TPSA

THIRD-PARTY SUPPLIER ACCOUNTABILITY

P O S I T I O N P A P E R

TPSA

Third-Party Supplier Accountability

A Framework for Standardized Security Accountability Between Suppliers and Their Clients

Version 1.0, April 2026

Author: Sébastien Poitrasson, Arthur Koenig Consulting

AK ARTHURKOENIG

Executive Summary

The growing reliance on third-party suppliers for critical IT services has created a systemic vulnerability that current security frameworks fail to adequately address. While standards such as CIS Controls v8, ISO/IEC 27001:2022, and regulatory frameworks including DORA and NIS2 all acknowledge the importance of supply chain security, they approach it exclusively from the client's perspective: assess your suppliers, manage your third-party risk, verify their security posture.

This unilateral approach leaves a fundamental gap. Suppliers are evaluated, questioned, and audited, yet no standardized mechanism exists to make them **accountable** in a structured, transparent, and verifiable manner. Clients send bespoke security questionnaires; suppliers respond with generic assurances. The asymmetry of information persists, and the actual security posture of the supply chain remains opaque.

The **Third-Party Supplier Accountability (TPSA)** framework proposes to close this gap by creating a standardized, bidirectional protocol for security transparency between suppliers and their clients. Rather than imposing additional constraints on suppliers, TPSA provides them with a **competitive advantage**: a label that demonstrates accountability, streamlines client due diligence, and facilitates regulatory compliance with DORA, NIS2, and ISO 27001.

TPSA is not a replacement for existing frameworks. It is a **companion specification** designed to operationalise the third-party security requirements already mandated by these standards, providing the missing link between a client's risk management obligations and a supplier's security transparency.

1. The Problem: An Accountability Gap in Third-Party Security

1.1 The Scale of the Threat

Supply chain attacks have become the preferred vector for sophisticated threat actors. Rather than attacking well-defended organizations directly, adversaries target their suppliers, exploiting the trust relationships, shared infrastructure, and access privileges that define modern digital supply chains.

The Axa XL / Thales “Resilience at Scale” report, published on 2 April 2026, confirms that cyber risk is no longer an isolated threat but a systemic phenomenon that extends well beyond the enterprise perimeter. In 2025, over 12,000 data breaches were recorded worldwide, with an average cost of $4.44 million per incident. ENISA and CISA report a 47% increase in supply chain incidents in 2025, with the trend continuing into 2026.

High-profile incidents continue to demonstrate the cascading impact: a single compromised supplier can paralyse thousands of organizations. The fundamental issue is not that organizations lack security controls, it is that they lack **visibility into and accountability from** the third parties on whom they depend.

1.2 The Current Landscape: Assessment Without Accountability

Existing frameworks and tools address third-party risk from the client side:

- **CIS Controls v8, Safeguard 15** (Service Provider Management): requires organizations to assess and monitor their service providers, but does not define what the provider must disclose or how.
- **ISO/IEC 27001:2022, Annex A.5.19–5.23**: mandates supplier security policies, monitoring, and change management, but leaves the format, depth, and mechanism of supplier communication undefined.
- **DORA (Regulation 2022/2554), Articles 28–30**: imposes detailed requirements on ICT third-party risk management for financial entities, including contractual provisions, but does not standardize the supplier’s response format.
- **NIS2 Directive, Article 21(2)(d)**: requires supply chain security measures, but provides no operational framework for supplier accountability.
- **SIG (Standardized Information Gathering), CAIQ (CSA)**: questionnaire-based assessment tools that rely on supplier self-declaration without standardized verification or ongoing dialogue.
- **SOC 2**: audit-based, periodic, confidential, and focused on the supplier’s general controls, not on the specific assets, data, or risks relevant to a given client.

The result is a fragmented landscape where clients invest significant effort in bespoke assessments, suppliers respond to dozens of different questionnaires with varying formats, and the actual security posture of the supply chain remains poorly understood by both parties.

1.3 The Missing Piece: Structured, Bidirectional Accountability

What is missing is not another assessment tool, but a **standardized accountability protocol** that:

1. Defines what suppliers must disclose, in what format, and at what level of detail.
2. Creates a bidirectional channel through which clients can submit risk scenarios relevant to their own context, and suppliers must respond formally.
3. Maps directly to existing regulatory requirements, so that adoption produces immediate compliance value for both parties.
4. Provides a recognizable label that suppliers can use as a competitive differentiator.

