TPSA

THIRD-PARTY SUPPLIER ACCOUNTABILITY

T P S A - 0 4

# Labelling & Certification Scheme

## Third-Party Supplier Accountability Framework

*Maturity Levels • Audit Process • Certification Lifecycle • Governance*

Version 1.0 April 2026

Author: Sébastien Poitrasson, Arthur Koenig Consulting



AK ARTHURKOENIG

 

# 1. Introduction

## 1.1 Purpose

This document defines the **TPSA-04: Labelling and Certification Scheme**, the fourth and final component of the Third-Party Supplier Accountability framework. It specifies the maturity levels, certification criteria, audit process, certification lifecycle, and governance model for the TPSA label.

The TPSA label is designed to function as a **market signal** — a recognisable credential that enables suppliers to demonstrate structured security accountability and enables clients to identify suppliers that meet defined transparency standards. The label operates analogously to ISO 27001 certification or SOC 2 attestation, but is specifically focused on **third-party accountability and transparency toward clients**.

## 1.2 Scope

TPSA-04 applies to all organisations seeking TPSA certification and to all entities involved in the certification process: suppliers (applicants), certification bodies (auditors), and the TPSA governance body (standard owner).

This document does not define the technical content of what is audited — that is specified in TPSA-01 (Supplier Disclosure Standard) and TPSA-02 (Risk Dialogue Protocol). TPSA-04 defines **how** conformance is assessed, **who** assesses it, and **what** the resulting certification means.

## 1.3 Principles

The TPSA certification scheme is built on five principles:

- **Independence**: certification is performed by accredited third-party auditing bodies, not by the standard owner, not by consultants, and not by the supplier itself.
- **Proportionality**: three maturity levels (BASIC, ENHANCED, FULL) allow suppliers of different sizes and criticality to engage with the standard at an appropriate level, without requiring the same effort from a 10-person SaaS startup as from a global cloud provider.
- **Transparency**: certification criteria are publicly available. Audit processes are documented. The label's meaning is unambiguous.
- **Compatibility**: the TPSA certification process is designed to integrate with, not duplicate, existing certification activities (ISO 27001, SOC 2, HDS, SecNumCloud). Where a supplier already holds relevant certifications, the TPSA auditor leverages those results.
- **Continuous validity**: certification is not a point-in-time snapshot. It includes ongoing surveillance, event-driven reviews, and a defined suspension/withdrawal process.

# 2. Maturity Levels

## 2.1 Overview

The TPSA framework defines three maturity levels. Each level builds on the previous one, adding requirements progressively. A supplier may seek certification at any level, but must meet **all** requirements of the chosen level and all levels below it.

| Level | Name | Summary |
|---|---|---|
| **Level 1** | **TPSA Basic** | Foundational transparency. The supplier publishes a conformant Disclosure Card (TPSA-01) with all mandatory fields populated. Annual review cycle. No Risk Dialogue Protocol requirement. |
| **Level 2** | **TPSA Enhanced** | Active accountability. Full Disclosure Card plus operational Risk Dialogue Protocol (TPSA-02). Demonstrated capacity to receive, acknowledge, and respond to client Risk Scenario Cards. Client-Specific Annexes supported. Semi-annual review cycle. |
| **Level 3** | **TPSA Full** | Complete accountability. All TPSA-01 and TPSA-02 requirements including TIBER-EU integration capability. Continuous Disclosure Card maintenance. Classification Uplift process demonstrated. Auditor countersignature on Disclosure Cards. |

## 2.2 Level 1: TPSA Basic — Detailed Requirements

### TPSA-01 Requirements

- A Common Disclosure Card conforming to the TPSA-01 JSON Schema is published and digitally signed (ED25519).
- All Mandatory (M) fields across all seven domains (D1–D7) are populated with substantive, current, and verifiable content.
- The Card is reviewed and updated at least annually (H-05 validity ≤ 12 months).
- A designated security contact (H-11) is reachable and responsive.

### TPSA-02 Requirements

- Not required at BASIC level.

