TPRM Practitioner Handbook

From supplier onboarding to defensible risk decisions

Companion to the GRC Workshop TPRM Practitioner Toolkit v1.0 | Clean template + worked example

LEARNING OBJECTIVE
Complete a supplier assessment using the workbook, challenge supporting evidence, document risk, obtain a traceable decision, and maintain oversight throughout the relationship.

Audience Aspiring GRC analysts, early-career practitioners, and experienced analysts refreshing their third-party assessment workflow.

Level Beginner to intermediate | Suggested format Guided practice + independent case study

Edition 1.0 | October 2026 | Educational reference, not an assurance certification or legal opinion.

How to use this handbook

1. Read Sections 1–3 before entering data. Open the clean workbook and keep the worked example alongside it for comparison.
2. Follow the lifecycle in Sections 4–9. Complete the registers as evidence becomes available; the worksheet order is a navigation guide, not a rigid approval process.
3. Use the decision quality checks in Section 10 before relying on dashboard outputs.
4. Complete the independent practice exercise in Section 11 and use the review rubric to identify weaknesses in your work.

Contents

1 What TPRM is and what the analyst owns

2 Workbook map and operating rules

3 Setting up a defensible assessment

4 Intake, classification and due diligence

5 Evidence, controls, findings and risk

6 Treatments, contractual requirements and decisions

7 Monitoring, incidents and concentration

8 Supplier exit and final reporting

9 Detailed worksheet reference

10 Quality assurance and frequent mistakes

11 Practical assessment and review rubric

12 Workbook limitations

1 What TPRM is and what the analyst owns

Third-party risk management (TPRM) is the process of understanding and managing risk created by suppliers and other external service providers. An analyst connects business dependency, supplier controls, evidence, risks, contractual commitments and management decisions into an auditable record.

Your task is not to prove that a supplier is risk-free. It is to provide decision-makers with clear, supported conclusions, including what is unknown.

Roles in a typical assessment

Role	Accountability in practice
Business owner	Explains service criticality and business consequences; owns the business exposure.
Relationship owner / procurement	Coordinates supplier information, contracts, onboarding and supplier engagement.
GRC / security analyst	Scopes due diligence, assesses evidence and controls, records findings and risks, recommends actions and follows up.
Control or treatment owner	Implements or supplies evidence of agreed remediation.
Approver / risk acceptance authority	Makes and documents decisions within delegated authority.
Legal / privacy / specialist teams	Review issues requiring their expertise; the workbook does not replace their advice.

KEY DISTINCTION
Assessment is an analyst activity. Approval and risk acceptance are management decisions. A recommendation does not become an authorisation merely because it appears in Excel.

2 Workbook map and operating rules

The workbook has 19 sheets. “01 Start Here” gives operational instructions; “02 Methodology & Settings” contains configuration, scoring and appetite inputs. Sheets 03–17 hold records. “18 Assessment Report” assembles a supplier summary; “19 Portfolio Dashboard” aggregates the portfolio.

Stage	Worksheet(s)	What the record establishes
Preparation	01–02	Edition, organisation, as-of date, scoring and appetite methodology
Intake / criticality	03–04	Supplier identity, service dependency and proposed tier
Assessment	05–10	Risks, questionnaire, evidence, controls and findings
Response / governance	11–13	Treatment, authorised decisions

		and contract security clauses
Ongoing oversight	14–16	Reviews, incidents and fourth-party dependencies
Closure / reporting	17–19	Exit actions, supplier report and portfolio measures

Rules that protect data integrity

- Use stable identifiers such as SUP-001, TPR-001 and EV-001. Do not recycle IDs after records are used by other sheets.
- Blue cells are designed for entry. Calculated and lookup cells should not be overwritten.
- An “Incomplete”, “Not configured”, “Pending” or “CHECK” result is useful information, not an instruction to force a green status.
- Cross-referenced IDs must belong to the same supplier. Review the integrity indicators before making decisions.
- Use a controlled location for actual supplier documents; store references in the workbook rather than assuming the workbook is an evidence repository.
- The clean edition has no pre-approved decisions or preconfigured appetite. Determine those locally and obtain appropriate approval.

