TPSA

THIRD-PARTY SUPPLIER ACCOUNTABILITY

T P S A - 0 2

Risk Dialogue Protocol

Third-Party Supplier Accountability Framework

Specification Document

Bidirectional Risk Communication Between Suppliers and Clients

Version 1.0 April 2026

Author: Sébastien Poitrasson, Arthur Koenig Consulting

AK ARTHURKOENIG

The KRI Exchange adds a quantitative, continuous monitoring layer to the Risk Dialogue Protocol. While Risk Scenario Cards (RSC) are episodic exercises that assess the supplier's posture against specific threat scenarios, KRIs provide ongoing, measurable signals of the supplier's operational security health as it relates to client data and services.

1. Introduction

1.1 Purpose

This document defines the **TPSA-02: Risk Dialogue Protocol**, the second component of the Third-Party Supplier Accountability framework. It specifies the mechanisms, formats, processes, and timelines for **bidirectional risk communication** between a supplier and its clients.

The Risk Dialogue Protocol addresses a fundamental gap in current third-party risk management: the absence of a standardised channel through which clients can communicate their specific threat landscape to their suppliers, and suppliers can respond with structured, verifiable assessments of their defensive posture against those threats.

While TPSA-01 (Supplier Disclosure Standard) establishes the supplier's baseline security transparency, TPSA-02 creates a **living dialogue** that adapts to evolving threats, client-specific risk contexts, and regulatory requirements including DORA's Threat-Led Penetration Testing (TLPT/TIBER-EU) provisions.

1.2 Scope

TPSA-02 applies to all suppliers holding or pursuing TPSA certification at **ENHANCED** or **FULL** level. Suppliers at BASIC level are not required to implement the Risk Dialogue Protocol but may choose to do so voluntarily.

The protocol covers three types of exchanges: **Risk Scenario Cards** (client-initiated threat scenarios), **Supplier Risk Assessments** (supplier responses), and **TIBER-EU Coordination Messages** (specific to DORA-regulated contexts). Each exchange type has a defined format, lifecycle, and timeline.

1.3 Relationship to Other TPSA Components

- **TPSA-01**: the Risk Dialogue Protocol depends on the Supplier Disclosure Card as its baseline data source. Risk scenarios reference assets, controls, and classifications documented in the Disclosure Card.
- **TPSA-03**: regulatory mappings identify which Risk Dialogue Protocol elements satisfy specific DORA, NIS2, and ISO 27001 requirements.
- **TPSA-04**: the Labelling & Certification Scheme defines the maturity level at which the Risk Dialogue Protocol becomes mandatory, and the audit criteria for assessing protocol implementation.

1.4 Normative References

In addition to the normative references listed in TPSA-01, the following are specific to TPSA-02:

- **EBIOS Risk Manager** (ANSSI, 2018) — Workshops 1–5 structure and terminology.
- **MITRE ATT&CK® Enterprise** (current version) — Tactics, techniques, and sub-techniques for operational scenario description.
- **MITRE ATT&CK® for ICS** (current version) — For suppliers providing industrial control system (ICS/OT) services.
- **TIBER-EU Framework** (ECB, 2018; updated 2024) — Threat Intelligence-Based Ethical Red Teaming methodology.
- **DORA Regulation 2022/2554** — Articles 26–27 (Threat-Led Penetration Testing), Article 28–30 (ICT Third-Party Risk Management).
- **STIX 2.1** (OASIS) — Structured Threat Information Expression, for threat intelligence exchange format.

2. Protocol Architecture

2.1 Overview

The Risk Dialogue Protocol operates as a structured, asynchronous, bidirectional exchange channel between a client and a supplier. It is not a real-time communication system but a **formal protocol for exchanging risk-relevant documents** with defined formats, acknowledgement requirements, and response timelines.

Exchange Type	Initiator	Responder	Purpose
Risk Scenario Card (RSC)	Client	Supplier	Client submits a threat scenario specific to their context and asks the supplier to assess its defensive posture against it.
Supplier Risk Assessment (SRA)	Supplier	Client	Supplier responds formally to a Risk Scenario Card with a structured assessment of controls, gaps, and remediation plans.
TIBER-EU Coordination (TEC)	Either party	Either party	Coordination messages for TLPT/TIBER-EU exercises involving the supplier. Scoping, scheduling, results sharing, remediation tracking.
Classification Uplift Request (CUR)	Client	Supplier	Client notifies the supplier of a higher data classification on specific assets (as defined in TPSA-01, Section 4).
Key Risk Indicator Exchange (KRI)	Supplier (publication) / Client (request)	Either party	Continuous quantitative monitoring of the supplier's risk posture through standardised indicators. Enables early warning and targeted RSC triggering when thresholds are breached.

2.2 Channel Requirements

All exchanges under the Risk Dialogue Protocol must traverse a **secure, authenticated channel** that ensures confidentiality, integrity, and non-repudiation.

