TPSA

THIRD-PARTY SUPPLIER ACCOUNTABILITY

T P S A - 0 1

Supplier Disclosure Standard

Third-Party Supplier Accountability Framework

Specification Document

Version 1.0, April 2026

Author: Sébastien Poitrasson, Arthur Koenig Consulting

AK ARTHURKOENIG

1. Introduction

1.1 Purpose

This document defines the **TPSA-01: Supplier Disclosure Standard**, the first component of the Third-Party Supplier Accountability (TPSA) framework. It specifies the structure, content, format, and maintenance requirements for the **Supplier Disclosure Card**, the standardised document through which a supplier communicates its security posture to its clients.

The Supplier Disclosure Card is the foundational artifact of the TPSA framework. All other components, the Risk Dialogue Protocol (TPSA-02), the Regulatory Mapping Matrix (TPSA-03), and the Labelling & Certification Scheme (TPSA-04), depend on the Disclosure Card as their primary data source.

1.2 Scope

TPSA-01 applies to any organisation that provides ICT services, platforms, infrastructure, or software to other organisations and wishes to demonstrate structured security accountability. This includes, but is not limited to: cloud service providers (IaaS, PaaS, SaaS), managed service providers (MSP/MSSP), software vendors, data centre operators, telecommunications providers, and any third party processing, storing, or transmitting client data.

The standard is **technology-agnostic** and **regulation-agnostic** in its core design. It can be implemented regardless of the supplier's technology stack, hosting model, or geographical location. Regulatory mappings (DORA, NIS2, ISO 27001, CIS Controls) are provided in TPSA-03 as a companion reference.

1.3 Normative References

- **ISO/IEC 27001:2022**, Information security management systems
- **ISO/IEC 27002:2022**, Information security controls
- **ISO/IEC 27036-1 to 27036-4**, Information security for supplier relationships
- **CIS Controls v8**, Center for Internet Security Critical Security Controls
- **DORA (Regulation 2022/2554)**, Digital Operational Resilience Act
- **NIS2 Directive (2022/2555)**, Network and Information Security Directive
- **EBIOS Risk Manager**, ANSSI risk analysis methodology
- **MITRE ATT&CK**, Adversarial Tactics, Techniques, and Common Knowledge
- **TIBER-EU**, Threat Intelligence-Based Ethical Red Teaming

1.4 Terms and Definitions

Terms defined in the TPSA Position Paper (v1.0, April 2026) apply. Additional terms specific to this document:

- **Disclosure Card**: the structured document defined by this standard, published by a supplier for a given client or as a common baseline.
- **Common Disclosure**: the portion of a Disclosure Card that describes shared infrastructure, controls, and practices applicable to all clients.
- **Client-Specific Annex**: the portion of a Disclosure Card tailored to a specific client, detailing assets, data classification, and measures particular to that relationship.
- **Mandatory field**: a field that must be populated for the Disclosure Card to be considered conformant at any TPSA maturity level.
- **Conditional field**: a field that becomes mandatory when specific conditions are met (e.g., multi-tenant environment, DORA-regulated client).
- **Optional field**: a field that provides additional transparency but is not required for conformance.

2. Disclosure Card Structure

2.1 Architecture Overview

A Supplier Disclosure Card is a structured document composed of a **header section** (metadata, versioning, scope) and **seven disclosure domains**, each containing a defined set of fields. The card is further divided into a **Common Disclosure** layer and optional **Client-Specific Annexes**.

Layer	Content	Audience
Header	Supplier identity, card version, validity period, scope definition, contact information.	All stakeholders. Machine-readable metadata for automated processing.
Common Disclosure	Shared infrastructure, controls, certifications, and practices applicable to all clients. Domains D1–D7.	All clients. Published once, maintained centrally by the supplier.
Client-Specific Annex	Client-dedicated assets, data classification overrides, tailored controls, specific SLAs. Per-client overlay on D1–D7.	Individual client. Confidential between supplier and client.

2.2 Header Section

The header section provides metadata necessary for identification, versioning, and automated processing of the Disclosure Card.

