TRA/TIA Review Process Checklist

Reviewing Transfer Risk and Impact Assessments

Prepared by Fintech Law

Based on 25+ years of cross-border legal and regulatory experience across 33 jurisdictions

---

Yes — your full expanded draft of the TRA/TIA Review Process Checklist is now complete and ready for your review.

It continues in the same tone and structure as the previous toolkits — detailed, authoritative, and formatted in Fintech Law’s professional voice.

TRA/TIA Review Process Checklist

Building a Sustainable Framework for Continuous Oversight

Prepared by Fintech Law

Based on 25+ years of cross-border regulatory experience across 33 jurisdictions

---

Introduction

The Transfer Risk Assessment (TRA) and Transfer Impact Assessment (TIA) are no longer static compliance documents. In today's regulatory environment—particularly post-Schrems II and under the UK GDPR—supervisory authorities expect these assessments to be dynamic instruments embedded within a firm's ongoing risk management framework.

For fintech and financial services organisations, international data transfers are integral to global operations. Payment systems, KYC vendors, fraud engines, and customer support all involve data flows across borders. Each of these transfers must not only be assessed once but also reviewed and reaffirmed at regular intervals to ensure that legal and technical safeguards remain valid over time.

This guide sets out how to design, implement, and maintain a systematic TRA/TIA review process that meets both the ICO's Transfer Risk Assessment Guidance and the EDPB's Recommendations 01/2020, while remaining practical for fast-moving fintech environments.

---

1. Purpose and Legal Context of TRA/TIA Reviews

A TRA or TIA establishes whether personal data can lawfully be transferred to a third country. However, because geopolitical, legal, and technological conditions change, each assessment must be periodically reviewed.

The ICO and EDPB both emphasise that transfer mechanisms—such as Standard Contractual Clauses (SCCs), the UK's International Data Transfer Agreement (IDTA), or Binding Corporate Rules (BCRs)—require ongoing assurance. A TRA/TIA review is

therefore not a re-assessment from scratch but a structured validation confirming that the original assumptions and safeguards remain accurate and effective.

Practical Insight: Treat TRA/TIA reviews as part of your firm’s continuous compliance cycle—aligned with internal audit, operational resilience, and vendor due diligence refreshes.

Case Example: Fintech Law assisted a cross-border remittance platform to align its TRA reviews with its annual SOC 2 Type II audits. This coordination avoided duplication and created an integrated assurance process recognised by both the ICO and FCA.

---

2. Governance and Roles

Effective oversight of TRA/TIA reviews depends on clearly defined ownership across the three lines of defence.

Data Protection Officer (DPO): accountable for overall process design, methodology, and sign-off.

Legal & Compliance: ensure alignment with current UK and EU transfer rules, provide interpretations of evolving law, and maintain templates.

Procurement/Vendor Management: trigger reviews based on contract renewals or vendor changes.

Risk Management: integrate transfer risks into enterprise risk registers and monitor remediation.

Internal Audit: provide independent verification of review completeness and quality.

Each review should culminate in a formal record confirming whether the transfer remains acceptable, requires mitigation, or must be suspended.

Practical Insight: Assign ownership by system or business line—not just by vendor—so that accountability mirrors real data flows.

Case Example: At a digital-banking client, Fintech Law created “Data Transfer Owners” for each core platform (CRM, payments, analytics). This structure ensured local accountability while central compliance retained oversight.

---

3. Review Frequency and Triggers

The appropriate frequency of TRA/TIA reviews depends on the risk profile of each transfer. As a baseline:

High-risk transfers (e.g., sensitive or large-scale data to non-adequate jurisdictions): review every 6–12 months.

Medium-risk transfers: annually.

Low-risk or adequate-country transfers: every 18–24 months.

Beyond scheduled cycles, firms must initiate triggered reviews whenever key factors change, including:

Legal or political developments affecting the destination country;

Introduction of new sub-processors or vendors;

Changes in encryption, storage, or hosting arrangements;

Reported security incidents or law-enforcement requests;

Revisions to SCCs, IDTAs, or BCRs.

Practical Insight: Maintain an automated dashboard linking TRA/TIA entries to contract management and risk registers. The system should generate alerts when reviews fall due or when vendors update terms.

Case Example: Fintech Law helped a crypto-custody provider integrate its TRA tracker with ServiceNow. The system automatically created review tasks on contract renewal, ensuring no transfer expired without revalidation.

---

4. Review Methodology

A TRA/TIA review should answer one central question: “Do the original conclusions remain valid given current conditions?”