### Audit Evidence

- The auditor verifies the Disclosure Card against source evidence: asset registers, configuration records, backup logs, pentest reports, certification documents, incident records.
- Minimum **3 fields per domain** are verified against source evidence (sampled by the auditor).

## 2.3 Level 2: TPSA Enhanced — Detailed Requirements

**TPSA-01 Requirements (in addition to BASIC)**

- All Mandatory (M) and all applicable Conditional (C) fields are populated.
- Client-Specific Annexes are produced for all clients requesting them.
- The Card is reviewed semi-annually and updated within 30 days of any material change.

**TPSA-02 Requirements**

- The Risk Dialogue Protocol is operationally implemented: the supplier can receive, acknowledge, and respond to Risk Scenario Cards.
- At least one transport mechanism (API, encrypted email, or offline exchange) is documented and functional.
- Acknowledgement timeline: ≤ 10 business days. Response timeline: ≤ 30 business days.
- A log of all exchanges is maintained and accessible to the auditor.
- The supplier has demonstrated the ability to produce a conformant Supplier Risk Assessment (SRA) by completing at least one RSC/SRA cycle (real or simulated during the certification audit).

**Audit Evidence**

- All BASIC evidence requirements, plus:
- Review of at least **one completed RSC/SRA exchange** (real client exchange or audit simulation).
- Verification of exchange log integrity and completeness.
- Verification that Client-Specific Annexes exist for clients that have requested them.
- Minimum **5 fields per domain** verified against source evidence.

## 2.4 Level 3: TPSA Full — Detailed Requirements

**TPSA-01 Requirements (in addition to ENHANCED)**

- All Mandatory (M), Conditional (C), and recommended Optional (O) fields are populated.
- Continuous Card maintenance: updates published within 15 days of any material change.
- Classification Uplift process is documented and has been exercised at least once (real or simulated).
- Disclosure Cards are countersigned by the TPSA certification auditor at each surveillance audit.

**TPSA-02 Requirements (in addition to ENHANCED)**

- Acknowledgement timeline: ≤ 5 business days. Response timeline: ≤ 15 business days.
- TIBER-EU Coordination Messages (TEC) are supported: the supplier can participate in TLPT scoping, execution coordination, and results handling.
- TIBER-EU readiness has been demonstrated through at least one exercise (real or tabletop).
- The TPSA Reference Platform API (or conformant equivalent) is implemented and operational.

**Audit Evidence**

- All ENHANCED evidence requirements, plus:
- Review of at least **three completed RSC/SRA exchanges**.
- Evidence of at least one Classification Uplift cycle (request, assessment, outcome).
- Evidence of TIBER-EU readiness (TEC-SCOPE documentation, tabletop exercise record, or actual TLPT participation).
- **All fields across all domains** verified against source evidence (100% coverage).

# 3. Certification Process

## 3.1 Process Overview

The TPSA certification process follows a four-phase model consistent with established certification practices (ISO 17021, IAF MD guidelines):

| Phase | Name | Description |
|---|---|---|
| **Phase 1** | Application & Scoping | The supplier submits an application to an accredited certification body, specifying the target TPSA level, the scope of services to be certified, and existing certifications. The CB reviews the application and issues a scoping proposal. |
| **Phase 2** | Document Review (Stage 1) | The CB reviews the Disclosure Card(s), Risk Dialogue Protocol documentation, exchange logs, and supporting evidence. The CB identifies any gaps or non-conformities that must be resolved before proceeding. This phase may be conducted remotely. |
| **Phase 3** | On-site/Remote Audit (Stage 2) | The CB performs the substantive audit: verification of Disclosure Card content against source evidence, review of Risk Dialogue Protocol operations (for ENHANCED/FULL), interview of key personnel, and assessment of processes and controls. Includes an RSC/SRA simulation for first-time ENHANCED/FULL applicants without real exchanges to review. |
| **Phase 4** | Certification Decision | The CB issues the certification decision based on audit findings. The decision is made by a person or committee independent of the audit team. Three outcomes: CERTIFIED (no major non-conformities), CONDITIONAL (minor NCs requiring correction within 90 days), DENIED (major NCs). |