2. The TPSA Framework: Architecture and Components

The Third-Party Supplier Accountability framework consists of four interlocking components, each addressing a specific dimension of the accountability gap.

Component	Name	Purpose
TPSA-01	Supplier Disclosure Standard	Defines the standardised format and mandatory content of the Supplier Disclosure Card.
TPSA-02	Risk Dialogue Protocol	Formalises the bidirectional exchange of risk scenarios between clients and suppliers, leveraging EBIOS RM and MITRE ATT&CK.
TPSA-03	Regulatory Mapping Matrix	Maps every TPSA requirement to CIS Controls v8, ISO 27001:2022, DORA, and NIS2.
TPSA-04	Labelling & Certification	Defines maturity levels, certification criteria, and the audit process for TPSA labelling.

2.1 TPSA-01: Supplier Disclosure Standard

The Supplier Disclosure Card is the foundational document of the TPSA framework. It is a structured, machine-readable declaration published by the supplier, containing the information that clients need to assess and monitor the security of services provided to them.

Mandatory Disclosure Domains

The Disclosure Card covers the following domains, each containing a defined set of mandatory and optional fields:

- **Asset Inventory**: explicit identification of all assets (infrastructure, platforms, applications, data stores) that process, store, or transmit client data. This includes asset classification, location (geographical and logical), and shared/dedicated status.
- **Data Protection Measures**: encryption at rest and in transit, key management practices, data segregation mechanisms for multi-tenant environments, and data retention/deletion policies.
- **Backup & Recovery**: backup frequency, scope, retention periods, tested recovery time objectives (RTO) and recovery point objectives (RPO), and , critically , the date and outcome of the last backup restoration test.
- **Access Control**: authentication mechanisms, privileged access management, access review frequency, and client-facing access controls (APIs, portals, administrative consoles).
- **Vulnerability Management**: patch management policy and SLAs, vulnerability scanning frequency, penetration testing schedule with dates and scope of the most recent test, and remediation timelines.
- **Incident Management**: incident detection capabilities, notification procedures and timelines (aligned with DORA Article 19 requirements where applicable), escalation paths, and post-incident review process.
- **Certification & Compliance Status**: current certifications (ISO 27001, SOC 2, etc.), scope of certification, validity dates, and any known gaps or exclusions.

Shared vs. Client-Specific Disclosures

For suppliers operating multi-tenant environments, the Disclosure Card is structured in two layers: a **common disclosure** covering shared infrastructure and controls applicable to all clients, and a **client-specific annex** detailing the particular assets, data classification, and tailored measures relevant to each individual client relationship.

This two-layer approach minimises the disclosure burden for the supplier while providing each client with the specific transparency they require.

2.2 TPSA-02: Risk Dialogue Protocol

The Risk Dialogue Protocol is the most innovative component of the TPSA framework. It establishes a **formalised, bidirectional channel** through which clients and suppliers can exchange risk-relevant information in a structured format.

The Problem It Solves

Today, a client who identifies a specific threat to their organisation has no standardised way to ask their supplier: “How do your controls address this threat?” The client’s risk analysis and the supplier’s security posture exist in disconnected silos. A bank that identifies an APT group targeting the financial sector cannot formally ask its cloud provider to assess the relevance of that threat to the specific assets hosting the bank’s data.

The Risk Dialogue Protocol solves this by defining a structured exchange mechanism built on two established methodologies:

EBIOS RM Integration

The protocol leverages the EBIOS Risk Manager methodology (published by ANSSI) as the structural backbone for risk dialogue:

- **Workshop 1 (Scope & Context)**: largely pre-populated by the Supplier Disclosure Card (TPSA-01). Assets, business values, and the security baseline are already documented.
- **Workshop 2 (Risk Sources)**: the client identifies their specific risk sources and threat objectives (SR/OV pairs) and submits them to the supplier via the Risk Dialogue Protocol. The supplier may not have considered that their infrastructure is a target for threats specific to the client’s sector.
- **Workshops 3 & 4 (Strategic & Operational Scenarios)**: the client constructs attack scenarios using **MITRE ATT&CK** techniques, mapping them to the supplier’s disclosed assets. The supplier must respond formally: which controls cover each technique, which gaps are identified, and what remediation is planned.
- **Workshop 5 (Risk Treatment)**: the shared analysis produces a joint risk treatment plan, with clear ownership of actions on both sides.