Authentication

Both parties authenticate using **ED25519 certificate pairs**, consistent with the Disclosure Card signing mechanism defined in TPSA-01 (field H-13). Each party holds a private key and has registered the corresponding public key with the other party. Every message is signed by the sender and verified by the receiver.

Confidentiality

Messages are encrypted in transit using TLS 1.3 (minimum) for network-level protection. Message payloads are additionally encrypted using the recipient's public key (NaCl/libsodium crypto_box or equivalent), ensuring end-to-end confidentiality even if the transport layer is compromised or messages traverse intermediary systems.

Transport Agnosticism

The protocol is **transport-agnostic**. Messages may be exchanged via:

- The **TPSA Reference Platform** API (REST endpoints defined in Section 7, project).
- A supplier's proprietary portal implementing the TPSA message format.
- **Encrypted email** (PGP/S/MIME) with attached JSON payloads, for environments where API integration is not feasible.
- **Offline exchange** (signed JSON files on encrypted media), for air-gapped or highly restricted environments.

Regardless of transport, the **message format and lifecycle** remain identical. Conformance is assessed on format and process, not on transport mechanism.

2.3 Message Lifecycle

Every exchange follows a five-state lifecycle:

State	Transition	Description
DRAFT	Author creates	Message is being composed. Not yet transmitted. May be reviewed internally before submission.
SUBMITTED	Author sends	Message is transmitted to the counterparty. The acknowledgement timer begins.
ACKNOWLEDGED	Receiver confirms receipt	The receiver has confirmed receipt and accepted the message for processing. The response timer begins.
RESPONDED	Responder sends response	A formal response (SRA, CUR response, TEC update) has been sent. The initiator reviews.
CLOSED	Initiator accepts or escalates	The exchange is closed. Both parties retain the full exchange record for audit and compliance purposes.

2.4 Timelines

Action	BASIC	ENHANCED	FULL
Acknowledgement	N/A (protocol not required)	10 business days	5 business days
Response to RSC	N/A	30 business days	15 business days
Response to CUR	N/A	30 business days	15 business days
TEC Scoping Response	N/A	20 business days	10 business days
Escalation (no response)	N/A	After response deadline + 10 days	After response deadline + 5 days

Timelines are measured in business days from the date of submission (for acknowledgement) or acknowledgement (for response). Escalation procedures are defined in Section 6.

3. Risk Scenario Card (RSC)

3.1 Purpose and Rationale

The Risk Scenario Card is the primary instrument through which a client communicates a **specific, contextualised threat** to a supplier and requests a formal assessment of the supplier's defensive posture against that threat.

The RSC is fundamentally different from a security questionnaire. A questionnaire asks generic questions ("Do you encrypt data at rest?"). An RSC presents a **concrete attack scenario** relevant to the client's threat landscape and asks the supplier to map its defences against each step of the attack path. This forces a level of specificity and honesty that generic questionnaires cannot achieve.

3.2 EBIOS RM Alignment

The RSC is structured around the EBIOS Risk Manager methodology (ANSSI), adapted for the client-supplier context. Each RSC maps to specific EBIOS RM workshops:

EBIOS Workshop	EBIOS RM Function	TPSA Mapping	Source
WS1 Scope	Define scope, business values, assets, existing security baseline.	Pre-populated from the Supplier Disclosure Card (TPSA-01). No additional input needed for the RSC.	Supplier (via TPSA-01)
WS2 Risk Sources	Identify risk sources (SR) and their objectives/motivations (OV).	RSC Section A: Risk Source Identification. The client identifies SR/OV pairs relevant to their context.	Client
WS3 Strategic Scenarios	Build high-level attack scenarios: SR → target → feared event.	RSC Section B: Strategic Scenario. The client describes the high-level attack path through the supplier's environment.	Client
WS4 Operational Scenarios	Detail technical attack paths using specific techniques.	RSC Section C: Operational Scenario (MITRE ATT&CK). The client maps the attack to specific ATT&CK techniques on the supplier's assets.	Client
WS5 Risk Treatment	Define risk treatment measures and residual risk.	Supplier Risk Assessment (SRA) response. Joint risk treatment plan.	Supplier (SRA) + Joint

3.3 RSC Structure

A Risk Scenario Card is a JSON document composed of a header and three sections (A, B, C), each corresponding to EBIOS RM workshops 2, 3, and 4.

