

ODA3 INSTITUTE

CROSSWALK

GAISSF™—CIS Controls Mapping

Cybersecurity Control-Family Alignment Crosswalk — CIS Controls v8.1

GAISSF-CRO-033 | Informative crosswalk | Draft for Publication

Version 1.0 | Updated 6 October 2026

© 2026 ODA3 Pvt Ltd

Field	Controlled value
Document ID	GAISSF-CRO-033
Publisher	ODA3 Institute
Legal entity	ODA3 Pvt Ltd
GAISSF baseline	GAISSF™ v1.0; 59 controls / 9 domains; Applicable-Control Baseline = 52 D1-D8 + applicable D9
External baseline	CIS Controls v8.1; 18 Controls / 153 Safeguards
Mapping unit	18 CIS Control families
Safeguard context	153 Safeguards across IG1-IG3; not reproduced
Verification date	6 October 2026
Distribution	Public — docs.oda3.org / official ODA3 publication channels
Version	1.0
Status	Draft for Publication
Classification	Informative Control-family crosswalk / public

The crosswalk compares GAISSF control outcomes with the 18 CIS Control families. Safeguard-level requirements, asset classes, Implementation Group assignments, frequencies, measurement criteria and operating evidence remain governed by official CIS materials. Relationship and confidence ratings are analytical judgments only; they do not establish implementation, assessment results, evidence sufficiency, operating effectiveness or equivalence.

4. High-Alignment Areas

- Asset, software and supplier inventory
- Data protection, secure configuration and access control
- Vulnerability, logging, monitoring and malware defense
- Secure software development and penetration testing
- Incident response, recovery and workforce training

5. Material Residual Work

- Determine the applicable CIS Implementation Group using the enterprise's risk profile, resources, asset/data sensitivity and threat exposure; a GAISSF mapping does not select the Implementation Group.
- Assess every applicable CIS Safeguard at the Safeguard level rather than relying on Control-family coverage.
- Define enterprise asset classes, implementation frequencies and ownership
- Collect CIS-specific implementation and measurement evidence and evaluate operating effectiveness using the applicable CIS Controls Assessment Specification and organizational assessment method.
- Address enterprise IT controls outside GAISSF AI-system scope

6. Notably Absent

No basis is established to claim CIS endorsement, CIS Controls Accreditation, CIS SecureSuite status, implementation of all 153 Safeguards, correct Implementation Group selection, successful CIS Controls assessment, evidence sufficiency, operating effectiveness, or automatic GAISSF conformance.

7. CIS Control Coverage Register

Control	Title	Mapped GAISSF controls	Coverage
1	Inventory and Control of Enterprise Assets	10	Substantially Addressed
2	Inventory and Control of Software Assets	6	Partially Addressed
3	Data Protection	21	Substantially Addressed
4	Secure Configuration of Enterprise Assets and Software	7	Partially Addressed
5	Account Management	14	Substantially Addressed
6	Access Control Management	9	Substantially Addressed
7	Continuous Vulnerability Management	12	Substantially Addressed
8	Audit Log Management	21	Substantially Addressed
9	Email and Web Browser Protections	9	Substantially Addressed
10	Malware Defenses	14	Substantially Addressed
11	Data Recovery	1	Indirectly Supported
12	Network Infrastructure Management	3	Partially Addressed
13	Network Monitoring and Defense	13	Substantially Addressed
14	Security Awareness and Skills Training	10	Substantially Addressed
15	Service Provider Management	8	Substantially Addressed
16	Application Software Security	11	Substantially Addressed
17	Incident Response Management	5	Partially Addressed
18	Penetration Testing	20	Substantially Addressed

Annex A — Complete Mapping Register

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
GAISSF-CRO-033-MAP-0001	D1-CTL-01	8 — Audit Log Management	P	Medium	GAISSF D1-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0002	D1-CTL-01	3 — Data Protection	S	Medium	GAISSF D1-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0003	D1-CTL-01	18 — Penetration Testing	S	Medium	GAISSF D1-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0004	D1-CTL-01	13 — Network Monitoring and Defense	S	Medium	GAISSF D1-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 13 (Network