MITRE ATT&CK for Operational Scenarios

Operational scenarios exchanged through the Risk Dialogue Protocol are expressed using MITRE ATT&CK techniques, providing a common, precise, and unambiguous language for describing attack paths. A client can submit a scenario such as: “SR-07 targets the supplier’s public-facing application (T1190), moves laterally via remote services (T1021) to the tenant hosting our data, and exfiltrates via web service (T1567).” The supplier responds with a structured assessment of their controls against each technique.

TIBER-EU and DORA Article 26 Integration

DORA Article 26(4) requires that critical ICT third-party service providers participate in Threat-Led Penetration Testing (TLPT) exercises, aligned with the TIBER-EU framework. The TPSA Risk Dialogue Protocol directly supports this requirement:

- The Supplier Disclosure Card provides the **pre-defined asset perimeter** for TIBER-EU test scoping, eliminating weeks of mapping effort by the threat intelligence provider.
- The Risk Scenario Cards use the same ATT&CK-based format as TIBER-EU threat scenarios, creating a **seamless bridge** between ongoing risk dialogue and periodic penetration testing.
- TLPT results feed back into updated Disclosure Cards and Risk Dialogue responses, creating a **continuous improvement loop**.

Classification Uplift Through Bidirectional Dialogue

A critical emergent property of the TPSA framework is the **classification uplift mechanism**. When a client informs a supplier, through the Disclosure Card feedback process, that certain assets hold data classified at a higher level than the supplier had assessed (e.g., “this storage asset holds data classified as Confidential for our organisation”), the supplier updates its classification. In multi-tenant environments, this uplift benefits all clients hosted on the same infrastructure: the highest classification drives the security posture for shared assets.

This “rising tide” effect inverts the current dynamic where multi-tenant environments default to the lowest common denominator. Under TPSA, they converge toward the highest standard, benefiting all parties, including those who did not initiate the classification uplift.

2.3 TPSA-03: Regulatory Mapping Matrix

Every TPSA requirement is mapped to the corresponding controls or articles in:

- **CIS Controls v8** , particularly Safeguard 15 (Service Provider Management) and related controls across asset management, data protection, access control, and incident response.
- **ISO/IEC 27001:2022** , Annex A controls A.5.19 through A.5.23 (Supplier Relationships), A.5.29–5.30 (ICT Continuity), and supporting controls across all domains.
- **DORA (Regulation 2022/2554)** , Articles 28–30 (ICT Third-Party Risk Management), Article 26 (TLPT/TIBER-EU), Article 19 (Incident Reporting).
- **NIS2 Directive** , Article 21(2)(d) (Supply Chain Security), and related provisions on risk management and incident handling.

This mapping serves a dual purpose. For **clients**, it provides auditable evidence that their third-party risk management meets regulatory requirements, an auditor asking “how do you manage supplier security under NIS2 Article 21?” receives a documented, traceable answer. For **suppliers**, it demonstrates that TPSA certification covers the security transparency requirements of multiple regulatory frameworks simultaneously, reducing the compliance burden of responding to framework-specific questionnaires.

2.4 TPSA-04: Labelling and Certification Scheme

The TPSA label is designed to function as a market signal, analogous to ISO 27001 certification or SOC 2 attestation, but specifically focused on third-party accountability.

Maturity Levels

The labelling scheme defines three levels of maturity:

Level	Requirements	Target Audience
TPSA Basic	Complete Disclosure Card (TPSA-01) with all mandatory domains populated. Annual review.	SME suppliers, non-critical service providers. Entry-level accountability for organisations beginning their TPSA journey.
TPSA Enhanced	Full Disclosure Card plus active Risk Dialogue Protocol (TPSA-02). Demonstrated capacity to receive and respond to client risk scenarios. Semi-annual review.	Mid-tier suppliers, SaaS providers, managed service providers serving regulated clients.
TPSA Full	Complete TPSA-01 and TPSA-02 implementation, including TIBER-EU integration capability. Continuous disclosure updates. Demonstrated classification uplift process.	Critical ICT third-party providers to DORA-regulated entities, major cloud and infrastructure providers.

Certification Process

TPSA certification is performed by accredited third-party auditing bodies (e.g., AFNOR, Bureau Veritas, LSTI, BSI). The TPSA framework defines the audit criteria; accredited bodies perform the assessment and issue the label. This separation ensures independence and leverages established certification infrastructure.

The framework author and associated consultancies may provide advisory, gap analysis, and implementation support, but do not perform certification audits, consistent with the established separation of consulting and certification in the ISO ecosystem.