RSC Header

ID	Field	Type	Req.	Description
RSC-H01	**RSC Identifier**	UUID	M	Unique identifier for this Risk Scenario Card.
RSC-H02	**Client Name**	String	M	Name of the client submitting the scenario.
RSC-H03	**Client Contact**	Object	M	Security contact for this RSC: name, role, email, PGP key.
RSC-H04	**Target Supplier**	String	M	Name of the supplier (must match TPSA-01 H-01).
RSC-H05	**Disclosure Card Ref**	String	M	Reference to the Disclosure Card version against which this scenario is constructed (TPSA-01 H-03).
RSC-H06	**Submission Date**	ISO 8601	M	Date of submission.
RSC-H07	**Priority**	Enum	M	CRITICAL, HIGH, MEDIUM, LOW. Determines response timeline weighting.
RSC-H08	**Regulatory Context**	Array	C	Applicable regulations driving this RSC (e.g., DORA Art. 28, NIS2 Art. 21). Mandatory when the RSC is regulatory-driven.
RSC-H09	**TIBER-EU Flag**	Boolean	C	Whether this RSC is part of or preparatory to a TIBER-EU/TLPT exercise. Triggers TIBER-EU-specific handling (Section 5).
RSC-H10	**Digital Signature**	ED25519	M	Client’s signature on the RSC content.

Section A: Risk Source Identification (EBIOS WS2)

This section identifies the threat actors and their objectives relevant to the client's context. The client is not asking the supplier to identify threats — the client is **informing the supplier** of the threats that concern them and that may transit through the supplier's environment.

ID	Field	Type	Req.	Description
RSC-A01	**Risk Sources**	Array	M	List of risk sources (SR). Each entry includes: SR identifier (e.g., SR-01), SR type (State-sponsored, Organised Crime, Hacktivist, Insider, Competitor, Opportunistic), SR name or description, known TTPs or affiliations (e.g., APT group designation), and motivation/objective summary.
RSC-A02	**Target Objectives**	Array	M	For each SR, the feared objectives (OV): data exfiltration, service disruption, espionage, ransomware deployment, supply chain compromise, reputational damage, etc.
RSC-A03	**Sector Context**	Text	M	Brief description of the client's sector, regulatory environment, and why these specific risk sources are relevant (e.g., "Financial institution subject to DORA, targeted by APT38 for SWIFT-related fraud").
RSC-A04	**Threat Intel References**	Array	O	References to threat intelligence sources supporting the risk source identification: CERT advisories, STIX bundles, vendor threat reports, internal CTI.

Section B: Strategic Scenario (EBIOS WS3)

This section describes the high-level attack path: how the risk source reaches its objective by transiting through the supplier's environment. It connects the threat actor to the client's feared event via the supplier's assets.

ID	Field	Type	Req.	Description
RSC-B01	**Scenario Title**	String	M	Short descriptive title (e.g., "APT exfiltration via SaaS platform API").
RSC-B02	**Entry Point**	Reference	M	The supplier asset(s) targeted for initial access. Must reference asset IDs from the Disclosure Card (TPSA-01, D1-01).
RSC-B03	**Attack Path**	Text	M	Narrative description of the strategic attack path: initial access → lateral movement → objective. Describes how the attacker moves from entry point to the client's data or service.
RSC-B04	**Target Assets**	Array	M	The supplier asset(s) where the feared event materialises (data store, application, network segment). References TPSA-01 D1-01.
RSC-B05	**Feared Event**	Text	M	The impact on the client if the scenario succeeds: data breach, service outage, integrity compromise, regulatory sanction, etc.
RSC-B06	**Likelihood Estimate**	Enum	O	Client's assessment of scenario likelihood: VERY HIGH, HIGH, MEDIUM, LOW, VERY LOW. Based on threat intelligence and sector exposure.
RSC-B07	**Impact Estimate**	Enum	M	Client's assessment of potential impact: CRITICAL, HIGH, MEDIUM, LOW.

Section C: Operational Scenario — MITRE ATT&CK Mapping (EBIOS WS4)

This section translates the strategic scenario into a **technical attack path** using MITRE ATT&CK® techniques. Each step of the attack is mapped to a specific ATT&CK technique (or sub-technique), a target asset from the Disclosure Card, and the expected defensive control. This is the section that forces the most precise and actionable supplier response.

ID	Field	Type	Req.	Description
RSC-C01	**Attack Steps**	Array	M	Ordered list of attack steps. Each step includes: step number, ATT&CK Technique ID (e.g., T1190), ATT&CK Technique name, ATT&CK Tactic (e.g., Initial Access), target asset ID (from TPSA-01 D1-01), description of how the technique is applied in this scenario context.
RSC-C02	**ATT&CK Matrix**	Enum	M	Which ATT&CK matrix is used: ENTERPRISE or ICS. Must match the nature of the supplier's environment.
RSC-C03	**Kill Chain Mapping**	Object	O	Optional mapping of attack steps to Lockheed Martin Cyber Kill Chain phases for additional strategic context.
RSC-C04	**Detection Expectations**	Array	O	For each attack step, the client's expectation of the supplier's detection capability: DETECT, PARTIAL, BLIND, UNKNOWN.
RSC-C05	**Specific Questions**	Array	O	Free-form questions the client wants the supplier to address for specific attack steps (e.g., "For step 3 (T1021.002): do you monitor RDP sessions to the database segment?").