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Monitoring and Defense). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0005	D1-CTL-02	13 — Network Monitoring and Defense	P	Medium	GAISSF D1-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 13 (Network Monitoring and Defense). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0006	D1-CTL-02	7 — Continuous Vulnerability Management	S	Medium	GAISSF D1-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 7 (Continuous Vulnerability Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0007	D1-CTL-02	18 — Penetration Testing	S	Medium	GAISSF D1-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0008	D1-CTL-02	10 — Malware Defenses	S	Medium	GAISSF D1-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0009	D1-CTL-03	13 — Network Monitoring and Defense	P	Medium-High	GAISSF D1-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 13 (Network Monitoring and Defense). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0010	D1-CTL-03	7 — Continuous Vulnerability Management	S	Medium	GAISSF D1-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 7 (Continuous Vulnerability Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies,

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0011	D1-CTL-03	4 — Secure Configuration of Enterprise Assets and Software	S	Medium	GAISSF D1-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 4 (Secure Configuration of Enterprise Assets and Software). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0012	D1-CTL-03	18 — Penetration Testing	S	Medium	GAISSF D1-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0013	D1-CTL-04	16 — Application Software Security	P	Medium	GAISSF D1-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 16 (Application Software Security). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
GAISSF-CRO-033-MAP-0014	D1-CTL-04	10 — Malware Defenses	P	Medium	GAISSF D1-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0015	D1-CTL-04	8 — Audit Log Management	S	Medium	GAISSF D1-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0016	D1-CTL-04	4 — Secure Configuration of Enterprise Assets and Software	S	Medium	GAISSF D1-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 4 (Secure Configuration of Enterprise Assets and Software). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0017	D1-CTL-05	18 — Penetration Testing	S	Medium	GAISSF D1-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					(Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0018	D1-CTL-05	10 — Malware Defenses	S	Medium	GAISSF D1-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0019	D1-CTL-05	7 — Continuous Vulnerability Management	S	Medium	GAISSF D1-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 7 (Continuous Vulnerability Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0020	D1-CTL-05	4 — Secure Configuration of Enterprise Assets and Software	S	Medium	GAISSF D1-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 4 (Secure Configuration of Enterprise Assets and Software). The relationship is outcome-based and does not establish implementation of the underlying CIS

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0021	D1-CTL-06	4 — Secure Configuration of Enterprise Assets and Software	P	Medium-High	GAISSF D1-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 4 (Secure Configuration of Enterprise Assets and Software). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0022	D1-CTL-06	16 — Application Software Security	P	Medium	GAISSF D1-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 16 (Application Software Security). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0023	D1-CTL-06	18 — Penetration Testing	S	Medium	GAISSF D1-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes,

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0024	D1-CTL-06	10 — Malware Defenses	S	Medium	GAISSF D1-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0025	D1-CTL-07	18 — Penetration Testing	S	Medium	GAISSF D1-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0026	D1-CTL-07	13 — Network Monitoring and Defense	S	Medium	GAISSF D1-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 13 (Network Monitoring and Defense). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-	D1-CTL-07	10 — Malware	S	Medium	GAISSF D1-CTL-07

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
MAP-0027		Defenses			provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0028	D1-CTL-07	7 — Continuous Vulnerability Management	S	Medium	GAISSF D1-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 7 (Continuous Vulnerability Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0029	D1-CTL-08	13 — Network Monitoring and Defense	P	Medium	GAISSF D1-CTL-08 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 13 (Network Monitoring and Defense). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0030	D1-CTL-08	18 — Penetration Testing	P	Medium	GAISSF D1-CTL-08 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing).

