

ODA3 INSTITUTE

CROSSWALK

GAISSF™-PCI DSS Mapping

Payment Card Industry Data Security Standard Alignment Crosswalk

GAISSF-CRO-032 | Informative crosswalk | Draft for Publication

Version 1.0 | Updated 7 October 2026

© 2026 ODA3 Pvt Ltd

Field	Controlled Value
Document ID	GAISSTF-CRO-032
Publisher	ODA3 Institute
Legal entity	ODA3 Pvt Ltd
GAISSTF™ baseline	59 controls across nine domains
External baseline	PCI DSS v4.0.1
Mapping unit	12 principal requirement families
Verification date	29 June 2026
Distribution	Website / GitHub

1. Executive Summary

This crosswalk contains 187 outcome-based records covering all 59 GAISSTF™ controls and all 12 PCI DSS requirement families. It supports payment-security control rationalization, gap analysis and evidence planning. It does not establish PCI DSS compliance or validation.

2. PCI DSS Assurance Architecture

PCI DSS applies to entities that store, process or transmit account data and to systems connected to or affecting the security of the cardholder data environment. Validation may involve a Report on Compliance, Self-Assessment Questionnaire, Attestation of Compliance, Qualified Security Assessor or Internal Security Assessor activities, acquirer instructions and payment-brand requirements. These assurance and acceptance layers are separate from this mapping.

3. Scope and Method

The mapping uses the 12 principal requirements as the controlled publication layer. The official subrequirements, applicability notes, testing procedures, defined and customized approaches, targeted risk analyses, compensating-control requirements and appendices remain authoritative. Mappings compare control outcomes, implementation capability and evidence potential.

4. High-Alignment Areas

- Secure configuration, network protection and system hardening

- Cryptography, data protection and controlled retention
- Malware, vulnerability and secure-development controls
- Identity, authentication and least-privilege access
- Logging, monitoring, testing and incident response
- Governance, supplier management, awareness and policy

5. Material Residual Work

- Cardholder data environment and connected-to scope validation
- Account-data discovery and data-flow documentation
- PCI-specific subrequirement and testing-procedure evidence
- Payment-page script and change/tamper controls where applicable
- Targeted risk analyses and customized-approach documentation
- Compensating-control worksheets and business constraints
- ROC, SAQ, AOC and assessor or acquirer acceptance

6. Notably Absent

NOTABLY ABSENT

No basis was found to claim PCI DSS certification, automatic scope reduction, QSA approval, payment-brand acceptance, satisfaction of every subrequirement, operating effectiveness, or PCI SSC endorsement.

7. Requirement Coverage Register

Req.	Requirement family	Goal	Mapped controls	Coverage
1	Install and maintain network security controls	Build and Maintain a Secure Network and Systems	3	Partially Addressed
2	Apply secure configurations to all system components	Build and Maintain a Secure Network and Systems	7	Partially Addressed
3	Protect stored account data	Protect Account Data	21	Substantially Addressed
4	Protect cardholder data with strong cryptography during transmission over	Protect Account Data	8	Substantially Addressed

	open, public networks			
5	Protect all systems and networks from malicious software	Maintain a Vulnerability Management Program	23	Substantially Addressed
6	Develop and maintain secure systems and software	Maintain a Vulnerability Management Program	21	Substantially Addressed
7	Restrict access to system components and cardholder data by business need to know	Implement Strong Access Control Measures	10	Substantially Addressed
8	Identify users and authenticate access to system components	Implement Strong Access Control Measures	17	Substantially Addressed
9	Restrict physical access to cardholder data	Implement Strong Access Control Measures	8	Substantially Addressed
10	Log and monitor all access to system components and cardholder data	Regularly Monitor and Test Networks	28	Substantially Addressed
11	Test security of systems and networks regularly	Regularly Monitor and Test Networks	22	Substantially Addressed
12	Support information security with organizational policies and programs	Maintain an Information Security Policy	19	Substantially Addressed

