S|3 SPECIALIZED SECURITY SERVICES

TARGETED RISK ANALYSIS (TRA) READINESS CHECKLIST

Evaluate your organization's preparation for PCI DSS v4 Targeted Risk Analysis requirements

1. GOVERNANCE AND ACCOUNTABILITY

- [ ] » Our organization understands when a Targeted Risk Analysis (TRA) is required under PCI DSS v4.
- [ ] » Roles and responsibilities for performing, reviewing, and approving TRAs are clearly defined.
- [ ] » Executive management is aware of TRA requirements and participates in annual reviews.
- [ ] » The same risk methodology is used consistently across all TRA activities.
- [ ] » Completed TRAs are stored in a centralized, auditable location.

> **Tip from S3 Security**
> A consistent governance structure avoids fragmented documentation and ensures that TRAs align with broader security and compliance goals.

2. METHODOLOGY AND DOCUMENTATION

- [ ] » A formal TRA template or methodology is documented and approved by our leadership.
- [ ] » Our TRA process includes identification of assets, threats, impacts, and likelihood.
- [ ] » Each TRA clearly identifies the control, activity and/or frequency being justified.
- [ ] » We document how control frequency or methods reduces risk to an acceptable level.
- [ ] » Residual risk is defined and approved as part of each TRA.
- [ ] » TRAs include version control and are reviewed at least annually.

> **Tip from S3 Security**
> Well-documented TRAs demonstrate maturity and help streamline future PCI assessments by showing risk-based decisions are repeatable and defensible.

3. APPLICATION AND FREQUENCY

- [ ] » We have identified all PCI DSS requirements that allow customized or periodic control frequencies.
- [ ] » TRA coverage includes both standard and customized approaches (where applicable).
- [ ] » TRA updates occur after significant system, process or policy changes.
- [ ] » Risk evaluation results influence how frequently controls are performed (i.e., vulnerability scans, malware reviews, access reviews).
- [ ] » TRA results are reflected in our PCI documentation and evidence packages.

> **Tip from S3 Security**
> A well-scoped TRA program ensures that risk decisions are not just documented but also reflected in operational processes and compliance evidence.

4. VALIDATION AND REVIEW

- [ ] » Each TRA is reviewed and approved by management and the PCI QSA.
- [ ] » We maintain evidence of QSA review or feedback within our audit documentation.
- [ ] » TRA findings or changes are communicated to affected stakeholders.
- [ ] » There is a defined process to validate the continued effectiveness of controls analyzed in TRAs.
- [ ] » TRA outcomes inform updates to our broader risk management program.

> **Tip from S3 Security**
> Annual validation confirms that TRAs are not "one-and-done" exercises but part of continuous compliance improvement.

5. CONTINUOUS IMPROVEMENT

- [ ] » We regularly assess whether our TRA process is efficient and effective.
- [ ] » Lessons learned from assessments or audits are incorporated into our next TRA cycle.
- [ ] » Training is provided for compliance, security, and operational staff who contribute to TRAs.
- [ ] » TRA results are reviewed alongside vulnerability management, incident response, and other risk metrics.
- [ ] » Our TRA process scales effectively across business units and/or locations.

> **Tip from S3 Security**
> Mature organizations integrate TRA results into strategic security planning, creating measurable value beyond compliance.

CONTINUE TO

YOUR READINESS SNAPSHOT & SCORING GUIDE

YOUR READINESS SNAPSHOT

Category	Fully Met	Partially Met	Needs Work
Governance & Accountability (5)	☐	☐	☐
Methodology & Documentation (6)	☐	☐	☐
Application & Frequency (5)	☐	☐	☐
Validation and Review (5)	☐	☐	☐
Continuous Improvement (5)	☐	☐	☐

Scoring Guide

- **20–26 items checked as Fully Met**: You have a mature and well-documented TRA process.
- **10–19 items checked as Fully Met**: You are on track but could benefit from targeted improvements or validation.
- **Fewer than 10 items checked as Fully Met**: Your organization may need to formalize its TRA process before the next PCI DSS assessment.

NEXT STEPS

S3 Security can help you:

- Develop or refine a TRA methodology tailored to your business.
- Review your current TRA templates for completeness and accuracy.
- Validate your documentation ahead of your next PCI assessment.
- Train your team to perform, review, and maintain TRAs with confidence.

Let's simplify compliance together.