4. Supplier Risk Assessment (SRA)

4.1 Purpose

The Supplier Risk Assessment is the **formal response** to a Risk Scenario Card. It is not a generic compliance statement but a **point-by-point assessment** of the supplier's controls against each step of the client's operational scenario. The SRA is the document that transforms the TPSA from an information-sharing exercise into an **accountability mechanism**.

4.2 SRA Structure

SRA Header

ID	Field	Type	Req.	Description
SRA-H01	**SRA Identifier**	UUID	M	Unique identifier for this Supplier Risk Assessment.
SRA-H02	**RSC Reference**	UUID	M	Reference to the Risk Scenario Card being responded to (RSC-H01).
SRA-H03	**Response Date**	ISO 8601	M	Date of this response.
SRA-H04	**Assessor**	Object	M	Name, role, and qualifications of the person(s) who performed the assessment.
SRA-H05	**Assessment Scope**	Text	M	Confirmation that the assessment covers all attack steps in the RSC, or explicit declaration of which steps could not be assessed and why.
SRA-H06	**Digital Signature**	ED25519	M	Supplier's signature on the SRA content.

SRA Body: Per-Step Assessment

The core of the SRA is a **step-by-step response** to each attack step defined in the RSC's Section C. For each attack step, the supplier provides:

ID	Field	Type	Req.	Description
SRA-S01	**Step Reference**	Integer	M	The attack step number from the RSC being addressed.
SRA-S02	**ATT&CK Technique**	String	M	Confirmation of the ATT&CK technique ID being assessed (must match RSC-C01).
SRA-S03	**Control Status**	Enum	M	COVERED: existing controls address this technique. PARTIAL: controls exist but with known limitations. GAP: no effective control in place. NOT_APPLICABLE: the technique cannot be applied in this environment (must be justified).
SRA-S04	**Controls Description**	Text	M	Detailed description of the specific controls addressing this technique: technology,

				configuration, monitoring rules, detection logic, response procedures.
SRA-S05	**Detection Capability**	Enum	M	DETECT: the supplier's monitoring would identify this technique in use. PARTIAL: detection is possible but not certain (e.g., depends on volume, timing). BLIND: no detection capability for this specific technique.
SRA-S06	**Evidence Reference**	Array	C	References to evidence supporting the control status: configuration screenshots, monitoring rule IDs, audit log samples, test results. Mandatory when Control Status = COVERED.
SRA-S07	**Gap Analysis**	Text	C	For PARTIAL or GAP status: description of the gap, root cause, and risk exposure. Mandatory when Control Status ≠ COVERED.
SRA-S08	**Remediation Plan**	Object	C	For PARTIAL or GAP status: planned remediation action, responsible party, target completion date, and interim/compensating controls. Mandatory when Control Status ≠ COVERED.

SRA Summary

ID	Field	Type	Req.	Description
SRA-R01	**Overall Assessment**	Enum	M	Aggregated assessment: ADEQUATE (all steps COVERED or NOT_APPLICABLE), PARTIALLY_ADEQUATE (mix of COVERED and PARTIAL), INADEQUATE (one or more GAPs on critical steps).
SRA-R02	**Coverage Statistics**	Object	M	Number of steps by status: COVERED, PARTIAL, GAP, NOT_APPLICABLE.
SRA-R03	**Residual Risk Statement**	Text	M	Supplier's assessment of the residual risk after accounting for existing controls and planned remediations.
SRA-R04	**Remediation Roadmap**	Array	C	Consolidated list of all remediation actions across all steps, with priorities and timeline. Mandatory when any step has PARTIAL or GAP status.
SRA-R05	**Recommendations**	Text	O	Supplier's recommendations to the client for risk reduction on the client side (e.g., additional access controls, monitoring, contractual provisions).
SRA-R06	**Disclosure Card Update**	Boolean	M	Whether the SRA findings will trigger an update to the Supplier Disclosure Card (TPSA-01). If yes, expected update version and date.

5. TIBER-EU / TLPT Integration

5.1 Regulatory Context

DORA Article 26(4) requires that critical ICT third-party service providers **participate in threat-led penetration testing (TLPT)** exercises conducted by their clients, in accordance with the TIBER-EU framework. This creates a legal obligation for supplier cooperation in simulated attack exercises.

The TPSA Risk Dialogue Protocol provides the **operational infrastructure** for this cooperation, reducing the coordination overhead from weeks of ad hoc negotiation to a structured, pre-defined process.

