TPSA

THIRD-PARTY SUPPLIER ACCOUNTABILITY

T P S A - 0 3

Regulatory Mapping Matrix

Third-Party Supplier Accountability Framework

CIS Controls v8.1.2 • ISO 27001:2022 • DORA • NIS2

Version 1.0 April 2026

Author: Sébastien Poitrasson, Arthur Koenig Consulting

AK ARTHURKOENIG

1. Introduction

1.1 Purpose

This document defines the **TPSA-03: Regulatory Mapping Matrix**, the third component of the Third-Party Supplier Accountability framework. It provides a systematic, field-by-field mapping of every TPSA requirement to the corresponding controls or articles in four reference frameworks: CIS Controls v8.1.2, ISO/IEC 27001:2022, DORA (Regulation 2022/2554), and the NIS2 Directive (2022/2555).

The Regulatory Mapping Matrix serves two primary purposes:

- **For clients**: it provides auditable traceability from TPSA compliance to regulatory obligations. When an auditor asks “how do you meet DORA Article 28 on third-party risk management?”, the client can point to specific TPSA Disclosure Card fields and Risk Dialogue Protocol exchanges, each mapped to the relevant DORA article.
- **For suppliers**: it demonstrates that TPSA certification covers the third-party transparency requirements of multiple regulatory frameworks simultaneously, reducing the burden of responding to framework-specific questionnaires and assessments.

1.2 Scope

The mapping covers all mandatory and conditional fields defined in TPSA-01 (Supplier Disclosure Standard) and all exchange types defined in TPSA-02 (Risk Dialogue Protocol). Optional fields are included where they map to regulatory requirements.

The mapping identifies the **most directly relevant** control or article in each framework. Where a TPSA requirement maps to multiple controls/articles, the primary mapping is listed first, with supporting mappings in parentheses.

1.3 Mapping Methodology

Each mapping entry identifies the relationship between the TPSA requirement and the target framework element:

- **Direct mapping**: the TPSA requirement substantially addresses the same concern as the target control/article. Implementing the TPSA requirement provides evidence of compliance with the target.
- **Partial mapping**: the TPSA requirement addresses part of the target control/article, or the target requires additional measures beyond what TPSA specifies. Noted with “(partial)”.
- **Supporting mapping**: the TPSA requirement contributes to but does not directly satisfy the target. Noted with “(supports)”.

A dash (“—”) indicates no applicable mapping in that framework.

1.4 Framework Versions

- **CIS Controls v8** (June 2021) — Safeguards referenced by number (e.g., 15.1).
- **ISO/IEC 27001:2022** — Annex A controls referenced by number (e.g., A.5.19). Clause references for ISMS requirements (e.g., 8.1).
- **DORA** — Regulation (EU) 2022/2554, articles referenced by number and paragraph (e.g., Art. 28(2)).
- **NIS2** — Directive (EU) 2022/2555, articles referenced by number and paragraph (e.g., Art. 21(2)(d)).

2. Domain D1: Asset Inventory & Data Mapping

TPSA Ref.	TPSA Requirement	CIS Controls v8	ISO 27001:2022	DORA (2022/2554)	NIS2 (2022/2555)
D1-01	Asset Register — all assets processing client data	1.1, 2.1 (HW/SW inventory)	A.5.9 (Inventory of assets), A.5.10 (Acceptable use)	Art. 28(3) (register of contractual arrangements)	Art. 21(2)(a) (risk analysis policies)
D1-02	Asset Location — geographical and logical	1.1 (HW inventory attributes)	A.5.9, A.8.1 (User endpoint devices)	Art. 28(7)(a) (location of data processing)	Art. 21(2)(d) (supply chain security)
D1-03	Hosting Model — dedicated/shared + isolation	1.1 (asset attributes)	A.8.22 (Segregation of networks)	Art. 28(7)(b) (data segregation)	Art. 21(2)(d)
D1-04	Data Types Hosted — categories per asset	3.2 (Data inventory)	A.5.12 (Classification of information), A.5.13 (Labelling)	Art. 28(7)(a) (description of data)	Art. 21(2)(d)
D1-05	Data Flow Diagram	3.8 (Data flow documentation)	A.5.14 (Information transfer)	Art. 28(3) (supports)	—
D1-06	Sub-processors — fourth parties	15.2 (Monitor service providers) 15.3 (classify service providers)	A.5.21 (ICT supply chain security)	Art. 29 (subcontracting)	Art. 21(2)(d)
D1-07	Asset Classification	3.7 (Data classification scheme)	A.5.12, A.5.13	Art. 28(7)(a) (partial)	Art. 21(2)(a) (partial)
D1-08	Asset Owner	1.1 (SW asset owner)	A.5.9 (ownership)	Art. 28(3) (supports)	—