3 Setting up a defensible assessment

5. Save a controlled working copy of the clean workbook. Record the workbook owner, version, and location outside the spreadsheet if your organisation requires change control.
6. In 02 Methodology & Settings, enter your organisation name. Use the as-of date override only when taking a reproducible snapshot or completing training.
7. Review the defined criticality scale, likelihood/impact matrix, risk bands, appetite input and review settings. Do not invent an appetite threshold for a real organisation.
8. Agree business owner, service scope, decision authority and the questions the assessment needs to answer.
9. Select a representative worked example to understand entries, but do not copy fictional approvals into live assessments.

WHEN APPETITE IS UNDEFINED
Record “Not configured” and escalate for policy clarification. A workbook cannot infer an organisation’s risk appetite from its risk scoring matrix.

4 Intake, classification and due diligence

Step 1 — Register the supplier (03 Supplier Inventory)

Create one supplier record with a stable Supplier ID, legal/display name, service description, business owner, relationship owner, supported business process, lifecycle status and relevant contract dates. Define what the supplier actually does, not simply that it is "IT" or "SaaS".

Example: "Cloud hosting for the online account servicing application" makes the dependency assessable. "Technology supplier" does not.

Step 2 — Propose criticality (04 Criticality Assessment)

Score five dimensions on the workbook's 1–3 scale: business dependency, information sensitivity, system access, disruption impact, and replaceability/recovery difficulty. The workbook uses a highest-impact approach, so one dimension scored 3 can yield a High tier. Record an explanation for the scores and obtain the applicable confirmation; the calculated tier is only a proposal.

If you observe…	Do this
Low tier indicated	Check that no dimension is underestimated, then apply proportionate due diligence.
High tier indicated	Expand review depth for business continuity, data, access, sub-processors and contract rights.
Any missing/invalid score	Resolve the missing assessment rather than treating it as Low.
Calculated tier awaiting confirmation	Keep the approval status distinct from the proposed tier.

Step 3 — Scope questions (06 Question Bank; 07 Questionnaire Assessment)

The bank contains 72 starter questions organised by security domain and references, with suggested tier, supporting evidence and review considerations. The bank is a selection aid, not an automatic complete questionnaire. The analyst determines relevance to the specific service and enters selected question IDs on the assessment sheet.

10. Review the supplier's service and tier; identify relevant risks and data handling.
11. Select applicable Question IDs, checking the bank's applicability condition and suggested tier.
12. Record applicability with a reason for genuine exclusions.
13. Record the supplier's response, evidence IDs, review outcome, reviewer and dates.
14. Challenge unsupported "Yes" responses. Request supporting material and record unresolved gaps.

PRACTITIONER PROMPT
If the supplier answers "Yes, we perform quarterly privileged-access reviews", what evidence shows the reviews occurred, on the relevant systems, within the period under examination?

5 Evidence, controls, findings and risk

Step 4 — Index and evaluate evidence (08 Evidence Register)

Create an EV-ID for every material document or assurance item. Capture type, title, issuer, dates, applicable scope, storage reference and review outcome. Check relevance, completeness, authenticity and period coverage. A current certificate may cover a narrower service than the one being assessed.

Distinguish document expiry from a historical reporting period: an expired certificate may need renewal, while a completed SOC 2 reporting period remains historical evidence whose continued relevance must be assessed. Do not treat a prior-year report as current continuous assurance.

Step 5 — Assess controls independently (09 Control Assessment)

Evaluate design, implementation and operating effectiveness separately. The questionnaire describes supplier claims; control assessment states your evidence-based conclusion. Use the available assessment values and record the assessment objective, linked risk, evidence IDs, reviewer and rationale.

Where evidence is insufficient, say so. Lack of evidence does not by itself prove a control is ineffective. A confirmed control weakness requires a supported finding about design, implementation or operation.