5.2 TIBER-EU Coordination Messages (TEC)

The TIBER-EU Coordination Message is a specific exchange type within the Risk Dialogue Protocol, designed to support the three phases of a TIBER-EU exercise:

Phase 1: Scoping (TEC-SCOPE)

The client (or the client's Threat Intelligence provider) submits a TEC-SCOPE message to the supplier. This message leverages the Disclosure Card to define the test perimeter:

- **Target assets**: selected from the Disclosure Card D1-01 asset register, already identified with location, hosting model, and classification.
- **In-scope services**: the supplier services to be included in the TLPT exercise.
- **Excluded assets/services**: any supplier assets explicitly excluded from testing, with justification.
- **Test window**: proposed dates and times for the exercise.
- **Rules of engagement**: agreed boundaries, escalation procedures, and communication protocols during the test.

Because the Disclosure Card already provides a structured, up-to-date asset inventory, the scoping phase is **dramatically accelerated**. The Threat Intelligence provider does not need to perform reconnaissance to identify the supplier's assets — they are already documented.

Phase 2: Execution (TEC-EXEC)

During the TLPT exercise, TEC-EXEC messages may be exchanged for:

- **Incident coordination**: if the supplier's SOC detects the red team activity and escalates, the exercise coordinators may need to communicate to prevent disruption.
- **Scope adjustments**: if the red team identifies assets not in the original scope that are relevant, the scope may be expanded via a TEC-EXEC amendment.
- **Safety signals**: if the red team encounters production risks, a safety signal can pause the exercise.

Phase 3: Results & Remediation (TEC-RESULTS)

After the exercise, the TEC-RESULTS message formalises the findings:

- **Findings mapped to ATT&CK techniques**: using the same format as the RSC/SRA exchange, ensuring consistency and traceability.
- **Detection performance**: which techniques were detected by the supplier's SOC, which were missed, and at what stage.
- **Remediation plan**: using the SRA remediation format (SRA-S08), with target dates and responsible parties.
- **Disclosure Card update trigger**: findings that change the supplier's security posture or asset classification trigger a TPSA-01 update.

The TEC-RESULTS message creates a **feedback loop** between TIBER-EU exercises and the ongoing Disclosure Card/Risk Dialogue process. Penetration testing is no longer a point-in-time exercise but part of a continuous accountability cycle.

5.3 Pre-existing RSCs as TIBER-EU Input

A key efficiency of the TPSA framework is that **Risk Scenario Cards already submitted and assessed can serve as input for TIBER-EU test design**. If a client has previously submitted an RSC describing an APT scenario and received an SRA showing partial coverage, the TIBER-EU Threat Intelligence provider can use that scenario as a starting point for the TLPT exercise, specifically targeting the identified gaps. This creates continuity between ongoing risk dialogue and periodic penetration testing, ensuring that TLPT exercises are not designed in isolation but are informed by the actual risk context documented through the TPSA process.

6. Key Risk Indicator (KRI) Exchange

6.1 Purpose

The KRI Exchange adds a quantitative, continuous monitoring layer to the Risk Dialogue Protocol. While Risk Scenario Cards (RSC) are episodic exercises that assess the supplier's posture against specific threat scenarios, KRIs provide ongoing, measurable signals of the supplier's operational security health as it relates to client data and services.

KRIs serve three functions within the TPSA framework. First, they provide **continuous visibility**: clients receive regular, standardised metrics without requiring a full RSC/SRA cycle. Second, they act as **early warning triggers**: a KRI that breaches a defined threshold may prompt the client to submit a targeted RSC to investigate the underlying issue. Third, they create a **shared language for risk appetite**: by agreeing on KRI definitions and thresholds, client and supplier establish a quantitative baseline for what constitutes acceptable risk.

6.2 KRI Structure

Each KRI is defined using a standardised format:

ID	Field	Type	Req.	Description
KRI-01	KRI Identifier	String	M	Unique identifier for this indicator (e.g., KRI-VULN-001).
KRI-02	Category	Enum	M	Domain alignment: ASSET_MGMT, DATA_PROTECTION, BACKUP, ACCESS_CONTROL, VULNERABILITY, INCIDENT, COMPLIANCE. Maps to TPSA-01 domains D1–D7.
KRI-03	Metric Name	String	M	Human-readable name (e.g., "Critical vulnerability remediation rate within SLA").
KRI-04	Metric Definition	Text	M	Precise definition of the metric: what is measured, how it is calculated, data source, and measurement perimeter.
KRI-05	Unit	String	M	Unit of measurement (percentage, count, hours, days, ratio).
KRI-06	Frequency	Enum	M	Reporting frequency: REAL_TIME, DAILY, WEEKLY, MONTHLY, QUARTERLY.
KRI-07	Current Value	Number	M	Most recent measured value.
KRI-08	Measurement Date	ISO 8601	M	Date/time of the most recent measurement.
KRI-09	Threshold - Acceptable	Number	M	The value at or below/above which the indicator is considered within acceptable risk appetite.
KRI-10	Threshold - Warning	Number	C	The value at which the indicator signals elevated risk. Triggers attention but not escalation. Mandatory at FULL level.
KRI-11	Threshold - Critical	Number	C	The value at which the indicator signals unacceptable risk and should trigger an RSC or immediate dialogue. Mandatory at FULL level.
KRI-12	Trend	Enum	O	Trend over the last 3 measurement periods: IMPROVING, STABLE, DEGRADING.
KRI-13	Commentary	Text	O	Supplier's contextual commentary on the current value (e.g., explaining a temporary degradation due to a planned migration).