Annex A — Complete Mapping Register

Record	GAISSTF™	PCI DSS	Rel.	Confidence	Rationale / Gap
CRO032-MAP-0001	D1-CTL-01	Req. 5 — Protect all systems and	SP	Medium-High	GAISSTF D1-CTL-01 provides

		networks from malicious software			governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0002	D1-CTL-01	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium	GAISSTF D1-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0003	D1-CTL-01	Req. 3 — Protect stored account data	S	Medium	GAISSTF D1-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a

					cardholder data environment.
CRO032-MAP-0004	D1-CTL-01	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSTF D1-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0005	D1-CTL-02	Req. 5 — Protect all systems and networks from malicious software	P	Medium	GAISSTF D1-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0006	D1-CTL-02	Req. 11 — Test security of systems and networks regularly	S	Medium	GAISSTF D1-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The

					relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0007	D1-CTL-02	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSTF D1-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0008	D1-CTL-02	Req. 2 — Apply secure configurations to all system components	S	Medium	GAISSTF D1-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 2 (Apply secure configurations to all system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environm...
CRO032-MAP-0009	D1-CTL-03	Req. 5 — Protect all systems and networks from malicious software	P	Medium-High	GAISSTF D1-CTL-03 provides governance, technical, or evidentiary

					capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0010	D1-CTL-03	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium	GAISSTF D1-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0011	D1-CTL-03	Req. 2 — Apply secure configurations to all system components	S	Medium	GAISSTF D1-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 2 (Apply secure configurations to all system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data

					environm...
CRO032-MAP-0012	D1-CTL-03	Req. 11 — Test security of systems and networks regularly	S	Medium	GAISSF D1-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0013	D1-CTL-04	Req. 5 — Protect all systems and networks from malicious software	SP	High	GAISSF D1-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0014	D1-CTL-04	Req. 6 — Develop and maintain secure systems and software	P	Medium	GAISSF D1-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is

					outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0015	D1-CTL-04	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium	GAISSTF D1-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0016	D1-CTL-04	Req. 2 — Apply secure configurations to all system components	S	Medium	GAISSTF D1-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 2 (Apply secure configurations to all system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environm...
CRO032-MAP-0017	D1-CTL-05	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSTF D1-CTL-05 provides governance, technical, or evidentiary capability relevant

					to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0018	D1-CTL-05	Req. 5 — Protect all systems and networks from malicious software	S	Medium	GAISSTF D1-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0019	D1-CTL-05	Req. 2 — Apply secure configurations to all system components	S	Medium	GAISSTF D1-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 2 (Apply secure configurations to all system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data

					environm...
CRO032-MAP-0020	D1-CTL-05	Req. 11 — Test security of systems and networks regularly	S	Medium	GAISSF D1-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0021	D1-CTL-06	Req. 6 — Develop and maintain secure systems and software	P	Medium-High	GAISSF D1-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0022	D1-CTL-06	Req. 2 — Apply secure configurations to all system components	P	Medium	GAISSF D1-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 2 (Apply secure configurations to all system components). The relationship is outcome-based

					and does not establish applicability, assessment status, or compliance for a cardholder data environm...
CRO032-MAP-0023	D1-CTL-06	Req. 5 — Protect all systems and networks from malicious software	S	Medium	GAISSF D1-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0024	D1-CTL-06	Req. 11 — Test security of systems and networks regularly	S	Medium	GAISSF D1-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0025	D1-CTL-07	Req. 5 — Protect all systems and networks from malicious software	P	Medium	GAISSF D1-CTL-07 provides governance, technical, or evidentiary capability relevant

					to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0026	D1-CTL-07	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSF D1-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0027	D1-CTL-07	Req. 2 — Apply secure configurations to all system components	S	Medium	GAISSF D1-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 2 (Apply secure configurations to all system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data

					environm...
CRO032-MAP-0028	D1-CTL-07	Req. 11 — Test security of systems and networks regularly	S	Medium	GAISSF D1-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0029	D1-CTL-08	Req. 5 — Protect all systems and networks from malicious software	P	Medium-High	GAISSF D1-CTL-08 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0030	D1-CTL-08	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium	GAISSF D1-CTL-08 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data).