Step 6 — Record findings (10 Findings Register)

Write findings as testable observations: requirement; observed condition; evidence; business implication; severity; owner; status and next action. Separate an Evidence gap from a Confirmed control weakness. Severity is an analyst judgement requiring context, not an automatic output from the questionnaire.

Weak finding: “Supplier IAM is bad.” Stronger finding: “The supplier stated privileged access is reviewed quarterly, but no review records for the assessed period were provided; operating effectiveness cannot be concluded.”

Step 7 — Record risk (05 Supplier Risk Register)

Use one row for each credible risk scenario. Capture threat/event, relevant cause/exposure, business consequences, business owner, inherent likelihood and impact, current controls, current residual likelihood and impact, target likelihood/impact and treatment links.

Concept	What it means
Inherent risk	Exposure before considering controls.
Current residual risk	Present exposure after controls that are actually evidenced and operating.
Target residual risk	Desired future exposure if additional treatments succeed.
Appetite comparison	Whether the current residual exposure exceeds the configured threshold.
Risk acceptance	An authorised decision to tolerate exposure, not an automatic reduction of severity.

SCORING EXAMPLE

A likelihood of 3 and impact of 4 gives 12 (High in the supplied test scenario). The score is only as

defensible as the assumptions and evidence supporting its inputs.

6 Treatments, contractual requirements and decisions

Step 8 — Track corrective action (11 Treatment Tracker)

Link each treatment to its supplier and, where relevant, the risk or finding. Specify approach, action, delivery owner, accountable internal owner, due date, delivery status, verification and evidence. Delivered means the action owner says it has been completed. Only verified remediation should be regarded as closed in the workbook.

Reassess current residual risk separately after verification. Do not assume that marking an action delivered, or even verified, automatically changes the risk score.

Step 9 — Examine the contract (13 Contract Requirements)

Review relevant security and operational resilience commitments, such as notification, security responsibilities, data handling, audit/assurance rights, subcontracting, recovery and exit. Link clauses to risks and record gaps. A clause being marked present does not establish legal adequacy or enforceability; seek specialist review when necessary.

Step 10 — Recommend and record decisions (12 Acceptance & Decisions)

Prepare a concise recommendation that states what is known, what remains outstanding, the impact of proceeding, any conditions, review dates, and the accountable decision-maker. The decision register distinguishes recommendation, authorisation and associated evidence.

15. Confirm whether this is supplier approval, conditional approval, risk acceptance or another recorded decision.
16. Identify whether it is supplier-level or linked to a specific risk.
17. Record approver, decision, date, rationale, conditions and evidence of authority in the applicable fields.
18. Where appetite is exceeded, retain the original above-appetite flag even after authorisation.
19. Set follow-up obligations, owners and dates; maintain the linked treatment and monitoring records.

RED FLAG
A populated approver name without supporting authorisation evidence is not sufficient to establish that a decision has been authorised. The workbook can check record completeness, not actual organisational authority.

7 Monitoring, incidents and concentration

Step 11 — Schedule oversight (14 Supplier Monitoring)

Record reviews, dates, evidence, findings and relevant KRIs. Use the review status and threshold indicators to identify follow-up work. An overdue scheduled review is an administrative lapse and should not automatically become a supplier control finding. A KRI breach is a signal to investigate and evaluate in context.

Step 12 — Track supplier incidents (15 Incident Log)

Record notice time, affected services, confirmed facts, suspected exposure, unresolved questions, business impact, actions, communications and status. Separate fact from allegation. Follow the organisation's incident response, privacy, legal and notification processes; the workbook is an oversight record and does not decide whether an incident is reportable.

Step 13 — Assess dependencies (16 Dependency & Concentration)

Record important fourth parties, shared technology, geography, business impact and the related risk. Use consistent provider names so the workbook can count how many registered suppliers declare the same dependency. A count of two suppliers on one provider is an indicator for review, not proof of unacceptable concentration.