3. Domain D2: Data Protection

TPSA Ref.	TPSA Requirement	CIS Controls v8	ISO 27001:2022	DORA (2022/2554)	NIS2 (2022/2555)
D2-01	Encryption at Rest	3.11 (Encrypt data at rest)	A.8.24 (Use of cryptography)	Art. 9(2) (cryptographic controls)	Art. 21(2)(h) (cryptography)
D2-02	Encryption in Transit	3.10 (Encrypt data in transit)	A.8.24, A.5.14 (Information transfer)	Art. 9(2)	Art. 21(2)(h)
D2-03	Key Management	3.6 (supports), 3.10, 3.11 (supports)	A.8.24 (key management provisions)	Art. 9(2) (partial)	Art. 21(2)(h) (partial)
D2-04	Data Segregation — multi-tenant	3.12 (Segment data by sensitivity)	A.8.22 (Network segregation)	Art. 28(7)(b) (data segregation)	Art. 21(2)(d)
D2-05	Data Retention Policy	3.1 (Data management process)	A.5.33 (Protection of records)	Art. 28(7)(d) (data return/deletion)	Art. 21(2)(a) (supports)
D2-06	Data Deletion Process	3.5 (Data disposal)	A.8.10 (Information deletion),	Art. 28(7)(d), Art. 28(8) (post-	Art. 21(2)(a) (supports)

			A.7.14 (Secure disposal)	termination)	
D2-07	Data Classification Scheme	3.7 (Data classification scheme)	A.5.12, A.5.13	Art. 28(7)(a) (partial)	—
D2-08	Cross-border Transfers	—	A.5.14 (partial)	Art. 28(7)(a) (geographical restrictions)	Art. 21(2)(d) (supports)

4. Domain D3: Backup & Recovery

TPSA Ref.	TPSA Requirement	CIS Controls v8	ISO 27001:2022	DORA (2022/2554)	NIS2 (2022/2555)
D3-01	Backup Policy — scope, frequency, retention	11.1 (Perform automated backups)	A.8.13 (Information backup)	Art. 11(1) (ICT response and recovery), Art. 12 (Backup policies)	Art. 21(2)(c) (business continuity, backup)
D3-02	Backup Location — geographic/logical	11.4 (Backup storage)	A.8.13 (offsite provisions)	Art. 12(2) (separate location)	Art. 21(2)(c)
D3-03	Backup Encryption	11.3 (Protect backup data)	A.8.13, A.8.24	Art. 9(2) (supports)	Art. 21(2)(h) (supports)
D3-04	RTO Declared	11.1 (Recovery objectives)	A.5.29 (ICT continuity planning)	Art. 11(4) (recovery time objectives)	Art. 21(2)(c)
D3-05	RPO Declared	11.1 (Recovery objectives)	A.5.29	Art. 11(4) (recovery point objectives)	Art. 21(2)(c)
D3-06	Last Restore Test — date, scope, outcome	11.5 (Test backup recovery)	A.8.13 (testing provisions), A.5.30 (ICT readiness testing)	Art. 11(6) (testing of plans), Art. 12(2) (restoration testing)	Art. 21(2)(c)
D3-07	Restore Test Frequency	11.5	A.5.30	Art. 11(6)	Art. 21(2)(c)
D3-08	DR Plan Reference	11.1 (Recovery plan)	A.5.29, A.5.30	Art. 11(1)–(3) (ICT response/recovery plans)	Art. 21(2)(c)
D3-09	DR Test Results	11.5 (Test DR plans)	A.5.30 (ICT readiness for business continuity)	Art. 11(6), Art. 25 (testing of ICT tools)	Art. 21(2)(c)