ID	Field	Type	Req.	Description
H-01	**Supplier Name**	String	M	Legal name of the supplier organisation.
H-02	**Supplier Identifier**	String	M	Unique identifier (e.g., LEI, DUNS, SIREN/SIRET, company registration number).
H-03	**Card Version**	SemVer	M	Version number following semantic versioning (MAJOR.MINOR.PATCH).
H-04	**Issue Date**	ISO 8601	M	Date of publication of this version.
H-05	**Valid Until**	ISO 8601	M	Expiration date. Maximum validity: 12 months from issue date.
H-06	**Scope Description**	Text	M	Narrative description of the services, platforms, and infrastructure covered by this Disclosure Card.
H-07	**Card Type**	Enum	M	COMMON (shared baseline) or CLIENT_SPECIFIC (client annex). A CLIENT_SPECIFIC card must reference its parent COMMON card.
H-08	**Parent Card Ref**	String	C	Reference (ID + version) of the parent COMMON card. Mandatory when Card Type = CLIENT_SPECIFIC.
H-09	**Client Name**	String	C	Name of the client. Mandatory when Card Type = CLIENT_SPECIFIC.
H-10	**TPSA Level**	Enum	M	Declared TPSA maturity level: BASIC, ENHANCED, or FULL.
H-11	**Contact, Security**	Object	M	Security team contact: name, role, email, PGP key or S/MIME certificate reference.
H-12	**Contact, Compliance**	Object	O	Compliance/GRC team contact for audit and certification matters.
H-13	**Digital Signature**	ED25519	M	ED25519 signature of the card content, enabling integrity verification and non-repudiation.

M = Mandatory | C = Conditional | O = Optional

3. Disclosure Domains

The Disclosure Card is organised into seven domains (D1–D7), each addressing a critical dimension of the supplier's security posture relevant to its clients. Fields within each domain are classified as Mandatory (M), Conditional (C), or Optional (O).

3.1 Domain D1: Asset Inventory & Data Mapping

This domain identifies the assets that process, store, or transmit client data. It is the foundation for all subsequent domains and for the Risk Dialogue Protocol (TPSA-02). Accurate asset identification is critical for TIBER-EU test scoping under DORA Article 26.

ID	Field	Type	Req.	Description
D1-01	**Asset Register**	Array	M	List of all assets (infrastructure, platforms, applications, data stores) involved in the delivery of services to the client. Each asset entry includes: unique asset ID, asset name, asset type (server, database, application, network device, storage system, etc.), and a brief functional description.
D1-02	**Asset Location**	Object	M	For each asset: geographical location (country, region, data centre identifier) and logical location (network zone, VPC/VLAN, cloud region/AZ). Required for data residency compliance.
D1-03	**Hosting Model**	Enum	M	For each asset: DEDICATED (single-tenant) or SHARED (multi-tenant). If SHARED, the supplier must describe the isolation mechanism (logical, physical, hypervisor-level, container-level).
D1-04	**Data Types Hosted**	Array	M	For each asset: categories of client data processed or stored (e.g., personal data, financial data, health data, authentication credentials, logs, metadata). Aligned with data classification in D2.
D1-05	**Data Flow Diagram**	Reference	C	Reference to a data flow diagram showing how client data moves between assets, including ingress/egress points and inter-system communications. Mandatory at ENHANCED and FULL levels.
D1-06	**Sub-processors**	Array	C	List of any sub-processors (fourth parties) involved in processing client data, including their identity, role, location, and applicable contractual controls. Mandatory when sub-processors exist.
D1-07	**Asset Classification**	Enum	M	Supplier's classification of each asset (e.g., Public, Internal, Confidential, Restricted). Subject to Classification Uplift via client feedback (see Section 4).
D1-08	**Asset Owner**	String	M	Named role or team responsible for each asset's security and maintenance.

3.2 Domain D2: Data Protection

This domain describes the measures applied to protect client data at rest, in transit, and during processing, including key management, data segregation, and retention/deletion policies.