## 3.2 Audit Duration

Recommended minimum audit durations (on-site/remote audit days, excluding document review):

| Supplier Size | BASIC | ENHANCED | FULL |
|---|---|---|---|
| **Small** (< 50 employees) | 1 day | 2 days | 3 days |
| **Medium** (50–500 employees) | 1.5 days | 3 days | 5 days |
| **Large** (> 500 employees) | 2 days | 4 days | 7+ days |

*Durations are indicative. The CB may adjust based on scope complexity, number of services, and geographical distribution.*

## 3.3 Integration with Existing Certifications

The TPSA audit is designed to **leverage existing certification evidence** to avoid duplication of effort:

- **ISO 27001:2022**: if the supplier holds a valid ISO 27001 certificate covering the services in scope, the TPSA auditor may rely on the ISO 27001 Statement of Applicability and last audit report for domains D2 (Data Protection), D4 (Access Control), D5 (Vulnerability Management), and D6 (Incident Management) — focusing the TPSA audit on D1 (Asset Inventory, which is TPSA-specific in its client-orientation), D3 (Backup, where TPSA requires tested restore evidence), D7 (Compliance status), and the Risk Dialogue Protocol (TPSA-02).
- **SOC 2 Type II**: a current SOC 2 report covering Security and Availability trust criteria may be accepted as supporting evidence for D4, D5, and D6. The TPSA auditor reviews the report for relevant findings but does not re-audit the covered controls.
- **HDS / SecNumCloud / C5**: sector-specific certifications may provide evidence for specific domains. The CB determines the extent of reliance on a case-by-case basis.

This approach reduces audit cost and time for suppliers who already maintain mature certification portfolios, making TPSA adoption incremental rather than burdensome.

The TPSA audit is designed to **leverage existing certification evidence for baseline controls** while maintaining independent verification of all TPSA-specific requirements. This distinction is fundamental to the credibility of the TPSA label.

**What existing certifications can cover:**

If the supplier holds a valid ISO 27001 certificate, SOC 2 Type II report, or equivalent certification covering the services in scope, the TPSA auditor may accept the existence and general effectiveness of baseline security controls as established by those certifications. For example, the auditor does not need to re-verify that the supplier has an access control process (ISO 27001 A.8.2) or an incident response plan (A.5.24) if these are within a current certification scope.

**What the TPSA auditor must always verify independently, regardless of existing certifications:**

First, **Disclosure Card accuracy**: every field in the Disclosure Card must be verified against source evidence. An ISO 27001 certificate proves that a control exists; it does not prove that the supplier has accurately and completely described that control in the TPSA Disclosure Card. The TPSA auditor verifies that the content of D1 through D7 is truthful, current, specific, and sufficiently detailed for client consumption. A generic statement like "encryption is applied" when the Disclosure Card should specify algorithms, key lengths, and scope is a non-conformity even if the supplier is ISO 27001 certified.
Second, **Risk Dialogue Protocol operationality** (ENHANCED and FULL levels): no existing certification covers the RSC/SRA exchange process, KRI publication, or TIBER-EU coordination as defined in TPSA-02. These are unique TPSA requirements and must be fully audited.

Third, **Classification Uplift process** (FULL level): no existing certification addresses the bidirectional classification mechanism. The auditor must verify that the process is documented, has been exercised, and produces the expected outcomes.

Fourth, **Client-orientation of disclosures**: existing certifications assess whether the supplier protects its own information assets. TPSA assesses whether the supplier transparently and accurately communicates its security posture **to its clients**. These are fundamentally different objectives. A supplier may have excellent internal security and a valid ISO 27001 certificate while producing a Disclosure Card that is vague, incomplete, or misleading. The TPSA auditor assesses the client-facing transparency, not the internal control effectiveness.

Fifth, **KRI accuracy and timeliness**: the auditor verifies that published KRIs are based on real measurements, that the underlying data sources are reliable, and that values and thresholds are current. This is not covered by any existing certification.
**In summary**: existing certifications reduce the TPSA audit effort on the question "does the supplier have security controls?" They do not reduce the effort on the question "has the supplier accurately, completely, and usefully disclosed those controls to its clients?" The second question is the essence of TPSA and is always independently audited.