5. Domain D4: Access Control & Identity Management

TPSA Ref.	TPSA Requirement	CIS Controls v8	ISO 27001:2022	DORA (2022/2554)	NIS2 (2022/2555)
D4-01	Authentication Mechanisms — MFA, password, SSO	6.3 (Require MFA), 6.5 (Require MFA for admin)	A.8.5 (Secure authentication)	Art. 9(4)(c) (strong authentication)	Art. 21(2)(j) (MFA, continuous auth)
D4-02	Privileged Access Management	5.4 (Restrict admin privileges), 6.5	A.8.2 (Privileged access rights)	Art. 9(4)(c) (access rights management)	Art. 21(2)(i) (access control policies)
D4-03	Access Review Cycle	6.1 (access granting process) and 6.8 (role based access and review)	A.5.18 (Access rights)	Art. 9(4)(b) (access rights review)	Art. 21(2)(i)
D4-04	Least Privilege Policy	5.4, 6.8 (Define and Maintain Role-Based Access Control)	A.5.15 (Access control), A.8.3 (Restriction of access)	Art. 9(4)(a) (least privilege)	Art. 21(2)(i)

D4-05	Client-Facing Access Controls	6.7 (Centralise access control for cloud)	A.5.15, A.8.5	Art. 28(7)(c) (access rights provisions)	Art. 21(2)(i) (partial)
D4-06	Third-Party Access Controls	15.2 (service provider management)	A.5.19 (Supplier relationships), A.5.20 (Addressing security within supplier agreements)	Art. 29 (subcontracting provisions)	Art. 21(2)(d)
D4-07	Logging & Monitoring of Access	8.2 (Collect audit logs), 8.5 (Centralise logging)	A.8.15 (Logging), A.8.16 (Monitoring activities)	Art. 10 (Detection — anomalous activities)	Art. 21(2)(b) (incident handling)

6. Domain D5: Vulnerability Management & Testing

TPSA Ref.	TPSA Requirement	CIS Controls v8	ISO 27001:2022	DORA (2022/2554)	NIS2 (2022/2555)
D5-01	Vulnerability Scanning — tools, frequency, SLA	7.1 (Vuln management process), 7.5 (Automated vuln scanning), 7.7 (Remediation)	A.8.8 (Technical vulnerability management)	Art. 9(1) (identification of ICT risks)	Art. 21(2)(e) (vulnerability handling, disclosure)
D5-02	Patch Management — SLAs by severity	7.3 (Perform Automated Operating System Patch Management), 7.4 (Perform Automated Application Patch Management)	A.8.8, A.8.19 (Installation of software)	Art. 9(2) (ICT security tools), Art. 7(1) (supports)	Art. 21(2)(e)
D5-03	Penetration Testing — scope, methodology, last date	18.2 (External pentest), 18.3 (Internal pentest)	A.8.8 (partial), A.5.36 (Compliance review)	Art. 25 (Testing of ICT tools), Art. 26 (TLPT/TIBER-EU)	Art. 21(2)(e) (partial)
D5-04	Pentest Remediation Status	7.7 (Remediation of vulnerabilities)	A.8.8 (remediation provisions)	Art. 25 (supports), Art. 26(8) (remediation from TLPT)	Art. 21(2)(e) (supports)
D5-05	Bug Bounty / VDP	7.1 (supports)	A.8.8 (supports)	—	Art. 21(2)(e) (vulnerability disclosure)
D5-06	SBOM Availability	2.6 (Allowlisted SW), 16.4 (SW component inventory)	A.8.19 (supports), A.5.21 (ICT supply chain)	Art. 28(3) (supports)	Art. 21(2)(d) (supports)
D5-07	TIBER-EU Readiness	18.2, 18.3 (supports)	A.5.36 (supports)	Art. 26(1)–(4) (TLPT requirements), Art. 26(4) (third-party participation)	Art. 21(2)(e) (partial)

7. Domain D6: Incident Management & Notification

TPSA Ref.	TPSA Requirement	CIS Controls v8	ISO 27001:2022	DORA (2022/2554)	NIS2 (2022/2555)
D6-01	Detection Capabilities — SIEM, EDR, SOC, MTTD	13.1 (Centralise security event alerting), 13.3 (Detection solutions)	A.8.15 (Logging), A.8.16 (Monitoring)	Art. 10 (Detection)	Art. 21(2)(b) (incident handling)
D6-02	Incident Response Plan	17.4 (incident response process) 17.5 (IR roles)	A.5.24 (IR planning), A.5.25 (Assessment and decision)	Art. 17 (ICT-related incident management)	Art. 21(2)(b)
D6-03	Client Notification SLA — timelines by severity	17.2 (Notification procedures)	A.5.24, A.5.26 (Response to incidents)	Art. 19(1)–(4) (Reporting of major ICT incidents — 4h initial, 72h intermediate, 1 month final)	Art. 23 (Reporting obligations)