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0031	D1-CTL-08	16 — Application Software Security	S	Medium	GAISSF D1-CTL-08 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 16 (Application Software Security). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0032	D1-CTL-08	10 — Malware Defenses	S	Medium	GAISSF D1-CTL-08 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0033	D1-CTL-09	7 — Continuous Vulnerability Management	S	Medium	GAISSF D1-CTL-09 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 7 (Continuous Vulnerability Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0034	D1-CTL-09	18 — Penetration Testing	S	Medium	GAISSF D1-CTL-09 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0035	D1-CTL-09	13 — Network Monitoring and Defense	S	Medium	GAISSF D1-CTL-09 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 13 (Network Monitoring and Defense). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0036	D1-CTL-09	10 — Malware Defenses	S	Medium	GAISSF D1-CTL-09 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0037	D2-CTL-01	8 — Audit Log Management	P	Medium	GAISSF D2-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0038	D2-CTL-01	18 — Penetration Testing	P	Medium	GAISSF D2-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0039	D2-CTL-01	10 — Malware Defenses	P	Medium	GAISSF D2-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0040	D2-CTL-01	9 — Email and Web Browser Protections	S	Medium	GAISSF D2-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Control 9 (Email and Web Browser Protections). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0041	D2-CTL-02	8 — Audit Log Management	SP	Medium-High	GAISSF D2-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0042	D2-CTL-02	10 — Malware Defenses	P	Medium	GAISSF D2-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0043	D2-CTL-02	18 — Penetration Testing	P	Medium	GAISSF D2-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0044	D2-CTL-02	4 — Secure Configuration of Enterprise Assets and Software	S	Medium	GAISSF D2-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 4 (Secure Configuration of Enterprise Assets and Software). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0045	D2-CTL-03	18 — Penetration Testing	P	Medium-High	GAISSF D2-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0046	D2-CTL-03	8 — Audit Log Management	P	Medium	GAISSF D2-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope,

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0047	D2-CTL-03	13 — Network Monitoring and Defense	P	Medium	GAISSF D2-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 13 (Network Monitoring and Defense). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0048	D2-CTL-03	10 — Malware Defenses	P	Medium	GAISSF D2-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0049	D2-CTL-04	13 — Network Monitoring and Defense	P	Medium-High	GAISSF D2-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 13 (Network Monitoring and Defense). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0050	D2-CTL-04	10 — Malware Defenses	P	Medium	GAISSF D2-CTL-04 provides an AI-

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0051	D2-CTL-04	9 — Email and Web Browser Protections	S	Medium	GAISSF D2-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 9 (Email and Web Browser Protections). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0052	D2-CTL-04	8 — Audit Log Management	S	Medium	GAISSF D2-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0053	D2-CTL-05	8 — Audit Log Management	P	Medium-High	GAISSF D2-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0054	D2-CTL-05	4 — Secure Configuration of Enterprise Assets and Software	P	Medium	GAISSF D2-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 4 (Secure Configuration of Enterprise Assets and Software). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0055	D2-CTL-05	18 — Penetration Testing	P	Medium	GAISSF D2-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0056	D2-CTL-05	10 — Malware Defenses	P	Medium	GAISSF D2-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards,

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0057	D2-CTL-06	8 — Audit Log Management	P	Medium	GAISSF D2-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0058	D2-CTL-06	18 — Penetration Testing	P	Medium	GAISSF D2-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0059	D2-CTL-06	12 — Network Infrastructure Management	P	Medium	GAISSF D2-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 12 (Network Infrastructure Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
GAISSF-CRO-033-MAP-0060	D2-CTL-06	10 — Malware Defenses	P	Medium	materials. GAISSF D2-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0061	D3-CTL-01	6 — Access Control Management	P	Medium	GAISSF D3-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 6 (Access Control Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0062	D3-CTL-01	5 — Account Management	S	Medium	GAISSF D3-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0063	D3-CTL-01	10 — Malware Defenses	S	Medium	GAISSF D3-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 10 (Malware