## 3.4 Limits of Certification Reliance — Independent TPSA Verification

While existing certifications reduce audit effort on baseline controls, the TPSA auditor must always verify the following independently, regardless of the supplier's existing certification portfolio:

Disclosure Card accuracy: every field in the Disclosure Card must be verified against source evidence. An ISO 27001 certificate proves that a control exists; it does not prove that the supplier has accurately and completely described that control in the TPSA Disclosure Card. A generic statement like "encryption is applied" when the Disclosure Card should specify algorithms, key lengths, and scope is a non-conformity even if the supplier is ISO 27001 certified.

Risk Dialogue Protocol operationality (ENHANCED and FULL levels): no existing certification covers the RSC/SRA exchange process, KRI publication, or TIBER-EU coordination as defined in TPSA-02. These are unique TPSA requirements and must be fully audited.

Classification Uplift process (FULL level): no existing certification addresses the bidirectional classification mechanism. The auditor must verify that the process is documented, has been exercised, and produces the expected outcomes.

Client-orientation of disclosures: existing certifications assess whether the supplier protects its own information assets. TPSA assesses whether the supplier transparently and accurately communicates its security posture to its clients. These are fundamentally different objectives. A supplier may have excellent internal security and a valid ISO 27001 certificate while producing a Disclosure Card that is vague, incomplete, or misleading.
KRI accuracy and timeliness: the auditor verifies that published KRIs are based on real measurements, that the underlying data sources are reliable, and that values and thresholds are current.

In summary: existing certifications answer the question "does the supplier have security controls?" The TPSA audit answers the question "has the supplier accurately, completely, and usefully disclosed those controls to its clients and does the supplier maintain an operational dialogue about risk?" The second question is the essence of TPSA and is never delegated to another certification.

# 4. Certification Lifecycle

## 4.1 Certification Validity

TPSA certification is valid for **three years** from the date of the certification decision, subject to successful surveillance audits.

## 4.2 Surveillance Audits

Surveillance audits are conducted to verify ongoing conformance between initial certification and recertification:

| TPSA Level | Surveillance Frequency | Scope | Mode |
|---|---|---|---|
| **BASIC** | Annual | Verification of Disclosure Card currency. Sample verification of 2 fields per domain. | Remote |
| **ENHANCED** | Semi-annual | Disclosure Card verification + review of RSC/SRA exchanges since last audit. Sample 3 fields per domain. | Remote or on-site |
| **FULL** | Semi-annual + event-driven | Full Disclosure Card verification. All RSC/SRA/TEC exchanges reviewed. Classification Uplift activity reviewed. Countersignature of current Card. | On-site required for at least 1 per year |

## 4.3 Recertification

Before the three-year validity expires, the supplier undergoes a **recertification audit**. The recertification audit has the same scope as an initial certification audit (Phase 2 + Phase 3) but may be reduced in duration if the surveillance audit history shows consistent conformance.

If the supplier wishes to upgrade to a higher TPSA level (e.g., BASIC to ENHANCED), the upgrade audit covers the delta requirements of the target level and may be combined with a surveillance or recertification audit.

## 4.4 Non-Conformities

Non-conformities identified during initial, surveillance, or recertification audits are classified as:

| Classification | Definition | Required Action |
|---|---|---|

| | | |
|---|---|---|
| **Major NC** | A mandatory requirement is not implemented, is ineffective, or the Disclosure Card content is materially inaccurate on a critical point (e.g., asset omission, false pentest date). | Corrective action within 90 days. Verification audit required before certification or continuation. Two unresolved Major NCs at any audit trigger suspension. |
| **Minor NC** | A requirement is partially implemented, a field is incomplete or imprecise, or a process exists but has not been consistently followed. | Corrective action within 180 days. Verification at next surveillance audit. Three or more unresolved Minor NCs may be escalated to Major. |
| **Observation** | An area for improvement that does not constitute a non-conformity. A risk of future non-conformity if not addressed. | No mandatory corrective action. Reviewed at next surveillance. Good practice to address. |

## 4.5 Suspension and Withdrawal

### Suspension

TPSA certification may be **suspended** under the following conditions:

- Two or more unresolved Major non-conformities at any audit.
- Failure to undergo a scheduled surveillance audit within 60 days of the due date.
- The supplier requests voluntary suspension (e.g., during a major reorganisation).
- Credible evidence of material misrepresentation in the Disclosure Card is reported and substantiated.