6.3 Baseline KRIs

The following KRIs are **recommended as a baseline set**. Suppliers at ENHANCED level must publish at least 5 of these; suppliers at FULL level must publish all of them. Additional KRIs may be defined by mutual agreement between client and supplier.

KRI ID	Category	Metric	Recommended Threshold (Acceptable)
KRI-VULN-001	VULNERABILITY	Percentage of critical vulnerabilities remediated within SLA (24h)	≥ 95%
KRI-VULN-002	VULNERABILITY	Percentage of high vulnerabilities remediated within SLA (72h)	≥ 90%
KRI-VULN-003	VULNERABILITY	Number of unpatched critical/high vulnerabilities older than SLA	0
KRI-BACKUP-001	BACKUP	Last successful backup restoration test (days ago)	≤ 90 days
KRI-BACKUP-002	BACKUP	Backup success rate (last 30 days)	≥ 99.5%
KRI-ACCESS-001	ACCESS_CONTROL	Percentage of privileged accounts with MFA enabled	100%
KRI-ACCESS-002	ACCESS_CONTROL	Days since last access rights review	≤ 90 days
KRI-INCIDENT-001	INCIDENT	Mean time to detect (MTTD) for critical/high alerts (hours)	≤ 1 hour
KRI-INCIDENT-002	INCIDENT	Number of security incidents affecting client data (last 90 days)	Context-dependent
KRI-AVAIL-001	ASSET_MGMT	Service availability (last 30 days)	≥ 99.9%
KRI-COMPLIANCE-001	COMPLIANCE	Days until next certification expiry	≥ 90 days

6.4 KRI Publication and Client-Requested KRIs

Supplier-published KRIs are included in the Disclosure Card (TPSA-01) as an appendix or in the Client-Specific Annex. They are updated at the frequency defined in KRI-06. For suppliers using the TPSA Reference Platform, KRIs are exposed via a dedicated API endpoint.

Client-requested KRIs: a client may request additional KRIs specific to their risk context through the Risk Dialogue Protocol. The request follows the standard message lifecycle (SUBMITTED → ACKNOWLEDGED → RESPONDED → CLOSED). The supplier responds by either accepting the KRI (with proposed definition and threshold), proposing an alternative metric, or declining with justification. Agreed KRIs are added to the Client-Specific Annex.

6.5 KRI Breach and Escalation

When a KRI crosses the **Warning threshold**, the supplier should proactively notify affected clients and provide commentary (KRI-13) explaining the situation and expected remediation timeline.

When a KRI crosses the **Critical threshold**, the supplier must notify affected clients within the timelines defined in Section 2.4 (acknowledgement timelines). The client may treat a Critical KRI breach as grounds for submitting a targeted RSC focused on the affected domain.

Persistent KRI degradation (3 or more consecutive measurement periods in Warning or Critical status) is reportable at the next TPSA surveillance audit and may be considered in the certification body's conformance assessment.

7. Escalation and Dispute Resolution

7.1 Non-Response Escalation

If a supplier fails to acknowledge or respond within the timelines defined in Section 2.4, the following escalation path applies:

1. **Reminder**: the client sends a formal reminder referencing the original submission and the elapsed time. The reminder resets the response timer for one additional cycle.
2. **Escalation Notice**: if no response is received after the reminder cycle, the client issues an Escalation Notice to the supplier's designated compliance contact (TPSA-01, H-12). The notice is logged as a protocol violation.
3. **TPSA Conformance Impact**: repeated or unresolved escalation notices are reportable to the TPSA certification auditor and may affect the supplier's TPSA label status at the next certification review.

The escalation process is designed to be proportionate. A single missed deadline is handled as an operational issue. A pattern of non-responsiveness is a conformance issue that affects the supplier's label.

7.2 Content Disputes

If the client disagrees with the content of a Supplier Risk Assessment (e.g., the client believes a control status of COVERED is overstated), the following process applies:

4. **Clarification Request**: the client submits a follow-up message requesting additional evidence or justification for the disputed assessment.
5. **Joint Review**: if clarification is insufficient, either party may request a joint review session (documented via TEC message format) to discuss the disputed assessment.
6. **Independent Assessment**: for unresolved disputes, either party may engage an independent assessor (mutually agreed or appointed by the TPSA certification body) to provide a binding opinion on the disputed control status.