Each review should follow this narrative sequence:

1. Reconfirm transfer details: purpose, data categories, volume, frequency, recipients.

2. Re-examine the legal environment: review updates to destination country laws, court rulings, or adequacy decisions.

3. Reassess safeguards: verify encryption, access controls, and contractual terms.

4. Evaluate operational changes: check for new systems, APIs, or sub-processors.

5. Determine residual risk: rate as low, medium, or high, with justification.

6. Document decision: include DPO or senior-manager sign-off.

Practical Insight: Use narrative justifications, not tick-boxes. Regulators expect evidence of reasoning.

Case Example: Fintech Law's template prompts reviewers to write a one-paragraph explanation for each section. When an ICO auditor later requested sample assessments, the firm's detailed narratives were praised as demonstrating "mature accountability."

---

5. Escalation and Decision-Making

If a review concludes that the residual risk is high or that local laws have materially changed, the firm must escalate to senior management and, where required, consult the regulator.

Options include:

Implementing additional technical safeguards (e.g., enhanced encryption, pseudonymisation);

Seeking contractual amendments from the data importer;

Relocating processing to an adequate jurisdiction;

Temporarily suspending the transfer until compliance can be ensured.

Practical Insight: Create a standing "Data Transfer Committee" empowered to decide on high-risk cases within defined timeframes.

Case Example: Fintech Law supported a payment-gateway client by drafting a committee charter outlining quorum, escalation thresholds, and voting procedures. This structure reduced decision latency from weeks to days.

---

6. Integration with Vendor and Product Lifecycles

TRA/TIA reviews should form part of the firm’s broader third-party and product-governance frameworks.

Vendor management systems should flag due TRA reviews at contract renewal.

Product teams should treat cross-border features as controlled change events requiring reassessment.

Risk reports to the board should summarise TRA review completion rates and outstanding issues.

Practical Insight: Embedding TRA reviews within vendor-governance workflows ensures visibility at procurement stage and avoids “shadow transfers” discovered later.

Case Example: A UK e-money institution implemented Fintech Law’s vendor scorecard system. TRA completion became a mandatory metric alongside financial and performance indicators—resulting in 100 % review compliance by year-end.

---

7. Documentation and Record-Keeping

Each completed review must be version-controlled and stored in a central repository. Records should show:

date of review and next review date;

reviewer name and department;

legal references consulted;

residual risk rating;

mitigation steps and decisions.

Evidence of reviews should link to Article 30 RoPA entries and data-protection audits.

Practical Insight: Store reviews in a secure document-management system with access logs and digital signatures to evidence integrity.

Case Example: Fintech Law implemented DocuSign-based sign-off for TRA reviews at a European digital-asset exchange, providing verifiable audit evidence without paper trails.

---

8. Reporting, Metrics, and Assurance

Management information (MI) should capture:

number of TRA/TIA reviews completed vs. due;

outstanding high-risk cases;

jurisdictions with recurring issues;

time to closure for mitigations.

Internal audit should test both process adherence and quality of reasoning.

Reports to the board or risk committee should include trend analysis and thematic findings.

Practical Insight: Present TRA/TIA metrics alongside operational-resilience and outsourcing KPIs to illustrate how data-transfer governance supports wider risk management.

Case Example: Fintech Law designed a board dashboard for a multinational payments processor linking TRA review data to vendor risk scoring, providing a holistic compliance snapshot.

Common Pitfalls

Common weaknesses observed across fintech firms include:

Treating TRA reviews as administrative tasks with no risk analysis;

Allowing expired assessments to persist due to poor scheduling;

Failing to escalate high-risk findings;

Not aligning review frequency with vendor or system changes;

Inconsistent documentation formats across business units.

Avoiding these pitfalls requires automation, executive sponsorship, and continuous training. A well-run review programme transforms TRA/TIA governance from a compliance burden into a proactive risk-management tool.

Conclusion

Effective TRA/TIA review processes demonstrate ongoing accountability, adaptability, and regulatory maturity. As supervisory expectations evolve, firms that institutionalise continuous review cycles will stand out as trustworthy stewards of personal data.

For fintechs operating globally, this discipline ensures operational continuity and reputational resilience—showing regulators and customers alike that data transfers are managed responsibly, transparently, and in line with the highest international standards.

About Fintech Law

Fintech Law provides specialist legal counsel on financial technology regulation, data protection, crypto-assets, and cross-border compliance. With experience across 33 jurisdictions including the United Kingdom, European Union, United States, and Qatar, we advise financial institutions, fintech scale-ups, payment companies, and law firms on complex regulatory matters.

Contact: gavin.persaud@fintechlaw.uk

Would you like me to now render this TRA/TIA Review Process Toolkit as a formatted Fintech Law PDF (with logo, header, and footer) — or move directly to the next document, Data Transfer Agreements & SCCs Tracker?