During suspension, the supplier must **cease using the TPSA label** and must notify all clients with active Client-Specific Annexes. Suspension lasts a maximum of 6 months, during which the supplier must resolve the underlying issues and undergo a restoration audit. If not restored within 6 months, certification is withdrawn.

### Withdrawal

Certification is **withdrawn** when:

- Suspension is not resolved within 6 months.
- The supplier explicitly requests withdrawal.
- The supplier ceases to provide the services in the certified scope.
- Evidence of fraud or deliberate falsification of Disclosure Card content is established.

Withdrawal is permanent for the current certification cycle. The supplier may reapply after a minimum **12-month cooling period** and must undergo a full initial certification audit.

# 5. Certification Bodies

## 5.1 Accreditation Requirements

TPSA certification audits are performed by **accredited certification bodies (CBs)**. To be accredited for TPSA certification, a CB must meet the following requirements:

- **ISO/IEC 17021-1** accreditation (or national equivalent) for management system certification, OR **ISO/IEC 17065** accreditation for product/service certification.
- Demonstrated competence in information security auditing, evidenced by at least 3 years of ISO 27001, SOC 2, or equivalent certification activity.
- At least two qualified TPSA auditors on staff (see Section 5.2).
- Formal acceptance of the TPSA Certification Body Agreement, including adherence to the certification process, non-conformity classification, and reporting requirements defined in this document.

The TPSA governance body maintains a **public register of accredited CBs**. Only CBs listed in this register may issue TPSA certificates.

## 5.2 Auditor Qualifications

A TPSA auditor must hold:

- A recognised information security certification: **CISSP, CISA, ISO 27001 Lead Auditor**, or equivalent.
- At least **5 years of professional experience** in information security, including third-party risk management, supply chain security, or supplier auditing.
- Completion of the **TPSA Auditor Training Programme** (developed and delivered by the TPSA governance body or its authorised training partners).
- Demonstrated knowledge of the regulatory frameworks mapped in TPSA-03 (DORA, NIS2, ISO 27001, CIS Controls).

For TPSA Full audits involving TIBER-EU integration assessment, the audit team must include at least one member with **TLPT/TIBER-EU experience** (participation in a TIBER-EU exercise as threat intelligence provider, red team, or test manager).

## 5.3 Impartiality and Conflict of Interest

The TPSA certification scheme enforces strict separation between consulting and certification:

- A CB (or its affiliated entities) that has provided **consulting, advisory, or implementation services** to a supplier within the preceding 24 months **may not certify** that supplier.
- Individual auditors who have provided consulting services to the supplier within the preceding 24 months are disqualified from the audit team.

- The TPSA standard author and affiliated consultancies may provide advisory and implementation support but **never certification audits**. This separation is fundamental to the credibility of the label.

# 6. The TPSA Label

## 6.1 Label Designation

Upon successful certification, the supplier is authorised to use the TPSA label with the following designation format:

**TPSA Certified — [Level] — [Scope Summary]**
Certificate #[CB-REF] — Valid until [DATE]

Examples:

- **TPSA Certified — Enhanced — CloudWorks Document Management Platform** / Certificate #LSTI-TPSA-2027-001 / Valid until 2030-03-31
- **TPSA Certified — Basic — DataHost Infrastructure Services (EU regions)** / Certificate #AFNOR-TPSA-2027-042 / Valid until 2030-06-30

## 6.2 Label Usage Rules

- The label may be used in marketing materials, websites, proposals, and contractual documentation **only for the certified scope**.
- The label must always include the **level** (Basic, Enhanced, or Full) and the **scope summary**. Use of the label without level and scope is prohibited.
- The label must reference the **certificate number** and **validity date** in any context where clients rely on it for compliance decisions.
- The supplier must **cease using the label immediately** upon suspension or withdrawal.
- Misleading use of the label (e.g., implying FULL certification when certified at BASIC, or extending the label to out-of-scope services) is a **grounds for immediate suspension** and referral to the CB.