The dispute resolution process is deliberately lightweight at the early stages. Most disagreements should be resolved through clarification and evidence sharing, without requiring independent assessment.

8. Conformance Requirements

8.1 Supplier Conformance (ENHANCED Level)

A supplier at TPSA ENHANCED level must:

- Accept RSC submissions from any client with a valid Client-Specific Annex.
- Acknowledge RSCs within 10 business days.
- Respond with a complete SRA within 30 business days of acknowledgement.
- Maintain a log of all exchanges, accessible to the TPSA certification auditor.
- Designate a named contact responsible for Risk Dialogue Protocol operations.
- Support at least one of the defined transport mechanisms (API, encrypted email, or offline exchange).

8.2 Supplier Conformance (FULL Level)

In addition to ENHANCED requirements, a supplier at TPSA FULL level must:

- Acknowledge RSCs within 5 business days.
- Respond with a complete SRA within 15 business days.
- Support TIBER-EU Coordination Messages (TEC) and demonstrate readiness to participate in TLPT exercises.
- Implement the TPSA Reference Platform API or a conformant equivalent.
- Trigger Disclosure Card updates (TPSA-01) within 15 days when SRA findings reveal material changes to the security posture.

8.3 Client Obligations

The Risk Dialogue Protocol places obligations on clients as well:

- RSCs must be **well-formed**: complete, referenced to specific Disclosure Card assets, and using valid ATT&CK techniques. Suppliers may reject malformed RSCs with a request for correction.
- RSCs must be **proportionate**: the number of RSCs submitted should be proportional to the criticality of the supplier relationship. The TPSA certification scheme may define recommended annual RSC limits by supplier criticality tier.
- Clients must close exchanges (transition to CLOSED state) within 30 days of receiving an SRA, or submit a clarification request.
- Threat intelligence shared in RSCs must be handled with appropriate confidentiality by both parties.

Appendix A: Example Risk Scenario Card

Fictitious example: a banking client submits an RSC to the SaaS provider CloudWorks SAS (from the TPSA-01 example) concerning an APT-driven data exfiltration scenario.

RSC Header

Field	Value
RSC Identifier	f47ac10b-58cc-4372-a567-0e02b2c3d479
Client Name	Banque Européenne d'Investissement et de Commerce (BEIC)
Target Supplier	CloudWorks SAS
Disclosure Card Ref	CloudWorks Common Disclosure v1.2.0 (2026-04-01)
Priority	HIGH
Regulatory Context	DORA Art. 28 (ICT third-party risk), DORA Art. 26 (TLPT readiness)
TIBER-EU Flag	false (standalone RSC, not part of a TLPT exercise at this stage)

Section A: Risk Source Identification

SR ID	Type	Description	Objective (OV)
SR-01	State-sponsored	APT38 (Lazarus sub-group)	Financial theft and data exfiltration targeting banking clients. Known to compromise third-party service providers to access client financial data and internal documents.
SR-02	Organised Crime	FIN7	Ransomware deployment and data extortion via supply chain compromise. Known to target SaaS platforms serving financial institutions.

Sector Context: BEIC is a DORA-regulated credit institution. The CloudWorks DMP platform stores internal compliance documents, audit reports, and client correspondence. Compromise of this data could result in regulatory sanctions, competitive intelligence leakage, and reputational damage.

Section B: Strategic Scenario

Field	Value
Scenario Title	APT exfiltration of banking compliance documents via CloudWorks API
Entry Point	CW-SRV-01 (DMP App Cluster) — public-facing API gateway
Attack Path	SR-01 exploits a vulnerability in the CloudWorks API gateway (CW-SRV-01) to gain initial access. The attacker pivots from the application cluster to the primary database (CW-DB-01) to identify BEIC's tenant data, then moves to document storage (CW-STO-01) to exfiltrate encrypted client documents. The attacker either decrypts documents using compromised key material or exfiltrates encrypted blobs for offline decryption.
Target Assets	CW-DB-01 (metadata, tenant mapping), CW-STO-01 (client documents)
Feared Event	Exfiltration of BEIC internal compliance documents and client correspondence. Regulatory notification required under DORA Art. 19. Potential CSSF sanctions. Reputational impact with institutional clients.
Impact Estimate	CRITICAL

Section C: Operational Scenario (MITRE ATT&CK)

ATT&CK Matrix: ENTERPRISE

Step	Technique	Name	Tactic	Target Asset	Description
1	T1190	Exploit Public-Facing Application	Initial Access	CW-SRV-01	Exploit zero-day or known unpatched vulnerability in the CloudWorks API gateway.
2	T1059.004	Unix Shell	Execution	CW-SRV-01	Execute commands on the compromised container/pod to enumerate the Kubernetes environment.
3	T1078.004	Cloud Accounts	Privilege Escalation	CW-SRV-01	Leverage compromised service account credentials or Kubernetes secrets to escalate privileges.
4	T1021.002	Remote Services: SMB/Windows Admin Shares	Lateral Movement	CW-DB-01	Pivot from app cluster to database segment using stolen credentials or service mesh trust.
5	T1530	Data from Cloud Storage	Collection	CW-DB-01	Query the database to identify BEIC's tenant ID and document references in the index.
6	T1560.001	Archive via Utility	Collection	CW-STO-01	Stage and compress BEIC documents from object storage for exfiltration.
7	T1567.002	Exfiltration to Cloud Storage	Exfiltration	CW-STO-01	Exfiltrate compressed document archive to an attacker-controlled cloud storage endpoint.