ID	Field	Type	Req.	Description
D2-01	**Encryption at Rest**	Object	M	Algorithms, key lengths, and scope of encryption for stored client data. Per-asset or per-data-type if different standards apply.
D2-02	**Encryption in Transit**	Object	M	Protocols (TLS version, cipher suites), scope (client-to-supplier, inter-service, intra-DC), and certificate management practices.
D2-03	**Key Management**	Object	M	Key generation, storage (HSM, KMS, software), rotation frequency, access controls on key material, and whether the client can bring their own keys (BYOK) or hold their own keys (HYOK).
D2-04	**Data Segregation**	Object	C	Mechanisms ensuring client data isolation in multi-tenant environments: database-level, schema-level, encryption-level, or application-level. Mandatory when D1-03 = SHARED.
D2-05	**Data Retention Policy**	Object	M	Retention periods by data type, legal basis for retention, and automated/manual deletion process at end of retention period or contract termination.
D2-06	**Data Deletion Process**	Object	M	Procedures for secure deletion/destruction: method (cryptographic erasure, physical destruction, overwrite), verification mechanism, and timeline from request to completion.
D2-07	**Data Classification Scheme**	Object	M	The supplier's data classification levels and their definitions. This is the baseline against which Classification Uplift operates (see Section 4).
D2-08	**Cross-border Transfers**	Object	C	Mechanisms for international data transfers (SCCs, adequacy decisions, binding corporate rules). Mandatory when assets span multiple jurisdictions.

3.3 Domain D3: Backup & Recovery

This domain describes the supplier's backup strategy, recovery capabilities, and, critically, the evidence of tested recovery. A backup that has never been tested is not a backup.

ID	Field	Type	Req.	Description
D3-01	**Backup Policy**	Object	M	Scope (which assets/data are backed up), frequency (real-time/daily/weekly), type (full/incremental/differential), and retention period of backups.
D3-02	**Backup Location**	Object	M	Geographical and logical location of backup storage. Distance from primary site. Whether backups are offline/air-gapped or online.
D3-03	**Backup Encryption**	Object	M	Encryption standards applied to backup data, key management for backup encryption keys.
D3-04	**RTO Declared**	Duration	M	Recovery Time Objective: maximum tolerable time to restore service after a disruption, per service/asset.
D3-05	**RPO Declared**	Duration	M	Recovery Point Objective: maximum tolerable data loss measured in time, per service/asset.
D3-06	**Last Restore Test**	Object	M	Date of the most recent backup restoration test, scope of the test, outcome (success/partial/failure), and any issues identified.
D3-07	**Restore Test Frequency**	Enum	M	How often backup restoration tests are conducted: monthly, quarterly, semi-annually, annually.
D3-08	**DR Plan Reference**	Reference	C	Reference to the supplier's Disaster Recovery Plan applicable to client services. Mandatory at ENHANCED and FULL levels.
D3-09	**DR Test Results**	Object	C	Date and outcome of the most recent DR test/exercise. Mandatory at ENHANCED and FULL levels.

3.4 Domain D4: Access Control & Identity Management

This domain describes how the supplier controls access to assets and data relevant to the client, including privileged access, authentication mechanisms, and review processes.

ID	Field	Type	Req.	Description
D4-01	**Authentication Mechanisms**	Object	M	Authentication methods for internal access to client-relevant assets: MFA type, password policy, SSO integration, certificate-based auth.
D4-02	**Privileged Access Mgmt**	Object	M	How privileged accounts (admin, root, DBA) are managed: PAM tooling, session recording, just-in-time access, break-glass procedures.
D4-03	**Access Review Cycle**	Object	M	Frequency and scope of access rights reviews. Evidence of last review date and outcome.
D4-04	**Least Privilege Policy**	Text	M	Description of how least privilege is enforced: RBAC/ABAC model, segregation of duties, default-deny posture.
D4-05	**Client-Facing Access**	Object	M	Controls on client-facing interfaces: API authentication, portal access, administrative console security, IP whitelisting capabilities.
D4-06	**Third-Party Access**	Object	C	Controls on access by the supplier's own contractors, vendors, or support staff to client data/systems. Mandatory when third-party access exists.
D4-07	**Logging & Monitoring**	Object	M	What access events are logged, retention period of access logs, monitoring/alerting for anomalous access patterns, and whether logs are available to the client.