					The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0031	D1-CTL-08	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSF D1-CTL-08 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0032	D1-CTL-08	Req. 11 — Test security of systems and networks regularly	S	Medium	GAISSF D1-CTL-08 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0033	D1-CTL-09	Req. 5 — Protect all systems and networks from malicious software	S	Medium	GAISSF D1-CTL-09 provides governance, technical, or evidentiary capability relevant

					to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0034	D1-CTL-09	Req. 11 — Test security of systems and networks regularly	S	Medium	GAISSF D1-CTL-09 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0035	D1-CTL-09	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSF D1-CTL-09 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data

					environment.
CRO032-MAP-0036	D1-CTL-09	Req. 2 — Apply secure configurations to all system components	S	Medium	GAISSF D1-CTL-09 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 2 (Apply secure configurations to all system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environm...
CRO032-MAP-0037	D2-CTL-01	Req. 5 — Protect all systems and networks from malicious software	SP	Medium-High	GAISSF D2-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0038	D2-CTL-01	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium	GAISSF D2-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data).

					The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0039	D2-CTL-01	Req. 11 — Test security of systems and networks regularly	P	Medium	GAISSTF D2-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0040	D2-CTL-01	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSTF D2-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0041	D2-CTL-02	Req. 5 — Protect all systems and networks from malicious software	SP	High	GAISSTF D2-CTL-02 provides governance, technical, or evidentiary capability relevant

					to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0042	D2-CTL-02	Req. 10 — Log and monitor all access to system components and cardholder data	SP	Medium-High	GAISSTF D2-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0043	D2-CTL-02	Req. 11 — Test security of systems and networks regularly	P	Medium	GAISSTF D2-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data

					environment.
CRO032-MAP-0044	D2-CTL-02	Req. 4 — Protect cardholder data with strong cryptography during transmission over open, public networks	S	Medium	GAISSTF D2-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 4 (Protect cardholder data with strong cryptography during transmission over open, public networks). The relationship is outcome-based and does not establish applicability, assessment status, o...
CRO032-MAP-0045	D2-CTL-03	Req. 11 — Test security of systems and networks regularly	SP	Medium-High	GAISSTF D2-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0046	D2-CTL-03	Req. 5 — Protect all systems and networks from malicious software	P	Medium	GAISSTF D2-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is

					outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0047	D2-CTL-03	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium	GAISSF D2-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0048	D2-CTL-03	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSF D2-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0049	D2-CTL-04	Req. 5 — Protect all systems and networks from malicious software	P	Medium	GAISSF D2-CTL-04 provides governance, technical, or evidentiary capability relevant

					to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0050	D2-CTL-04	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium	GAISSTF D2-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0051	D2-CTL-04	Req. 4 — Protect cardholder data with strong cryptography during transmission over open, public networks	S	Medium	GAISSTF D2-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 4 (Protect cardholder data with strong cryptography during transmission over open, public networks). The relationship is outcome-based and does not establish applicability, assessment

					status, o...
CRO032-MAP-0052	D2-CTL-04	Req. 11 — Test security of systems and networks regularly	S	Medium	GAISSTF D2-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0053	D2-CTL-05	Req. 5 — Protect all systems and networks from malicious software	SP	Medium-High	GAISSTF D2-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0054	D2-CTL-05	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium-High	GAISSTF D2-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data).

					The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0055	D2-CTL-05	Req. 11 — Test security of systems and networks regularly	P	Medium	GAISSF D2-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0056	D2-CTL-05	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSF D2-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0057	D2-CTL-06	Req. 5 — Protect all systems and networks from malicious software	P	Medium	GAISSF D2-CTL-06 provides governance, technical, or evidentiary capability relevant

					to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0058	D2-CTL-06	Req. 11 — Test security of systems and networks regularly	P	Medium	GAISSF D2-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0059	D2-CTL-06	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium	GAISSF D2-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a

					cardhold...
CRO032-MAP-0060	D2-CTL-06	Req. 1 — Install and maintain network security controls	P	Medium	GAISSTF D2-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 1 (Install and maintain network security controls). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0061	D3-CTL-01	Req. 7 — Restrict access to system components and cardholder data by business need to know	P	Medium	GAISSTF D3-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 7 (Restrict access to system components and cardholder data by business need to know). The relationship is outcome-based and does not establish applicability, assessment status, or compliance f...
CRO032-MAP-0062	D3-CTL-01	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSTF D3-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not

					establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0063	D3-CTL-01	Req. 10 — Log and monitor all access to system components and cardholder data	S	Medium	GAISSTF D3-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0064	D3-CTL-01	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSTF D3-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0065	D3-CTL-02	Req. 11 — Test security of systems and networks regularly	S	Medium	GAISSTF D3-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11