Client's specific questions for the supplier:

- Step 1: What is the current patch status of the API gateway? When was the last vulnerability scan of public-facing endpoints?
- Step 3: Are Kubernetes secrets encrypted at rest? Is there runtime secret detection (e.g., Falco, KubeArmor)?
- Step 4: Is network segmentation enforced between the application cluster and the database segment? At what level (network policy, firewall, VLAN)?
- Step 5: Are tenant-level database queries logged and monitored for anomalous access patterns (e.g., bulk export, unusual query scope)?
- Step 7: Is egress traffic from the storage segment filtered? Are there alerting rules for large outbound data transfers?

Appendix B: Example Supplier Risk Assessment (Excerpt)

CloudWorks SAS response to the BEIC Risk Scenario Card (Appendix A). Excerpt showing steps 1, 4, and 7.

Step 1: T1190 — Exploit Public-Facing Application

Field	Assessment
Control Status	COVERED
Controls Description	API gateway runs behind Cloudflare WAF (OWASP Core Rule Set + custom rules). Application code undergoes SAST (SonarQube) on every commit and DAST (OWASP ZAP) weekly. External vulnerability scan (Qualys) weekly. Critical patches applied within 24h SLA. Last external pentest (Synacktiv, 2026-01-20): no critical findings on API surface.
Detection Capability	DETECT — WAF logging + Wazuh SIEM correlation. Anomalous API patterns trigger alert within 5 minutes. CrowdStrike Falcon on API gateway nodes.

Step 4: T1021.002 — Lateral Movement to Database

Field	Assessment
Control Status	PARTIAL
Controls Description	Network segmentation between app cluster and database uses Kubernetes NetworkPolicies (Calico). Database access requires mTLS certificate + password. No direct SSH access to database nodes.
Detection Capability	PARTIAL — Calico logs denied connections. Accepted connections to the database segment are logged but not currently correlated with application-level behaviour. A compromised service account with valid mTLS cert would not trigger an alert.
Gap Analysis	Gap: no behavioural analysis on database connection patterns from the application cluster. A compromised pod with valid service credentials could query the database without detection if the query pattern resembles normal application behaviour.
Remediation Plan	Action: deploy database activity monitoring (DAM) with baseline profiling per service account. Tool: Imperva Data Security or pgAudit + custom Wazuh rules. Target: Q3 2026. Interim control: weekly review of database connection logs for connections originating outside normal pod IP ranges.

Step 7: T1567.002 — Exfiltration to Cloud Storage

Field	Assessment
Control Status	GAP
Controls Description	Egress traffic from the storage segment is not currently filtered or monitored for volume anomalies. The object storage service requires internet egress for replication to the Frankfurt backup site (CW-STO-02).
Detection Capability	BLIND — No alerting on outbound data volume from the storage segment. Network flow logs are collected but not analysed for exfiltration indicators.
Gap Analysis	Critical gap: an attacker who has reached the storage segment can exfiltrate data without detection. The legitimate replication traffic to FR5 makes it difficult to distinguish malicious egress without content-aware inspection.
Remediation Plan	Action 1: Implement egress whitelist — restrict outbound from storage segment to FR5 backup endpoint only. Timeline: 30 days (Q2 2026). Action 2: Deploy NetFlow analysis with volume anomaly detection on the storage segment. Tool: Suricata + custom Wazuh rules. Timeline: Q3 2026. Interim control: daily manual review of egress volume metrics from CW-STO-01.

SRA Summary (Excerpt)

Field	Value
Overall Assessment	PARTIALLY_ADEQUATE
Coverage Statistics	COVERED: 3/7 steps. PARTIAL: 2/7 steps. GAP: 2/7 steps. NOT_APPLICABLE: 0.
Residual Risk	The exfiltration path (steps 6–7) represents a significant residual risk. An attacker who reaches the storage segment can currently extract data without detection. The remediation roadmap targets closure of this gap by Q3 2026. Until then, compensating controls (egress whitelist, manual volume review) reduce but do not eliminate the risk.
Disclosure Card Update	Yes. TPSA-01 Common Disclosure will be updated to v1.3.0 to reflect the DAM deployment (D4-07 update) and egress controls (new D2 supplementary control) once implemented.