3.5 Domain D5: Vulnerability Management & Testing

This domain describes the supplier's approach to identifying, assessing, and remediating vulnerabilities in assets relevant to the client. It includes penetration testing schedules and results, which are directly relevant to TIBER-EU test coordination under TPSA-02.

ID	Field	Type	Req.	Description
D5-01	**Vulnerability Scanning**	Object	M	Tools, frequency, scope (internal/external, infrastructure/application), and SLA for remediation by severity (Critical/High/Medium/Low).
D5-02	**Patch Management**	Object	M	Patch deployment process, SLAs by severity (e.g., Critical: 24h, High: 72h, Medium: 30d), and exception/deferral process.
D5-03	**Penetration Testing**	Object	M	Scope, methodology (black/grey/white box), frequency, and provider (internal/external). Date of last pentest and high-level outcome summary.
D5-04	**Pentest Remediation**	Object	M	Status of remediation for findings from the most recent penetration test: number of findings by severity, number remediated, number accepted, timeline for open items.
D5-05	**Bug Bounty Program**	Object	O	Whether the supplier operates a bug bounty or vulnerability disclosure program, scope, and responsiveness metrics.
D5-06	**SBOM Availability**	Boolean	C	Whether a Software Bill of Materials is maintained and available for client-facing applications. Mandatory at FULL level.
D5-07	**TIBER-EU Readiness**	Object	C	Whether the supplier has participated in or is prepared to participate in TIBER-EU/TLPT exercises. Last participation date if applicable. Mandatory at FULL level.

3.6 Domain D6: Incident Management & Notification

This domain describes the supplier's incident detection, response, and notification capabilities. Notification timelines are aligned with DORA Article 19 requirements for critical ICT third-party providers.

ID	Field	Type	Req.	Description
D6-01	**Detection Capabilities**	Object	M	Security monitoring tools (SIEM, EDR, NDR, SOC), coverage scope, and detection SLAs (mean time to detect).
D6-02	**Incident Response Plan**	Reference	M	Reference to the supplier's Incident Response Plan. Key elements: classification scheme, escalation matrix, roles and responsibilities.
D6-03	**Client Notification SLA**	Object	M	Maximum time from incident detection to client notification, by incident severity. DORA-regulated suppliers must align with Article 19 timelines (initial notification within 4 hours for major incidents).
D6-04	**Notification Content**	Object	M	Defined format and minimum content of incident notifications: affected assets, data impact assessment, containment measures, timeline, point of contact.
D6-05	**Post-Incident Review**	Object	M	Process for post-incident analysis: root cause analysis timeline, corrective action plan, lessons learned, and whether findings are shared with affected clients.
D6-06	**Incident History**	Array	C	Summary of security incidents affecting client data/services in the last 24 months: date, severity, impact, resolution. Mandatory at ENHANCED and FULL levels.
D6-07	**Communication Channel**	Object	M	Dedicated secure channel for incident communications: out-of-band communication method, escalation contacts, PGP/S/MIME for encrypted notifications.

3.7 Domain D7: Compliance & Certification Status

This domain provides transparency on the supplier's existing certifications, audit results, and regulatory compliance status. It enables clients to assess the supplier's baseline maturity and identify any gaps relative to their own regulatory requirements.

ID	Field	Type	Req.	Description
D7-01	**Certifications Held**	Array	M	List of current certifications: standard (ISO 27001, SOC 2, etc.), scope, issuing body, validity dates, certificate reference number.
D7-02	**Certification Scope**	Text	M	Clear description of what is and is not covered by each certification. Clients must be able to verify that the services they consume fall within the certified scope.
D7-03	**Audit Findings Summary**	Object	C	High-level summary of findings from the most recent certification audit: number of non-conformities by type (major/minor/observation), status of corrective actions. Mandatory at ENHANCED and FULL levels.
D7-04	**Regulatory Status**	Object	C	Compliance status with applicable regulations (DORA, NIS2, GDPR, sector-specific regulations). Self-assessed or independently verified.
D7-05	**Exclusions & Gaps**	Text	O	Known gaps in certification scope or compliance coverage. Transparency on exclusions builds trust and enables informed client decisions.
D7-06	**Insurance Coverage**	Object	O	Cyber insurance coverage: carrier, coverage limits, scope. Optional but relevant for client risk assessment.

