSF D9-CTL-05 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RS.AN-07. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0176	D9-CTL-06	Actuator Command Verification	PR.AA-06	PROTECT	S	Low	GAISSF D9-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0177	D9-CTL-06	Actuator Command Verification	DE.CM-02	DETECT	S	Low	GAISSF D9-CTL-06 provides AI-system-specific controls and evidence that support the cybersecurity outcome in DE.CM-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0178	D9-CTL-07	Physical Incident Evidence Preservation	PR.AA-06	PROTECT	P	Medium	GAISSF D9-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in PR.AA-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0179	D9-CTL-07	Physical Incident Evidence Preservation	RS.AN-06	RESPOND	P	Medium	GAISSF D9-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and

Record	GAISSF ID	GAISSF control	NIST ID	Function	Rel.	Confidence	Rationale	Residual gap
							RS.AN-06. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	require separate implementation evidence.
CRO023-MAP-0180	D9-CTL-07	Physical Incident Evidence Preservation	DE.CM-02	DETECT	P	Medium	GAISSF D9-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in DE.CM-02. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0181	D9-CTL-07	Physical Incident Evidence Preservation	RC.RP-04	RECOVER	P	Medium	GAISSF D9-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in RC.RP-04. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.
CRO023-MAP-0182	D9-CTL-07	Physical Incident Evidence Preservation	GV.SC-08	GOVERN	S	Low	GAISSF D9-CTL-07 provides AI-system-specific controls and evidence that support the cybersecurity outcome in GV.SC-08. The relationship is outcome-based; NIST CSF 2.0 remains broader and technology-neutral.	Organization-wide ICT scope, enterprise context, and non-AI assets remain outside the direct GAISSF control scope and require separate implementation evidence.

9. Evidence Reuse Guidance

Potentially reusable evidence includes AI system inventories, model and data provenance records, supplier assessments, threat models, vulnerability records, access-control configurations, security test reports, red-team reports, monitoring telemetry, incident records, recovery tests, risk-treatment decisions, and governance approvals. Reuse is valid only after scope, currency, ownership, and operating effectiveness are confirmed.

10. Limitations

- Mapping does not establish NIST endorsement, certification, equivalence, or regulatory compliance.
- GAISSF focuses on AI systems; NIST CSF 2.0 applies across organizational ICT, including non-AI assets.
- Relationship classifications describe textual and operational support, not operating effectiveness.
- Profiles, Tiers, and organization-specific risk tolerances must be developed by the implementing organization.
- Revalidate mappings when either source baseline changes.

11. Notably Absent

- No NIST certification or endorsement of GAISSF.
- No finding that GAISSF conformance automatically achieves a CSF Organizational Profile.
- No treatment of CSF Implementation Examples as mandatory requirements.
- No organization-independent compliance percentage or universal risk-tolerance threshold.
- No automatic coverage of non-AI enterprise assets, workforce processes, or broader ICT operations.

12. Conclusion

GAISSF can operate as an AI-security specialization layer within a broader NIST CSF 2.0 cybersecurity risk program. The mapping supports evidence reuse and gap identification, but it does not replace organization-wide cybersecurity governance, CSF Profile development, or verification of operating effectiveness.