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Defenses). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0064	D3-CTL-01	8 — Audit Log Management	S	Medium	GAISSF D3-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0065	D3-CTL-02	18 — Penetration Testing	S	Medium	GAISSF D3-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0066	D3-CTL-02	8 — Audit Log Management	S	Medium	GAISSF D3-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0067	D3-CTL-02	6 — Access Control Management	S	Medium	GAISSF D3-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 6 (Access Control Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0068	D3-CTL-02	5 — Account Management	S	Medium	GAISSF D3-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0069	D3-CTL-03	6 — Access Control Management	S	Medium	GAISSF D3-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 6 (Access Control Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0070	D3-CTL-03	5 — Account Management	S	Medium	GAISSF D3-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0071	D3-CTL-03	18 — Penetration Testing	S	Medium	GAISSF D3-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0072	D3-CTL-03	16 — Application Software Security	S	Medium	GAISSF D3-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 16 (Application Software Security). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0073	D3-CTL-04	16 — Application Software Security	S	Medium	GAISSF D3-CTL-04 provides an AI-security governance, technical or evidentiary capability

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					relevant to CIS Control 16 (Application Software Security). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0074	D3-CTL-04	6 — Access Control Management	S	Medium	GAISSF D3-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 6 (Access Control Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0075	D3-CTL-04	5 — Account Management	S	Medium	GAISSF D3-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0076	D3-CTL-04	18 — Penetration Testing	S	Medium	GAISSF D3-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0077	D3-CTL-05	18 — Penetration Testing	P	Medium	GAISSF D3-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0078	D3-CTL-05	6 — Access Control Management	S	Medium	GAISSF D3-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 6 (Access Control Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0079	D3-CTL-05	5 — Account Management	S	Medium	GAISSF D3-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies,

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0080	D3-CTL-05	16 — Application Software Security	S	Medium	GAISSF D3-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 16 (Application Software Security). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0081	D3-CTL-06	8 — Audit Log Management	P	Medium	GAISSF D3-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0082	D3-CTL-06	6 — Access Control Management	S	Medium	GAISSF D3-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 6 (Access Control Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-	D3-CTL-06	3 — Data Protection	S	Medium	GAISSF D3-CTL-06

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
MAP-0083					provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0084	D3-CTL-06	5 — Account Management	S	Medium	GAISSF D3-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0085	D3-CTL-07	16 — Application Software Security	SP	High	GAISSF D3-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 16 (Application Software Security). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0086	D3-CTL-07	6 — Access Control Management	S	Medium	GAISSF D3-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 6 (Access Control Management). The

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0087	D3-CTL-07	5 — Account Management	S	Medium	GAISSF D3-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0088	D3-CTL-07	4 — Secure Configuration of Enterprise Assets and Software	S	Medium	GAISSF D3-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 4 (Secure Configuration of Enterprise Assets and Software). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0089	D4-CTL-01	2 — Inventory and Control of Software Assets	P	Medium	GAISSF D4-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 2 (Inventory and Control of Software Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0090	D4-CTL-01	15 — Service Provider Management	P	Medium	GAISSF D4-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 15 (Service Provider Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0091	D4-CTL-01	1 — Inventory and Control of Enterprise Assets	S	Medium	GAISSF D4-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 1 (Inventory and Control of Enterprise Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0092	D4-CTL-01	7 — Continuous Vulnerability Management	S	Medium	GAISSF D4-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 7 (Continuous Vulnerability Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies,