4. Classification Uplift Mechanism

The Classification Uplift is an emergent property of the TPSA framework that leverages bidirectional disclosure to improve security posture across multi-tenant environments.

4.1 Mechanism

When a client reviews the Disclosure Card (specifically D1-07: Asset Classification and D2-07: Data Classification Scheme), they may determine that the supplier's classification of a shared asset is lower than the client's own classification of the data hosted on that asset. For example, a supplier may classify a shared storage array as "Internal" while a banking client classifies the data it stores there as "Confidential."

Under the TPSA framework, the client submits a **Classification Uplift Request** through the Client-Specific Annex, informing the supplier that their data on the identified asset requires a higher classification level.

4.2 Supplier Obligations

Upon receiving a Classification Uplift Request, the supplier must:

- **Acknowledge** the request within 10 business days.
- **Assess** the impact of the uplift on existing controls and on other clients sharing the same asset.
- **Apply** the higher classification to the asset if technically and operationally feasible, or **propose** alternative measures (e.g., migration to a dedicated asset, additional encryption layer, logical isolation enhancement).
- **Update** the Common Disclosure Card to reflect the new classification, where applicable.
- **Notify** other clients on the same shared asset of the classification change (without disclosing the requesting client's identity).

4.3 Rising-Tide Effect

The Classification Uplift creates a **virtuous cycle** in multi-tenant environments. The most demanding client drives the security posture upward, and all other clients benefit from the enhanced controls. Over time, shared assets converge toward the highest classification level of any tenant, which is the security-optimal outcome.

This mechanism inverts the current market dynamic where multi-tenant environments default to the lowest common denominator. Under TPSA, suppliers are incentivised to serve demanding clients because the uplift effort is amortised across all tenants.

5. Disclosure Card Lifecycle

5.1 Publication

The supplier publishes the initial Disclosure Card upon TPSA adoption. The Common Disclosure is published first; Client-Specific Annexes are created as client relationships require them.

Publication format: the Disclosure Card must be available in **JSON format** conforming to the TPSA-01 JSON Schema (see Appendix A). Human-readable formats (PDF, HTML) may be generated from the canonical JSON representation. The JSON document must be digitally signed using ED25519 (field H-13).

5.2 Versioning

Disclosure Cards follow **semantic versioning**:

- **MAJOR** version increment: structural changes to the card (new domains, field removals, schema changes).
- **MINOR** version increment: content updates that change the security posture (new assets, changed controls, updated pentest results).
- **PATCH** version increment: corrections, clarifications, or formatting changes with no impact on security posture.

Every version change must update the Issue Date (H-04) and be re-signed (H-13). A changelog must be maintained.

5.3 Review Cycle

Disclosure Cards must be reviewed and updated at minimum:

- **TPSA Basic**: annually.
- **TPSA Enhanced**: semi-annually, and within 30 days of any material change (new asset, significant incident, certification change).
- **TPSA Full**: continuously maintained, with updates published within 15 days of any material change.

5.4 Revocation

A Disclosure Card may be revoked by the supplier if the described services are discontinued or if the card content becomes materially inaccurate pending update. Revocation must be communicated to all clients with active Client-Specific Annexes. A revoked card must not be relied upon for compliance purposes.

6. Conformance Requirements

A Disclosure Card is conformant with TPSA-01 when it meets the following criteria:

6.1 Structural Conformance

- The card is published in valid JSON conforming to the TPSA-01 JSON Schema.
- All Mandatory (M) fields are populated with substantive content.
- All applicable Conditional (C) fields are populated when their trigger conditions are met.
- The card is digitally signed using ED25519 (H-13) and the signature is verifiable.
- The card version (H-03) follows semantic versioning conventions.

6.2 Content Conformance

- Field values are factually accurate and current as of the Issue Date.
- Asset inventories (D1) are complete, no assets involved in client data processing are omitted.
- Dates (last pentest, last restore test, last access review) are specific and verifiable, not vague or approximate.
- Remediation statuses (D5-04, D7-03) reflect the actual state, not planned or aspirational outcomes.