D6-04	Notification Content — format, minimum content	17.2 (supports)	A.5.26, A.5.27 (Learning from incidents)	Art. 19(4) (content requirements for incident reports)	Art. 23(3) (notification content)
D6-05	Post-Incident Review — RCA, lessons learned	17.8 (Post-incident review)	A.5.27 (Learning from information security incidents)	Art. 17(3)(e) (post-incident reviews)	Art. 21(2)(b) (supports)
D6-06	Incident History (24 months)	17.8 (Conduct Post-Incident Reviews)	A.5.27 (supports)	Art. 17(3)(e) (supports), Art. 28(3) (transparency)	Art. 23 (supports)
D6-07	Secure Communication Channel	17.2 (Communication procedures)	A.5.14 (Information transfer), A.5.24	Art. 17(3)(c) (communication plans)	Art. 21(2)(b) (supports)

8. Domain D7: Compliance & Certification Status

TPSA Ref.	TPSA Requirement	CIS Controls v8	ISO 27001:2022	DORA (2022/2554)	NIS2 (2022/2555)
D7-01	Certifications Held — standard, scope, validity	15.1 (Service provider inventory)	A.5.22 (Monitoring, review of supplier services)	Art. 28(4) (due diligence on ICT providers)	Art. 21(2)(d) (supports)
D7-02	Certification Scope — in/out scope	15.3 (Assess service provider risk)	A.5.22	Art. 28(4)(b) (scope assessment)	Art. 21(2)(d) (supports)
D7-03	Audit Findings Summary	15.4 (Review service provider audit reports)	A.5.22, A.5.35 (Independent review)	Art. 28(3) (transparency provisions)	—
D7-04	Regulatory Status	15.1 (supports)	A.5.31 (Legal requirements), A.5.36 (Compliance review)	Art. 28(2) (due diligence, proportionality)	Art. 21(1) (risk management measures)
D7-05	Exclusions & Gaps	15.3 (supports)	A.5.22 (supports)	Art. 28(4) (supports)	—
D7-06	Insurance Coverage	—	—	Art. 28(3) (supports — risk transfer)	—

9. TPSA-02: Risk Dialogue Protocol Mapping

TPSA Ref.	TPSA Requirement	CIS Controls v8	ISO 27001:2022	DORA (2022/2554)	NIS2 (2022/2555)
RSC	Risk Scenario Card — client-initiated threat scenario submission	15.3 (Risk assessment of providers), 17.6 (Threat scenario definition)	A.5.19 (Supplier security policy), 8.1 (Operational planning — risk assessment)	Art. 28(1)(a) (risk assessment of ICT third-party), Art. 26(2) (threat scenarios for TLPT)	Art. 21(2)(a) (risk analysis), Art. 21(2)(d) (supply chain security)
SRA	Supplier Risk Assessment — formal response to RSC	15.4 (Review audit/assessment results)	A.5.22 (Monitoring supplier services), A.5.23 (Supplier service changes)	Art. 28(3) (transparency), Art. 28(6) (exercise of access/audit rights)	Art. 21(2)(d) (supports)
TEC-SCOPE	TIBER-EU Scoping — test perimeter from Disclosure Card	18.2, 18.3 (Pentest scoping)	A.5.36 (supports)	Art. 26(2)–(3) (TLPT scope definition), Art. 26(4) (third-party participation in scoping)	Art. 21(2)(e) (partial)
TEC-EXEC	TIBER-EU Execution coordination	18.2, 18.3 (supports)	A.5.36 (supports)	Art. 26(4) (cooperation during testing), Art. 26(7) (mutual recognition)	Art. 21(2)(e) (partial)
TEC-RESULTS	TIBER-EU Results — findings, remediation, feedback loop	18.5 (Pentest remediation)	A.5.36 (findings), A.5.27 (learning)	Art. 26(8) (remediation requirements), Art. 26(4) (results sharing with third party)	Art. 21(2)(e) (partial)
CUR	Classification Uplift Request — client-	3.7 (Classification updates)	A.5.12 (Classification), A.5.13	Art. 28(7)(a) (data classification	Art. 21(2)(a) (supports)

	driven reclassification		(Labelling)	provisions)	