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0093	D4-CTL-02	15 — Service Provider Management	P	Medium	GAISSF D4-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 15 (Service Provider Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0094	D4-CTL-02	7 — Continuous Vulnerability Management	S	Medium	GAISSF D4-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 7 (Continuous Vulnerability Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0095	D4-CTL-02	2 — Inventory and Control of Software Assets	S	Medium	GAISSF D4-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 2 (Inventory and Control of Software Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
GAISSF-CRO-033-MAP-0096	D4-CTL-02	16 — Application Software Security	S	Medium	GAISSF D4-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 16 (Application Software Security). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0097	D4-CTL-03	15 — Service Provider Management	P	Medium	GAISSF D4-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 15 (Service Provider Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0098	D4-CTL-03	7 — Continuous Vulnerability Management	S	Medium	GAISSF D4-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 7 (Continuous Vulnerability Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0099	D4-CTL-03	2 — Inventory and Control of Software Assets	S	Medium	GAISSF D4-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Control 2 (Inventory and Control of Software Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0100	D4-CTL-03	16 — Application Software Security	S	Medium	GAISSF D4-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 16 (Application Software Security). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0101	D4-CTL-04	7 — Continuous Vulnerability Management	P	Medium	GAISSF D4-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 7 (Continuous Vulnerability Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0102	D4-CTL-04	15 — Service Provider Management	P	Medium	GAISSF D4-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 15 (Service Provider Management). The relationship is outcome-based and does not establish

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0103	D4-CTL-04	8 — Audit Log Management	S	Medium	GAISSF D4-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0104	D4-CTL-04	2 — Inventory and Control of Software Assets	S	Medium	GAISSF D4-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 2 (Inventory and Control of Software Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0105	D4-CTL-05	15 — Service Provider Management	SP	High	GAISSF D4-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 15 (Service Provider Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0106	D4-CTL-05	7 — Continuous Vulnerability Management	P	Medium-High	GAISSF D4-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 7 (Continuous Vulnerability Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0107	D4-CTL-05	18 — Penetration Testing	P	Medium	GAISSF D4-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0108	D4-CTL-05	16 — Application Software Security	S	Medium	GAISSF D4-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 16 (Application Software Security). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
GAISSF-CRO-033-MAP-0109	D4-CTL-06	1 — Inventory and Control of Enterprise Assets	P	Medium	materials. GAISSF D4-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 1 (Inventory and Control of Enterprise Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0110	D4-CTL-06	15 — Service Provider Management	P	Medium	GAISSF D4-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 15 (Service Provider Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0111	D4-CTL-06	12 — Network Infrastructure Management	P	Medium	GAISSF D4-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 12 (Network Infrastructure Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0112	D4-CTL-06	2 — Inventory and Control of Software Assets	S	Medium	GAISSF D4-CTL-06 provides an AI-security governance, technical or evidentiary capability

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					relevant to CIS Control 2 (Inventory and Control of Software Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0113	D4-CTL-07	2 — Inventory and Control of Software Assets	P	Medium-High	GAISSF D4-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 2 (Inventory and Control of Software Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0114	D4-CTL-07	16 — Application Software Security	P	Medium	GAISSF D4-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 16 (Application Software Security). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0115	D4-CTL-07	7 — Continuous Vulnerability Management	P	Medium	GAISSF D4-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 7 (Continuous Vulnerability Management). The relationship is outcome-based and

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0116	D4-CTL-07	15 — Service Provider Management	P	Medium	GAISSF D4-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 15 (Service Provider Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0117	D5-CTL-01	3 — Data Protection	SP	Medium-High	GAISSF D5-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0118	D5-CTL-01	9 — Email and Web Browser Protections	P	Medium	GAISSF D5-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 9 (Email and Web Browser Protections). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards,