					(Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0066	D3-CTL-02	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSTF D3-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0067	D3-CTL-02	Req. 7 — Restrict access to system components and cardholder data by business need to know	S	Medium	GAISSTF D3-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 7 (Restrict access to system components and cardholder data by business need to know). The relationship is outcome-based and does not establish applicability, assessment status, or compliance f...
CRO032-MAP-	D3-CTL-02	Req. 6 — Develop	S	Medium	GAISSTF D3-CTL-

0068		and maintain secure systems and software			02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0069	D3-CTL-03	Req. 5 — Protect all systems and networks from malicious software	P	Medium	GAISSTF D3-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0070	D3-CTL-03	Req. 10 — Log and monitor all access to system components and cardholder data	S	Medium	GAISSTF D3-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish

					applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0071	D3-CTL-03	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSTF D3-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0072	D3-CTL-03	Req. 7 — Restrict access to system components and cardholder data by business need to know	S	Medium	GAISSTF D3-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 7 (Restrict access to system components and cardholder data by business need to know). The relationship is outcome-based and does not establish applicability, assessment status, or compliance f...
CRO032-MAP-0073	D3-CTL-04	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSTF D3-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure

					systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0074	D3-CTL-04	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSTF D3-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0075	D3-CTL-04	Req. 7 — Restrict access to system components and cardholder data by business need to know	S	Medium	GAISSTF D3-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 7 (Restrict access to system components and cardholder data by business need to know). The relationship is outcome-based and does not establish applicability, assessment status, or compliance f...
CRO032-MAP-0076	D3-CTL-04	Req. 5 — Protect all systems and networks from	S	Medium	GAISSTF D3-CTL-04 provides governance,

		malicious software			technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0077	D3-CTL-05	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSTF D3-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0078	D3-CTL-05	Req. 7 — Restrict access to system components and cardholder data by business need to know	S	Medium	GAISSTF D3-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 7 (Restrict access to system components and cardholder data by business need to know). The relationship is outcome-based and does not establish applicability,

					assessment status, or compliance f...
CRO032-MAP-0079	D3-CTL-05	Req. 11 — Test security of systems and networks regularly	S	Medium	GAISSTF D3-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0080	D3-CTL-05	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSTF D3-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0081	D3-CTL-06	Req. 5 — Protect all systems and networks from malicious software	P	Medium	GAISSTF D3-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious

					software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0082	D3-CTL-06	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium	GAISSTF D3-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0083	D3-CTL-06	Req. 8 — Identify users and authenticate access to system components	P	Medium	GAISSTF D3-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0084	D3-CTL-06	Req. 7 — Restrict access to system components and cardholder data by	S	Medium	GAISSTF D3-CTL-06 provides governance, technical, or

		business need to know			evidentiary capability relevant to PCI DSS Requirement 7 (Restrict access to system components and cardholder data by business need to know). The relationship is outcome-based and does not establish applicability, assessment status, or compliance f...
CRO032-MAP-0085	D3-CTL-07	Req. 6 — Develop and maintain secure systems and software	P	Medium	GAISSF D3-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0086	D3-CTL-07	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSF D3-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data

					e...
CRO032-MAP-0087	D3-CTL-07	Req. 7 — Restrict access to system components and cardholder data by business need to know	S	Medium	GAISSTF D3-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 7 (Restrict access to system components and cardholder data by business need to know). The relationship is outcome-based and does not establish applicability, assessment status, or compliance f...
CRO032-MAP-0088	D3-CTL-07	Req. 5 — Protect all systems and networks from malicious software	S	Medium	GAISSTF D3-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0089	D4-CTL-01	Req. 3 — Protect stored account data	P	Medium	GAISSTF D4-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not

					establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0090	D4-CTL-01	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSF D4-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0091	D4-CTL-01	Req. 4 — Protect cardholder data with strong cryptography during transmission over open, public networks	S	Medium	GAISSF D4-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 4 (Protect cardholder data with strong cryptography during transmission over open, public networks). The relationship is outcome-based and does not establish applicability, assessment status, o...
CRO032-MAP-0092	D4-CTL-01	Req. 12 — Support information security with organizational policies and programs	S	Medium	GAISSF D4-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12