10. Header & Cross-Cutting Requirements

TPSA Ref.	TPSA Requirement	CIS Controls v8	ISO 27001:2022	DORA (2022/2554)	NIS2 (2022/2555)
H-01–H-02	Supplier identification	15.1 (Service provider inventory)	A.5.19 (Supplier identification)	Art. 28(3) (register of arrangements)	Art. 21(2)(d) (supports)
H-03–H-05	Versioning and validity period	—	A.5.22 (Regular review)	Art. 28(3) (ongoing monitoring)	—
H-06	Scope description	15.1 (Scope of provider services)	A.5.20 (Scope in agreements)	Art. 28(2) (scope of ICT services)	Art. 21(2)(d) (partial)
H-10	TPSA Level declaration	15.1 (Criticality assessment)	A.5.22 (Monitoring level)	Art. 28(1)(a) (criticality classification)	—
H-11–H-12	Security/Compliance contacts	15.1 (supports), 17.2 (Incident contacts)	A.5.5 (Contact with authorities), A.5.24 (IR contacts)	Art. 28(7)(e) (designated contact points)	Art. 21(2)(b) (supports)
H-13	ED25519 Digital Signature — integrity, non-repudiation	3.14 (Log sensitive data access)	A.8.24 (Cryptography), A.5.33 (Record protection)	Art. 9(2) (supports)	Art. 21(2)(h) (supports)

11. Coverage Summary

The following table summarises the coverage of each target framework by the TPSA specification. Coverage refers to the third-party-relevant controls/articles that are directly or partially addressed by TPSA implementation.

Framework	Total Third-Party-Relevant Controls/Articles	Directly Mapped	Partially/Supporting	Key Gaps (require measures beyond TPSA)
CIS Controls v8	Safeguard 15 (6 sub-controls) + related controls across 12 categories	41 safeguards directly mapped	8 safeguards partially mapped	Safeguards related to internal security posture (not third-party-facing) are not covered by TPSA.
ISO 27001:2022	A.5.19–A.5.23 (5 controls) + supporting controls across all categories	28 Annex A controls directly mapped	12 controls partially mapped	ISMS process requirements (clauses 4–10) are not covered. TPSA addresses Annex A control implementation, not ISMS certification.
DORA	Art. 28–30 (ICT third-party risk) + Art. 9, 10, 11, 12, 17, 19, 25, 26	22 article paragraphs directly mapped	9 article paragraphs partially mapped	Oversight framework provisions (Art. 31–44) for critical ICT providers are regulatory-only, not addressable by TPSA.
NIS2	Art. 21(2)(a)–(j) (10 risk management measures)	7 measures directly mapped	3 measures partially mapped	Art. 21(2)(f) (effectiveness assessment), Art. 21(2)(g) (cyber hygiene, training) are only partially within TPSA scope.

11.1 Interpretation Guidance

TPSA certification does not replace certification or compliance with any of the mapped frameworks. A supplier certified TPSA provides **structured evidence** that facilitates a client's own compliance demonstration, but the client remains responsible for their overall compliance posture.

The mapping is designed to enable a **traceable audit trail**: an auditor can follow a path from a regulatory requirement (e.g., DORA Art. 28(7)(a)) to a TPSA domain (D1-02, D1-04) to a specific field in the supplier's Disclosure Card, and verify that the field is populated with substantive, current information.

Where the mapping indicates "partial" or "supports", the TPSA implementation contributes to but does not fully satisfy the target requirement. The client and/or supplier must identify and implement additional measures to achieve full compliance.

11.2 Framework Evolution

The Regulatory Mapping Matrix will be updated in alignment with the following events:

- **TPSA version updates**: when new fields or exchange types are added to TPSA-01 or TPSA-02, the mapping matrix is extended accordingly.

- **Framework revisions**: when CIS Controls, ISO 27001, DORA, or NIS2 are updated (e.g., CIS Controls v9, ISO 27001 amendments), the mappings are revised to reflect the new control/article numbering and content.
- **Framework expansion**: additional frameworks (NIST CSF 2.0, NIST SP 800-161r1, APRA CPS 234, SOX IT controls) may be added as supplementary mapping tables in future versions of TPSA-03.