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0119	D5-CTL-02	3 — Data Protection	P	Medium	GAISSF D5-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0120	D5-CTL-02	9 — Email and Web Browser Protections	S	Medium	GAISSF D5-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 9 (Email and Web Browser Protections). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0121	D5-CTL-02	8 — Audit Log Management	S	Medium	GAISSF D5-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
GAISSF-CRO-033-MAP-0122	D5-CTL-03	3 — Data Protection	P	Medium	materials. GAISSF D5-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0123	D5-CTL-03	9 — Email and Web Browser Protections	S	Medium	GAISSF D5-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 9 (Email and Web Browser Protections). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0124	D5-CTL-03	13 — Network Monitoring and Defense	S	Medium	GAISSF D5-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 13 (Network Monitoring and Defense). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0125	D5-CTL-04	3 — Data Protection	P	Medium	GAISSF D5-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0126	D5-CTL-04	9 — Email and Web Browser Protections	S	Medium	GAISSF D5-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 9 (Email and Web Browser Protections). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0127	D5-CTL-05	3 — Data Protection	SP	High	GAISSF D5-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0128	D5-CTL-05	9 — Email and Web Browser Protections	S	Medium	GAISSF D5-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 9 (Email and Web Browser Protections). The relationship is outcome-based and does not establish implementation of the underlying CIS

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0129	D5-CTL-06	3 — Data Protection	SP	High	GAISSF D5-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0130	D5-CTL-06	9 — Email and Web Browser Protections	S	Medium	GAISSF D5-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 9 (Email and Web Browser Protections). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0131	D5-CTL-06	18 — Penetration Testing	S	Medium	GAISSF D5-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope,

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0132	D6-CTL-01	8 — Audit Log Management	P	Medium	GAISSF D6-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0133	D6-CTL-01	14 — Security Awareness and Skills Training	P	Medium	GAISSF D6-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 14 (Security Awareness and Skills Training). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0134	D6-CTL-01	5 — Account Management	S	Medium	GAISSF D6-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0135	D6-CTL-01	3 — Data Protection	S	Medium	GAISSF D6-CTL-01 provides an AI-security governance,

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0136	D6-CTL-02	8 — Audit Log Management	P	Medium-High	GAISSF D6-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0137	D6-CTL-02	3 — Data Protection	P	Medium	GAISSF D6-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0138	D6-CTL-02	5 — Account Management	S	Medium	GAISSF D6-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0139	D6-CTL-02	17 — Incident Response Management	S	Medium	GAISSF D6-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 17 (Incident Response Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0140	D6-CTL-03	3 — Data Protection	P	Medium	GAISSF D6-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0141	D6-CTL-03	6 — Access Control Management	S	Medium	GAISSF D6-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 6 (Access Control Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes,

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0142	D6-CTL-03	5 — Account Management	S	Medium	GAISSF D6-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0143	D6-CTL-03	14 — Security Awareness and Skills Training	S	Medium	GAISSF D6-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 14 (Security Awareness and Skills Training). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0144	D6-CTL-04	17 — Incident Response Management	SP	High	GAISSF D6-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 17 (Incident Response Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
GAISSF-CRO-033-MAP-0145	D6-CTL-04	5 — Account Management	S	Medium	GAISSF D6-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0146	D6-CTL-04	3 — Data Protection	S	Medium	GAISSF D6-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0147	D6-CTL-04	14 — Security Awareness and Skills Training	S	Medium	GAISSF D6-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 14 (Security Awareness and Skills Training). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0148	D6-CTL-05	8 — Audit Log Management	P	Medium	GAISSF D6-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0149	D6-CTL-05	1 — Inventory and Control of Enterprise Assets	P	Medium	GAISSF D6-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 1 (Inventory and Control of Enterprise Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0150	D6-CTL-05	6 — Access Control Management	S	Medium	GAISSF D6-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 6 (Access Control Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0151	D6-CTL-05	5 — Account Management	S	Medium	GAISSF D6-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0152	D6-CTL-06	15 — Service Provider Management	SP	High	GAISSF D6-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 15 (Service Provider Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0153	D6-CTL-06	8 — Audit Log Management	S	Medium	GAISSF D6-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0154	D6-CTL-06	5 — Account Management	S	Medium	GAISSF D6-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0155	D6-CTL-06	3 — Data Protection	S	Medium	GAISSF D6-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0156	D6-CTL-07	11 — Data Recovery	SP	High	GAISSF D6-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 11 (Data Recovery). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0157	D6-CTL-07	5 — Account Management	S	Medium	GAISSF D6-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 5 (Account Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0158	D6-CTL-07	3 — Data Protection	S	Medium	GAISSF D6-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0159	D6-CTL-07	14 — Security Awareness and Skills Training	S	Medium	GAISSF D6-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 14 (Security Awareness and Skills Training). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0160	D7-CTL-H01	14 — Security Awareness and Skills Training	P	Medium	GAISSF D7-CTL-H01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 14 (Security Awareness and Skills Training). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0161	D7-CTL-H01	3 — Data Protection	S	Medium	GAISSF D7-CTL-H01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0162	D7-CTL-H01	9 — Email and Web Browser Protections	S	Medium	GAISSF D7-CTL-H01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 9 (Email and Web Browser Protections). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0163	D7-CTL-H02	14 — Security Awareness and Skills Training	SP	Medium-High	GAISSF D7-CTL-H02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 14 (Security Awareness and Skills Training). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0164	D7-CTL-H02	3 — Data Protection	S	Medium	GAISSF D7-CTL-H02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies,