## 6.3 Public Register

The TPSA governance body maintains a **publicly accessible register** of all certified suppliers, including: supplier name, certified scope, TPSA level, certifying body, certificate reference number, issue date, and expiry date. The register also shows any current suspensions or withdrawals.

The register enables clients, auditors, and regulators to verify the validity and scope of any TPSA certification claim in real time. This is the authoritative source; the supplier's own statements are secondary.

# 7. Governance

## 7.1 TPSA Governance Body

The TPSA standard and certification scheme are maintained by a **governance body** responsible for:

- Publication and maintenance of TPSA-01 through TPSA-04.
- Accreditation of certification bodies.
- Development and delivery of the TPSA Auditor Training Programme.
- Maintenance of the public register of certified suppliers.
- Dispute resolution between suppliers and CBs.
- Framework evolution and version management.

The governance body operates independently of any commercial consulting activity. Its funding model is based on CB accreditation fees, auditor training fees, and voluntary contributions. There are no fees charged to suppliers for adopting the standard or using the label — the only cost to suppliers is the certification audit itself, paid to the CB.

## 7.2 Advisory Board

An **Advisory Board** provides guidance on framework evolution. The Board includes representatives from:

- **Suppliers**: at least two certified suppliers (one SME, one large enterprise).
- **Clients**: at least two organisations that use TPSA as part of their third-party risk management.
- **Certification bodies**: at least one accredited CB.
- **Regulators/standards bodies**: observers from relevant regulatory authorities (e.g., ANSSI, ENISA, national financial supervisory authorities) and standards bodies (CIS, ISO national bodies).
- **Independent experts**: cybersecurity practitioners, academics, or legal experts with relevant expertise.

The Advisory Board meets semi-annually and provides non-binding recommendations to the governance body on standard revisions, new mappings, and certification process improvements.

## 7.3 Framework Evolution

TPSA versions follow the semantic versioning conventions defined in TPSA-01 (Section 5.2). Major version changes (e.g., TPSA v1.0 to v2.0) that affect certification criteria trigger a **transition period** during which both versions are accepted:

- **12-month transition** for BASIC level.
- **18-month transition** for ENHANCED and FULL levels.

During the transition period, suppliers certified under the previous version may maintain their certification. At recertification, they must conform to the new version. Minor version updates (e.g., v1.0 to v1.1) do not trigger transition periods and are applied at the next surveillance or recertification audit.

# 8. Fee Structure and Economics

## 8.1 Principle: No Barrier to Adoption

The TPSA framework is **free to adopt**. There is no licence fee, subscription fee, or membership requirement for suppliers to implement TPSA-01 and TPSA-02. The standard documents, JSON schemas, Disclosure Card templates, and the Reference Platform are available at no cost.

The only cost to suppliers is the **certification audit fee**, paid directly to the chosen certification body. This fee is set by the CB according to market conditions, audit duration, and scope complexity. The TPSA governance body does not set or cap audit fees but publishes recommended audit duration guidelines (Section 3.2) to ensure proportionality.

## 8.2 Revenue Streams for the Governance Body

The TPSA governance body is funded through:

- **CB accreditation fees**: one-time accreditation fee + annual renewal. Scaled by CB size.
- **Auditor training fees**: fees for the TPSA Auditor Training Programme.
- **Voluntary contributions**: from supporters, sponsors, and organisations that benefit from the standard.
- **No certification royalties**: the governance body does not take a percentage of CB audit fees. This keeps certification costs low and avoids misaligned incentives.