3. Strategic Positioning

3.1 A Tool for Suppliers, Not a Constraint

The TPSA framework is deliberately positioned as an **enabler for suppliers**, not an imposition by clients. A supplier that adopts TPSA gains:

- **Competitive differentiation**: the ability to tell prospects “we are TPSA-certified” replaces dozens of bespoke security questionnaires with a single, recognised credential.
- **Reduced due diligence overhead**: instead of responding to unique questionnaires from each client, the supplier maintains a standardised Disclosure Card that satisfies common requirements.
- **Regulatory alignment**: TPSA certification demonstrates coverage of DORA, NIS2, and ISO 27001 third-party requirements, opening doors to regulated markets (banking, insurance, energy, healthcare).
- **Client trust**: the bidirectional Risk Dialogue Protocol shows that the supplier takes client-specific risks seriously, building deeper trust and longer-lasting commercial relationships.

3.2 European-First, Globally Relevant

TPSA’s initial positioning is European, driven by the regulatory momentum of DORA (effective January 2025) and NIS2 (transposition deadline October 2024, enforcement ongoing). These regulations create an immediate and concrete demand for standardised third-party accountability. However, the framework is designed to be regulation-agnostic in its core architecture: the Disclosure Card format, the Risk Dialogue Protocol, and the labelling scheme are universally applicable. Mappings to non-European frameworks (NIST CSF, NIST C-SCRM, SOX, APRA CPS 234) can be added as the framework matures and adoption extends beyond the European market.

3.3 Complementary, Not Competitive

TPSA does not compete with existing standards or tools. It occupies a specific niche that none of them currently fill:

Existing Tool	What It Does	What TPSA Adds
CIS Controls v8	Tells the client what to do about supplier risk (Safeguard 15).	Tells the supplier how to demonstrate accountability in a standardised format.
ISO 27001	Requires supplier security policies and monitoring.	Provides the operational protocol and format for that monitoring.
SOC 2	Periodic, confidential audit of supplier controls.	Continuous, transparent, client-oriented disclosure with bidirectional risk dialogue.
SIG / CAIQ	Standardised questionnaires for supplier assessment.	Standardised disclosures initiated by the supplier, plus a mechanism for ongoing risk dialogue.
DORA / NIS2	Regulatory obligations on third-party risk management.	An operational framework to satisfy those obligations with documented, auditable evidence.

4. Conclusion and Call for Contribution

The TPSA framework addresses a structural gap in the cybersecurity landscape: the absence of a standardised, bidirectional accountability mechanism between suppliers and their clients. By shifting the paradigm from client-driven assessment to supplier-initiated disclosure and mutual risk dialogue, TPSA creates value for all stakeholders:

- **Suppliers** gain a competitive label, reduced questionnaire fatigue, and alignment with multiple regulatory frameworks.
- **Clients** gain standardised, auditable evidence of third-party security management, bidirectional risk dialogue capabilities, and a classification uplift mechanism for shared environments.
- **Regulators and auditors** gain a traceable, verifiable framework for assessing compliance with DORA, NIS2, and ISO 27001 third-party requirements.
- **The ecosystem** gains a rising-tide effect where the highest classification standards in multi-tenant environments benefit all participants.

This position paper is an invitation to the cybersecurity community, practitioners, regulators, standards bodies, suppliers, and clients, to contribute to the development of the TPSA framework. The standard will be shaped by the input of those who will use it.

Contact & Contributions

Sébastien Poitrasson , CISSP, ISO 27001 Lead Implementer
CIS Supporter , Arthur Koenig Consulting

Appendix A: Glossary

Term	Definition
TPSA	Third-Party Supplier Accountability. The framework defined in this document.
Disclosure Card	A structured, standardised document published by a supplier under TPSA-01, describing their security posture relevant to client data and services.
Risk Scenario Card	A formalised threat scenario submitted by a client to a supplier under TPSA-02, using EBIOS RM structure and MITRE ATT&CK techniques.
Risk Dialogue Protocol	The bidirectional exchange mechanism defined in TPSA-02 for structured risk communication between clients and suppliers.
Classification Uplift	The mechanism by which a client's higher data classification on shared assets drives the supplier to elevate security controls, benefiting all tenants.
EBIOS RM	Expression des Besoins et Identification des Objectifs de Sécurité , Risk Manager. The risk analysis methodology published by ANSSI (France).
TIBER-EU	Threat Intelligence-Based Ethical Red Teaming. The European framework for threat-led penetration testing, referenced in DORA Article 26.
TLPT	Threat-Led Penetration Testing, as defined in DORA Articles 26–27.