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0165	D7-CTL-H02	13 — Network Monitoring and Defense	S	Medium	GAISSF D7-CTL-H02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 13 (Network Monitoring and Defense). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0166	D7-CTL-H03	3 — Data Protection	S	Medium	GAISSF D7-CTL-H03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0167	D7-CTL-H03	14 — Security Awareness and Skills Training	S	Medium	GAISSF D7-CTL-H03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 14 (Security Awareness and Skills Training). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-	D7-CTL-H04	3 — Data Protection	S	Medium	GAISSF D7-CTL-H04

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
MAP-0168					provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0169	D7-CTL-H04	14 — Security Awareness and Skills Training	S	Medium	GAISSF D7-CTL-H04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 14 (Security Awareness and Skills Training). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0170	D7-CTL-H04	17 — Incident Response Management	S	Medium	GAISSF D7-CTL-H04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 17 (Incident Response Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0171	D7-CTL-H05	3 — Data Protection	S	Medium	GAISSF D7-CTL-H05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0172	D7-CTL-H05	14 — Security Awareness and Skills Training	S	Medium	GAISSF D7-CTL-H05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 14 (Security Awareness and Skills Training). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0173	D7-CTL-H05	13 — Network Monitoring and Defense	S	Medium	GAISSF D7-CTL-H05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 13 (Network Monitoring and Defense). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0174	D8-CTL-01	3 — Data Protection	S	Medium	GAISSF D8-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0175	D8-CTL-02	8 — Audit Log Management	S	Medium	GAISSF D8-CTL-02 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0176	D8-CTL-03	3 — Data Protection	S	Medium	GAISSF D8-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 3 (Data Protection). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0177	D8-CTL-04	17 — Incident Response Management	S	Medium	GAISSF D8-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 17 (Incident Response Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0178	D8-CTL-05	8 — Audit Log Management	S	Medium	GAISSF D8-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0179	D9-CTL-01	1 — Inventory and Control of Enterprise Assets	S	Medium	GAISSF D9-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 1 (Inventory and Control of Enterprise Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0180	D9-CTL-01	12 — Network Infrastructure Management	S	Medium	GAISSF D9-CTL-01 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 12 (Network Infrastructure Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0181	D9-CTL-02	1 — Inventory and Control of Enterprise Assets	S	Medium	GAISSF D9-CTL-02 provides an AI-security governance, technical or

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					evidentiary capability relevant to CIS Control 1 (Inventory and Control of Enterprise Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0182	D9-CTL-03	1 — Inventory and Control of Enterprise Assets	S	Medium	GAISSF D9-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 1 (Inventory and Control of Enterprise Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0183	D9-CTL-03	14 — Security Awareness and Skills Training	S	Medium	GAISSF D9-CTL-03 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 14 (Security Awareness and Skills Training). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0184	D9-CTL-04	13 — Network Monitoring and Defense	S	Medium	GAISSF D9-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 13 (Network Monitoring and Defense). The relationship is