## 8.3 Indicative Certification Costs

*The following are indicative ranges based on comparable certification schemes (ISO 27001, SOC 2). Actual costs are set by individual CBs.*

| Supplier Size | BASIC (initial) | ENHANCED (initial) | FULL (initial) |
|---|---|---|---|
| **Small** | € 3,000 – € 5,000 | € 6,000 – € 12,000 | € 12,000 – € 20,000 |
| **Medium** | € 5,000 – € 8,000 | € 10,000 – € 20,000 | € 20,000 – € 35,000 |
| **Large** | € 8,000 – € 15,000 | € 18,000 – € 35,000 | € 35,000 – € 60,000+ |

*Surveillance audits are typically 30–50% of initial certification cost. Suppliers with existing ISO 27001 or SOC 2 may benefit from reduced TPSA audit scope and cost (see Section 3.3).*

*TPSA certification costs are determined by the certification body (CB) based on audit duration, scope complexity, and local market conditions. The TPSA governance body does not set, cap, or recommend specific prices.*

*As a general principle, certification costs are comparable to those of existing information security certifications of equivalent audit scope. Suppliers already holding ISO 27001 or SOC 2 certifications may benefit from reduced TPSA audit duration (see Section 3.3), which proportionally reduces cost.*

*The three-level maturity model ensures that certification remains accessible: TPSA Basic, requiring approximately one audit day for a small supplier, represents an entry point that is proportional to the supplier's size and criticality.*

# 9. Transition and Early Adoption

## 9.1 Pre-Certification Period

Before accredited CBs are operational (expected 2027–2028), suppliers may adopt the TPSA framework in a **self-declaration** mode:

- The supplier publishes a conformant Disclosure Card and implements the Risk Dialogue Protocol.
- The supplier declares its self-assessed TPSA level.
- The self-declaration is clearly marked as "**TPSA Self-Declared — Not Independently Certified**" to distinguish it from formal certification.

Self-declaration has no formal audit backing but demonstrates the supplier's commitment and provides immediate value to clients. When CBs become operational, self-declared suppliers may undergo an expedited initial certification audit, leveraging the self-declaration history as evidence of operational maturity.

## 9.2 Pilot Programme

The TPSA governance body will operate a **pilot programme** during the pre-certification period (2026–2027):

- Selected suppliers across different sizes, sectors, and geographies participate as pilot adopters.
- Pilot suppliers publish Disclosure Cards and conduct RSC/SRA exchanges under the TPSA framework.
- Feedback from pilots informs v1.0 refinements before the standard is finalised for formal certification.
- Pilot participants receive a **"TPSA Early Adopter"** designation recognising their contribution, distinct from formal certification.

## 9.3 Roadmap

| Timeline | Milestone |
|---|---|
| **H1 2027** | TPSA Auditor Training Programme development. Engagement with CBs (AFNOR, LSTI, BSI, Bureau Veritas) for accreditation. |
| **H2 2027** | First CB accreditations. Auditor training delivery. Self-declaration to formal certification transition. |
| **2028** | First formally certified TPSA suppliers. Public register operational. Market scaling through DORA/NIS2 regulatory demand. |
| **2029+** | TPSA-03 expansion to non-European frameworks (NIST CSF, APRA CPS 234). Continuous improvement cycle. |

# 10. Conclusion

The TPSA Labelling and Certification Scheme completes the TPSA framework by providing the credibility, verifiability, and market recognition necessary for the standard's adoption. Together, the four TPSA documents form a comprehensive system:

- **TPSA-01** defines what suppliers must disclose.
- **TPSA-02** defines how suppliers and clients dialogue about risk.
- **TPSA-03** proves that the framework covers regulatory requirements.
- **TPSA-04** ensures that claims of conformance are independently verified.

The label is a tool for the market: suppliers use it to differentiate, clients use it to select and monitor, auditors use it to verify, and regulators use it to assess. The TPSA framework's strength lies in this ecosystem — not in any single document, but in the interaction between disclosure, dialogue, mapping, and certification.

### TPSA Framework — Complete Document Set

TPSA Position Paper • TPSA-01 Supplier Disclosure Standard • TPSA-02 Risk Dialogue Protocol • TPSA-03 Regulatory Mapping Matrix • TPSA-04 Labelling & Certification Scheme

Sébastien Poitrasson — CISSP, ISO 27001 Lead Implementer

CIS Supporter — Arthur Koenig Consulting