					(Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardh...
CRO032-MAP-0093	D4-CTL-02	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSTF D4-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0094	D4-CTL-02	Req. 3 — Protect stored account data	S	Medium	GAISSTF D4-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0095	D4-CTL-02	Req. 4 — Protect cardholder data	S	Medium	GAISSTF D4-CTL-02 provides

		with strong cryptography during transmission over open, public networks			governance, technical, or evidentiary capability relevant to PCI DSS Requirement 4 (Protect cardholder data with strong cryptography during transmission over open, public networks). The relationship is outcome-based and does not establish applicability, assessment status, o...
CRO032-MAP-0096	D4-CTL-02	Req. 12 — Support information security with organizational policies and programs	S	Medium	GAISSTF D4-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardh...
CRO032-MAP-0097	D4-CTL-03	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSTF D4-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment

					status, or compliance for a cardholder data environment.
CRO032-MAP-0098	D4-CTL-03	Req. 3 — Protect stored account data	S	Medium	GAISSF D4-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0099	D4-CTL-03	Req. 4 — Protect cardholder data with strong cryptography during transmission over open, public networks	S	Medium	GAISSF D4-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 4 (Protect cardholder data with strong cryptography during transmission over open, public networks). The relationship is outcome-based and does not establish applicability, assessment status, o...
CRO032-MAP-0100	D4-CTL-03	Req. 12 — Support information security with organizational policies and programs	S	Medium	GAISSF D4-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and

					programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardh...
CRO032-MAP-0101	D4-CTL-04	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium	GAISSF D4-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0102	D4-CTL-04	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSF D4-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0103	D4-CTL-04	Req. 3 — Protect stored account data	S	Medium	GAISSF D4-CTL-04 provides governance, technical, or evidentiary

					capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0104	D4-CTL-04	Req. 11 — Test security of systems and networks regularly	S	Medium	GAISSTF D4-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0105	D4-CTL-05	Req. 11 — Test security of systems and networks regularly	SP	Medium-High	GAISSTF D4-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.

CRO032-MAP-0106	D4-CTL-05	Req. 3 — Protect stored account data	P	Medium	GAISSTF D4-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0107	D4-CTL-05	Req. 6 — Develop and maintain secure systems and software	P	Medium	GAISSTF D4-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0108	D4-CTL-05	Req. 4 — Protect cardholder data with strong cryptography during transmission over open, public networks	S	Medium	GAISSTF D4-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 4 (Protect cardholder data with strong cryptography during transmission over open, public networks). The relationship is outcome-based and does not establish

					applicability, assessment status, o...
CRO032-MAP-0109	D4-CTL-06	Req. 12 — Support information security with organizational policies and programs	SP	Medium-High	GAISSTF D4-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardh...
CRO032-MAP-0110	D4-CTL-06	Req. 1 — Install and maintain network security controls	P	Medium	GAISSTF D4-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 1 (Install and maintain network security controls). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0111	D4-CTL-06	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSTF D4-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The

					relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0112	D4-CTL-06	Req. 4 — Protect cardholder data with strong cryptography during transmission over open, public networks	S	Medium	GAISSTF D4-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 4 (Protect cardholder data with strong cryptography during transmission over open, public networks). The relationship is outcome-based and does not establish applicability, assessment status, o...
CRO032-MAP-0113	D4-CTL-07	Req. 6 — Develop and maintain secure systems and software	SP	Medium-High	GAISSTF D4-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0114	D4-CTL-07	Req. 3 — Protect stored account data	S	Medium	GAISSTF D4-CTL-07 provides governance, technical, or evidentiary

					capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0115	D4-CTL-07	Req. 4 — Protect cardholder data with strong cryptography during transmission over open, public networks	S	Medium	GAISSTF D4-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 4 (Protect cardholder data with strong cryptography during transmission over open, public networks). The relationship is outcome-based and does not establish applicability, assessment status, o...
CRO032-MAP-0116	D4-CTL-07	Req. 12 — Support information security with organizational policies and programs	S	Medium	GAISSTF D4-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardh...