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0185	D9-CTL-04	18 — Penetration Testing	S	Medium	GAISSF D9-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 18 (Penetration Testing). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0186	D9-CTL-04	1 — Inventory and Control of Enterprise Assets	S	Medium	GAISSF D9-CTL-04 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 1 (Inventory and Control of Enterprise Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0187	D9-CTL-05	8 — Audit Log Management	S	Medium	GAISSF D9-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards,

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0188	D9-CTL-05	1 — Inventory and Control of Enterprise Assets	S	Medium	GAISSF D9-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 1 (Inventory and Control of Enterprise Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0189	D9-CTL-05	7 — Continuous Vulnerability Management	S	Medium	GAISSF D9-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 7 (Continuous Vulnerability Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0190	D9-CTL-05	13 — Network Monitoring and Defense	S	Medium	GAISSF D9-CTL-05 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 13 (Network Monitoring and Defense). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0191	D9-CTL-06	1 — Inventory and Control of Enterprise Assets	S	Medium	GAISSF D9-CTL-06 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 1 (Inventory and Control of Enterprise Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0192	D9-CTL-07	8 — Audit Log Management	S	Medium	GAISSF D9-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 8 (Audit Log Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0193	D9-CTL-07	1 — Inventory and Control of Enterprise Assets	S	Medium	GAISSF D9-CTL-07 provides an AI-security governance, technical or evidentiary capability relevant to CIS Control 1 (Inventory and Control of Enterprise Assets). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.
GAISSF-CRO-033-MAP-0194	D9-CTL-07	17 — Incident Response Management	S	Medium	GAISSF D9-CTL-07 provides an AI-security governance, technical or

Record	GAISSF	CIS Control	Rel.	Confidence	Rationale / Gap
					evidentiary capability relevant to CIS Control 17 (Incident Response Management). The relationship is outcome-based and does not establish implementation of the underlying CIS Safeguards. The organization must validate the applicable CIS v8.1 Safeguards, Implementation Group, asset classes, frequencies, enterprise scope, evidence and operating effectiveness using the official CIS materials.

Annex B — Source Register

Source	Role	Status
GAISSF-NOR-001 v1.0	Framework and conformance baseline	Normative
GAISSF-NOR-004 v1.0	Authoritative control catalogue	Normative
CIS Controls v8.1	Primary external baseline	Current official version
CIS Implementation Groups	IG1 / IG2 / IG3 — official prioritization guidance; IG1 = essential cyber hygiene	Official CIS Implementation Groups guidance
CIS CSAT / SecureSuite	Assessment and tooling	Separate assessment layer

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.

Limitations and Reliance Notice

- Mapping is not CIS Controls Accreditation, CIS SecureSuite status, CIS assessment, evidence sufficiency, or proof of Safeguard implementation or operating effectiveness.
- CIS Controls v8.1 contains 153 Safeguards prioritized through Implementation Groups. This publication maps only at the 18-Control family level and does not reproduce or replace the full Safeguard-level baseline.
- Implementation Group selection is risk- and resource-dependent and must be determined by the implementing enterprise.
- CIS Benchmarks, CIS RAM, CIS CSAT, the CIS Controls Assessment Specification, CIS SecureSuite and CIS Controls Accreditation are separate resources or programmes and are not substituted by this crosswalk.
- Similar terminology does not establish equivalence. CIS enterprise-cybersecurity outcomes and GAISSF AI-system controls differ in scope, abstraction, evidence expectations and applicability.
- A new CIS Controls edition or material GAISSF baseline change triggers revalidation of this crosswalk.

© 2026 ODA3 Pvt Ltd. Published by ODA3 Institute. CIS, CIS Controls, CIS Safeguards, CIS Benchmarks and related marks and materials remain the property of Center for Internet Security, Inc. No endorsement or affiliation is implied.