

ODA3 INSTITUTE

CROSSWALK

GAISSF™—NIST CSF 2.0 Mapping

Cybersecurity Alignment Crosswalk — NIST CSWP 29

GAISSF-CRO-023 | Informative crosswalk | Draft for Publication

Candidate 29 June 2026 | Updated 5 October 2026

© 2026 ODA3 Pvt Ltd

GAISSF-CRO-023 — Website and Executive Summary

A cybersecurity-alignment crosswalk for AI systems

GAISSF-CRO-023 maps all 59 GAISSF™ v1.0 controls to the 106 NIST Cybersecurity Framework (CSF) 2.0 Core subcategories in NIST CSWP 29. It supports AI-security integration into organization-wide cybersecurity risk programs while preserving the narrower AI-system scope of GAISSF.

Document control

Document ID	GAISSF-CRO-023
Version	1.0
Status	Draft for Publication
Classification	Informative crosswalk / public
Candidate date	29 June 2026
Updated	5 October 2026
Publisher	ODA3 Institute
NIST target	NIST CSWP 29 — Cybersecurity Framework (CSF) 2.0

What the package contains

- 59 GAISSF controls assessed against 106 NIST CSF 2.0 Core subcategories.
- 182 documented forward mapping relationships with relationship, confidence, rationale, residual-gap, and source fields.
- A complete 106-subcategory NIST-to-GAISSF reverse coverage register.
- Separate treatment of CSF Implementation Examples as informative, non-exhaustive resources rather than mapping requirements.
- DOCX, PDF, XLSX, Markdown, and JSON publication formats.

Key interpretation

NIST CSF 2.0 is organization-wide and technology-neutral. GAISSF supplies AI-system-specific security, governance, evidence, and Physical-AI controls. The crosswalk can support evidence-reuse analysis and gap identification, but it does not establish equivalence, evidence sufficiency, operating effectiveness, NIST endorsement, regulatory compliance, certification, or automatic conformance.

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

CSF 2.0 Core functions

Function	Core subcategories
GOVERN	31
IDENTIFY	21
PROTECT	22
DETECT	11
RESPOND	13
RECOVER	8

Appropriate uses

- Create an AI-focused overlay for a CSF Current or Target Profile
- Reuse verified GAISSF evidence for selected CSF outcomes
- Identify cybersecurity capabilities required beyond GAISSF
- Support internal assurance, control rationalization, and implementation planning

- Scope independent assessment and evidence collection

Not established

- NIST endorsement, certification, or formal equivalence
- Automatic GAISSF or NIST CSF conformance
- Evidence sufficiency or proof of operating effectiveness
- A replacement for organization-wide CSF Profile development or independent assessment
- Regulatory compliance, safe harbour, or automatic recognition