CRO032-MAP-0117	D5-CTL-01	Req. 3 — Protect stored account data	S	Medium	GAISSF D5-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0118	D5-CTL-01	Req. 10 — Log and monitor all access to system components and cardholder data	S	Medium	GAISSF D5-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0119	D5-CTL-02	Req. 10 — Log and monitor all access to system components and cardholder data	SP	High	GAISSF D5-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment

					status, or compliance for a cardhold...
CRO032-MAP-0120	D5-CTL-02	Req. 5 — Protect all systems and networks from malicious software	S	Medium	GAISSF D5-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0121	D5-CTL-02	Req. 3 — Protect stored account data	S	Medium	GAISSF D5-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0122	D5-CTL-03	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium-High	GAISSF D5-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data).

					The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0123	D5-CTL-03	Req. 3 — Protect stored account data	S	Medium	GAISSTF D5-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0124	D5-CTL-03	Req. 5 — Protect all systems and networks from malicious software	S	Medium	GAISSTF D5-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0125	D5-CTL-04	Req. 3 — Protect stored account data	S	Medium	GAISSTF D5-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS

					Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0126	D5-CTL-04	Req. 10 — Log and monitor all access to system components and cardholder data	S	Medium	GAISSTF D5-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0127	D5-CTL-05	Req. 3 — Protect stored account data	SP	Medium-High	GAISSTF D5-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0128	D5-CTL-05	Req. 10 — Log and monitor all access to system components and	P	Medium	GAISSTF D5-CTL-05 provides governance, technical, or

		cardholder data			evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0129	D5-CTL-06	Req. 3 — Protect stored account data	SP	Medium-High	GAISSF D5-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0130	D5-CTL-06	Req. 11 — Test security of systems and networks regularly	S	Medium	GAISSF D5-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.

CRO032-MAP-0131	D5-CTL-06	Req. 10 — Log and monitor all access to system components and cardholder data	S	Medium	GAISSF D5-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0132	D6-CTL-01	Req. 12 — Support information security with organizational policies and programs	SP	Medium-High	GAISSF D6-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardh...
CRO032-MAP-0133	D6-CTL-01	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium	GAISSF D6-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not

					establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0134	D6-CTL-01	Req. 3 — Protect stored account data	S	Medium	GAISSTF D6-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0135	D6-CTL-01	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSTF D6-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0136	D6-CTL-02	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium-High	GAISSTF D6-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system

					components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0137	D6-CTL-02	Req. 12 — Support information security with organizational policies and programs	P	Medium	GAISSF D6-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardh...
CRO032-MAP-0138	D6-CTL-02	Req. 3 — Protect stored account data	S	Medium	GAISSF D6-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0139	D6-CTL-02	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSF D6-CTL-02 provides governance, technical, or evidentiary

					capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0140	D6-CTL-03	Req. 3 — Protect stored account data	P	Medium	GAISSTF D6-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0141	D6-CTL-03	Req. 12 — Support information security with organizational policies and programs	P	Medium	GAISSTF D6-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardh...

CRO032-MAP-0142	D6-CTL-03	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSTF D6-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0143	D6-CTL-03	Req. 7 — Restrict access to system components and cardholder data by business need to know	S	Medium	GAISSTF D6-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 7 (Restrict access to system components and cardholder data by business need to know). The relationship is outcome-based and does not establish applicability, assessment status, or compliance f...
CRO032-MAP-0144	D6-CTL-04	Req. 12 — Support information security with organizational policies and programs	P	Medium-High	GAISSTF D6-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not

					establish applicability, assessment status, or compliance for a cardh...
CRO032-MAP-0145	D6-CTL-04	Req. 3 — Protect stored account data	S	Medium	GAISSTF D6-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0146	D6-CTL-04	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSTF D6-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0147	D6-CTL-04	Req. 7 — Restrict access to system components and cardholder data by business need to know	S	Medium	GAISSTF D6-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 7 (Restrict access to system components and