6.3 Maturity Level Requirements

Criterion	BASIC	ENHANCED	FULL
Fields Required	All M fields	All M + all applicable C fields	All M + C + recommended O fields
Review Cycle	Annual	Semi-annual + event-driven (30 days)	Continuous (15 days after material change)
Annex Support	Common Disclosure only	Common + Client-Specific Annexes	Common + Client-Specific + Classification Uplift process
Signature	ED25519 required	ED25519 required	ED25519 required + countersignature by auditor
TIBER-EU	Not required	Readiness declaration	Active participation capability demonstrated

Appendix A: JSON Schema (Excerpt)

The following is an excerpt of the TPSA-01 JSON Schema defining the Disclosure Card structure. The complete schema is published as a standalone machine-readable file (tpsa-01-schema.json).

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "$id": "https://tpsa.org/schemas/tpsa-01/v1.0",
  "title": "TPSA-01 Supplier Disclosure Card",
  "type": "object",
  "required": ["header", "domains"],
  "properties": {
    "header": {
      "type": "object",
      "required": ["supplier_name", "supplier_id", "card_version",
                   "issue_date", "valid_until", "scope_description",
                   "card_type", "tpsa_level", "contact_security",
                   "digital_signature"],
      "properties": {
        "supplier_name": { "type": "string" },
        "supplier_id": {
          "type": "object",
          "properties": {
            "type": { "enum": ["LEI","DUNS","SIREN","OTHER"] },
            "value": { "type": "string" }
          }
        },
        "card_version": { "type": "string", "pattern": "^\\d+\\.\\d+\\.\\d+$" },
        "issue_date": { "type": "string", "format": "date" },
        "valid_until": { "type": "string", "format": "date" },
        "card_type": { "enum": ["COMMON", "CLIENT_SPECIFIC"] },
        "tpsa_level": { "enum": ["BASIC", "ENHANCED", "FULL"] },
        "contact_security": { "$ref": "#/$defs/contact" },
        "digital_signature": { "$ref": "#/$defs/ed25519_sig" }
      }
    },
    "domains": {
      "type": "object",
      "required": ["d1_assets","d2_data_protection","d3_backup",
                   "d4_access_control","d5_vulnerability_mgmt",
                   "d6_incident_mgmt","d7_compliance"],
      "properties": {
        "d1_assets": { "$ref": "#/$defs/domain_d1" },
        "d2_data_protection": { "$ref": "#/$defs/domain_d2" },
        "d3_backup": { "$ref": "#/$defs/domain_d3" },
        "d4_access_control": { "$ref": "#/$defs/domain_d4" },
        "d5_vulnerability_mgmt": { "$ref": "#/$defs/domain_d5" },
        "d6_incident_mgmt": { "$ref": "#/$defs/domain_d6" },
        "d7_compliance": { "$ref": "#/$defs/domain_d7" }
      }
    }
  }
}
```

Appendix B: Example Disclosure Card

The following is a fictitious but realistic example of a Common Disclosure Card for a mid-tier SaaS provider. It illustrates how each domain is populated in practice.

Header

Field	Value
Supplier Name	CloudWorks SAS
Supplier ID	SIREN: 987 654 321
Card Version	1.2.0
Issue Date	2026-04-01
Valid Until	2027-03-31
Scope	CloudWorks Document Management Platform (DMP), SaaS application hosted on dedicated infrastructure in Equinix PA3 (Paris) and Equinix FR5 (Frankfurt). Covers all platform components: web application, API gateway, document storage, search indexing, and authentication services.
Card Type	COMMON
TPSA Level	ENHANCED
Contact, Security	Marie Dupont, CISO, security@cloudworks.example.com, PGP: 0xABCD1234

D1: Asset Inventory (excerpt)

Asset ID	Name	Type	Location	Hosting	Classification	Data Types
CW-SRV-01	DMP App Cluster	Kubernetes Cluster	Equinix PA3, FR	Shared	Confidential	App logic, session data