					cardholder data by business need to know). The relationship is outcome-based and does not establish applicability, assessment status, or compliance f...
CRO032-MAP-0148	D6-CTL-05	Req. 10 — Log and monitor all access to system components and cardholder data	P	Medium-High	GAISSF D6-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0149	D6-CTL-05	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSF D6-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0150	D6-CTL-05	Req. 7 — Restrict access to system components and cardholder data by	S	Medium	GAISSF D6-CTL-05 provides governance, technical, or

		business need to know			evidentiary capability relevant to PCI DSS Requirement 7 (Restrict access to system components and cardholder data by business need to know). The relationship is outcome-based and does not establish applicability, assessment status, or compliance f...
CRO032-MAP-0151	D6-CTL-05	Req. 3 — Protect stored account data	S	Medium	GAISSF D6-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0152	D6-CTL-06	Req. 12 — Support information security with organizational policies and programs	P	Medium-High	GAISSF D6-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a

					cardh...
CRO032-MAP-0153	D6-CTL-06	Req. 11 — Test security of systems and networks regularly	P	Medium	GAISSF D6-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0154	D6-CTL-06	Req. 3 — Protect stored account data	S	Medium	GAISSF D6-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0155	D6-CTL-06	Req. 10 — Log and monitor all access to system components and cardholder data	S	Medium	GAISSF D6-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not

					establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0156	D6-CTL-07	Req. 3 — Protect stored account data	S	Medium	GAISSTF D6-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0157	D6-CTL-07	Req. 12 — Support information security with organizational policies and programs	S	Medium	GAISSTF D6-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardh...
CRO032-MAP-0158	D6-CTL-07	Req. 11 — Test security of systems and networks regularly	S	Medium	GAISSTF D6-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and

					networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0159	D6-CTL-07	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSTF D6-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data e...
CRO032-MAP-0160	D7-CTL-H01	Req. 12 — Support information security with organizational policies and programs	P	Medium	GAISSTF D7-CTL-H01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a card...
CRO032-MAP-0161	D7-CTL-H02	Req. 12 — Support	P	Medium-High	GAISSTF D7-CTL-H02 provides

		information security with organizational policies and programs			governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a card...
CRO032-MAP-0162	D7-CTL-H02	Req. 10 — Log and monitor all access to system components and cardholder data	S	Medium	GAISSTF D7-CTL-H02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhol...
CRO032-MAP-0163	D7-CTL-H02	Req. 5 — Protect all systems and networks from malicious software	S	Medium	GAISSTF D7-CTL-H02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability,

					assessment status, or compliance for a cardholder data env...
CRO032-MAP-0164	D7-CTL-H03	Req. 12 — Support information security with organizational policies and programs	S	Medium	GAISSTF D7-CTL-H03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a card...
CRO032-MAP-0165	D7-CTL-H03	Req. 8 — Identify users and authenticate access to system components	S	Medium	GAISSTF D7-CTL-H03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 8 (Identify users and authenticate access to system components). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data ...
CRO032-MAP-0166	D7-CTL-H04	Req. 12 — Support information security with organizational policies and programs	S	Medium	GAISSTF D7-CTL-H04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information

					security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a card...
CRO032-MAP-0167	D7-CTL-H05	Req. 12 — Support information security with organizational policies and programs	S	Medium	GAISST D7-CTL-H05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a card...
CRO032-MAP-0168	D8-CTL-01	Req. 12 — Support information security with organizational policies and programs	S	Medium	GAISST D8-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardh...

CRO032-MAP-0169	D8-CTL-02	Req. 9 — Restrict physical access to cardholder data	S	Medium	GAISSF D8-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 9 (Restrict physical access to cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0170	D8-CTL-03	Req. 3 — Protect stored account data	S	Medium	GAISSF D8-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 3 (Protect stored account data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0171	D8-CTL-04	Req. 12 — Support information security with organizational policies and programs	S	Medium	GAISSF D8-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment

					status, or compliance for a cardh...
CRO032-MAP-0172	D8-CTL-05	Req. 6 — Develop and maintain secure systems and software	S	Medium	GAISSTF D8-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 6 (Develop and maintain secure systems and software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0173	D9-CTL-01	Req. 9 — Restrict physical access to cardholder data	P	Medium	GAISSTF D9-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 9 (Restrict physical access to cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0174	D9-CTL-01	Req. 1 — Install and maintain network security controls	S	Medium	GAISSTF D9-CTL-01 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 1 (Install and maintain network security controls). The relationship is outcome-based

					and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0175	D9-CTL-02	Req. 9 — Restrict physical access to cardholder data	P	Medium	GAISSTF D9-CTL-02 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 9 (Restrict physical access to cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0176	D9-CTL-03	Req. 9 — Restrict physical access to cardholder data	P	Medium	GAISSTF D9-CTL-03 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 9 (Restrict physical access to cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0177	D9-CTL-04	Req. 9 — Restrict physical access to cardholder data	P	Medium-High	GAISSTF D9-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 9 (Restrict physical

					access to cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0178	D9-CTL-04	Req. 5 — Protect all systems and networks from malicious software	S	Medium	GAISSTF D9-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 5 (Protect all systems and networks from malicious software). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data envi...
CRO032-MAP-0179	D9-CTL-04	Req. 10 — Log and monitor all access to system components and cardholder data	S	Medium	GAISSTF D9-CTL-04 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0180	D9-CTL-04	Req. 11 — Test security of systems	S	Medium	GAISSTF D9-CTL-04 provides

		and networks regularly			governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0181	D9-CTL-05	Req. 9 — Restrict physical access to cardholder data	P	Medium	GAISSTF D9-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 9 (Restrict physical access to cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0182	D9-CTL-05	Req. 11 — Test security of systems and networks regularly	P	Medium	GAISSTF D9-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 11 (Test security of systems and networks regularly). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a

					cardholder data environment.
CRO032-MAP-0183	D9-CTL-05	Req. 10 — Log and monitor all access to system components and cardholder data	S	Medium	GAISSF D9-CTL-05 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...
CRO032-MAP-0184	D9-CTL-06	Req. 9 — Restrict physical access to cardholder data	S	Medium	GAISSF D9-CTL-06 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 9 (Restrict physical access to cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0185	D9-CTL-07	Req. 9 — Restrict physical access to cardholder data	SP	Medium-High	GAISSF D9-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 9 (Restrict physical access to cardholder data). The relationship is outcome-based and does not

					establish applicability, assessment status, or compliance for a cardholder data environment.
CRO032-MAP-0186	D9-CTL-07	Req. 12 — Support information security with organizational policies and programs	S	Medium	GAISST D9-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 12 (Support information security with organizational policies and programs). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardh...
CRO032-MAP-0187	D9-CTL-07	Req. 10 — Log and monitor all access to system components and cardholder data	S	Medium	GAISST D9-CTL-07 provides governance, technical, or evidentiary capability relevant to PCI DSS Requirement 10 (Log and monitor all access to system components and cardholder data). The relationship is outcome-based and does not establish applicability, assessment status, or compliance for a cardhold...

Annex B — Source Register

Source	Role	Status
--------	------	--------

GAISST-NOR-001 v1.0	Framework and conformance baseline	Normative
GAISST-NOR-004 v1.0	Authoritative 59-control catalogue	Normative
PCI DSS v4.0.1	Primary payment-security standard	Current baseline

Limitations and Reliance Notice

- Mapping is not PCI DSS compliance, validation, certification, a ROC, SAQ, AOC, QSA opinion, or payment-brand acceptance.
- PCI DSS applicability and scope depend on storage, processing or transmission of account data and on systems connected to or affecting the security of the cardholder data environment.
- The official PCI DSS v4.0.1 requirements, testing procedures, applicability notes, defined approach, customized approach, targeted risk analyses and appendices remain controlling.
- Future-dated requirements are treated as active because their effective date of 31 March 2025 has passed.
- Compensating controls and customized approaches require PCI-specific documentation and assessment; GAISSTM mapping does not approve them.
- PCI SSC materials are proprietary; this publication uses requirement numbers and concise functional summaries, not a reproduction of the standard.

© 2026 ODA3 Pvt Ltd. Published by ODA3 Institute. PCI SSC, PCI DSS, payment-brand names and related materials remain the property of their respective owners. No endorsement, affiliation or validation conclusion is implied.