CW-DB-01	Primary DB (PostgreSQL)	Database	Equinix PA3, FR	Shared	Confidential	Client metadata, user accounts, document index
CW-STO-01	Document Storage (S3-compat)	Object Storage	Equinix PA3, FR	Shared	Restricted	Client documents (encrypted per-tenant)
CW-STO-02	Backup Storage	Object Storage	Equinix FR5, DE	Shared	Restricted	Encrypted backup replicas

D3: Backup & Recovery (excerpt)

Field	Value
Backup Policy	Full daily backup of CW-DB-01 at 02:00 UTC. Continuous replication of CW-STO-01 to CW-STO-02 (Equinix FR5). Incremental transaction log backups every 15 minutes. Retention: 30 days for daily, 90 days for weekly, 1 year for monthly.
Backup Location	CW-STO-02, Equinix FR5 Frankfurt, Germany. 450km from primary site. Online replication with 4-hour air-gap snapshot to offline LTO-9 tape weekly.
RTO Declared	Platform services: 4 hours. Document access: 8 hours. Full operational recovery: 24 hours.
RPO Declared	Database: 15 minutes (transaction log). Document storage: < 1 hour (continuous replication lag).
Last Restore Test	2026-02-15. Full restore of CW-DB-01 from daily backup to isolated environment. Outcome: SUCCESS. Time to restore: 2h47m (within 4h RTO). Data integrity verified via checksum comparison. 100% records recovered.
Restore Test Frequency	Quarterly. Next scheduled: 2026-05-15.

D5: Vulnerability Management (excerpt)

Field	Value
Vulnerability Scanning	External: weekly (Qualys). Internal: daily (Wazuh). Container images: on every build (Trivy). SLA: Critical 24h, High 72h, Medium 30d, Low 90d.
Penetration Testing	Annual external pentest by Synacktiv (grey box). Last test: 2026-01-20 to 2026-02-07. Scope: external attack surface + API + authentication flows. Methodology: OWASP WSTG + PTES.
Pentest Remediation	Findings: 0 Critical, 2 High, 5 Medium, 8 Low. High: 2/2 remediated (2026-02-28). Medium: 4/5 remediated, 1 accepted with compensating control (documented). Low: 6/8 remediated, 2 scheduled for Q2 2026.
TIBER-EU Readiness	Not yet participated. Readiness assessment completed March 2026. Scoping documentation prepared. Available for client-initiated TLPT exercises from Q3 2026.

D6: Incident Management (excerpt)

Field	Value
Detection Capabilities	SOC: internal 8x5, Sekoia.io MDR 24x7. SIEM: Wazuh. EDR: CrowdStrike Falcon on all endpoints. NDR: Suricata on network perimeters. Mean time to detect (MTTD): < 15 minutes for critical alerts.
Client Notification SLA	Critical/Major incident: initial notification within 4 hours of detection (DORA-aligned). Significant incident: within 24 hours. Minor incident: included in next periodic security report. Notification format: structured email (PGP-encrypted) with TPSA incident template.
Incident History (24m)	2025-09-12: Medium severity. Unauthorised access attempt on API gateway (brute-force). Detected in 8 minutes, blocked automatically. No data exposure. Root cause: lack of rate limiting on legacy endpoint. Remediated 2025-09-14 (rate limiting deployed). No client data affected.

D7: Compliance & Certification (excerpt)

Field	Value
Certifications Held	ISO 27001:2022, Scope: DMP platform operations and development. Issuing body: LSTI. Valid: 2025-06-01 to 2028-05-31. Certificate: LSTI-27001-2025-0847. SOC 2 Type II, Scope: Security and Availability trust criteria. Period: 2025-01-01 to 2025-12-31. Auditor: Mazars.
Audit Findings	ISO 27001 surveillance audit (2026-01): 0 major NC, 1 minor NC (incomplete evidence of supplier security review for one sub-processor). Corrective action completed 2026-02-15.
Exclusions & Gaps	Corporate IT (internal email, HR systems) is outside ISO 27001 scope. HDS (Hébergement de Données de Santé) certification not held, health data should not be stored on the platform without prior agreement and additional controls.