8 Supplier exit and final reporting

Step 14 — Manage exit (17 Supplier Exit Tracker)

Document responsibilities for the supplier exit checklist, including evidence of access removal, data return/deletion where relevant, transition and contractual closure. The workbook evaluates completeness of mandatory checklist actions; "Ready for closure review" is not a formal approval to terminate.

Step 15 — Produce the assessment (18 Assessment Report)

Select the Supplier ID and inspect the assembled profile, classifications, current risks, findings, actions and decisions. Ensure the assessment narrative reflects the records and limitations. The report is a compilation aid, not an independent validation or automated supplier approval.

Step 16 — Review the portfolio (19 Portfolio Dashboard)

Review supplier tiers, residual risk, appetite breaches, overdue actions, findings and data-quality indicators. Reconcile unusual totals against source registers. A dashboard figure is only meaningful if the register records are complete, linked correctly and up to date.

9 Worksheet-by-worksheet quick reference

Sheet	Start with...	Before moving on, check...
01 Start Here	Instructions and edition	Workbook limitations and editable cell convention
02 Methodology & Settings	Organisation, appetite, dates	Approved parameters, not fictional assumptions
03 Supplier Inventory	Supplier ID and service	Business/relationship owner and exact service
04 Criticality Assessment	Five dimension ratings	Reasoning and tier confirmation
05 Supplier Risk Register	Specific risk scenario	Inherent/current/target kept distinct
06 Question Bank	Candidate questions	Applicability and currency of question
07 Questionnaire Assessment	Selected Question IDs	Answers supported by evidence
08 Evidence Register	EV-ID and provenance	Scope, period and review conclusion
09 Control Assessment	Control objective and links	Evidence supports design/operation judgement
10 Findings Register	Observation and proof	Evidence gap versus weakness
11 Treatment Tracker	Action and ownership	Verification distinct from delivery
12 Acceptance & Decisions	Recommendation and authority	Decision evidence and unresolved exposure
13 Contract Requirements	Relevant clauses	Legal review where needed
14 Supplier Monitoring	Review event and due date	Thresholds, follow-up and dates
15 Incident Log	Facts and unknowns	Escalation outside workbook
16 Dependency & Concentration	Named shared provider	Indicator interpreted in context
17 Supplier Exit Tracker	Mandatory closure items	Evidence and formal closure review
18 Assessment Report	Supplier ID selection	Completeness and narrative
19 Portfolio Dashboard	Portfolio metrics	Integrity checks and reconciliation

10 Quality assurance and frequent mistakes

Pre-decision checklist

☐ Supplier identity, services, ownership and tier are accurate.

☐ Due-diligence coverage matches risk and service scope.

☐ Material supplier claims have verifiable and relevant evidence, or the gap is recorded.

☐ Control conclusions distinguish insufficient evidence from confirmed failure.

☐ Current residual risk reflects verified controls, not intended treatment.

☐ Risk appetite is configured and authorised, or the limitation is shown.

☐ Every treatment has an owner, due date and verification requirement.

☐ Contract gaps and incidents have been escalated to appropriate specialists.

☐ Approver authority and decision evidence are present and conditions are trackable.

☐ Cross-sheet links, integrity checks and dashboard totals have been reviewed.

Common mistakes

Mistake	Better practice
Treating a "Yes" answer as effective control	Review evidence for the relevant scope and period.
Using target residual as current residual	Keep planned control benefit separate until verified.
Hiding accepted risks from appetite breaches	Leave the breach visible and attach decision evidence.
Closing action when supplier says "done"	Require verification against acceptance criteria.
Calling overdue review a confirmed weakness	Escalate administration separately from control effectiveness.
Reading shared-provider count as unacceptable risk	Apply scenario, impact and substitutability analysis.
Assuming dashboard = source of truth	Check record quality and exceptions first.

11 Practical assessment: three-supplier challenge

This exercise is a recommended learning activity. Use fictional organisations and data only. Do not copy the worked example's decisions into your clean workbook.

Fictional supplier	Service	Likely areas to investigate
Aster Cloud Services	Hosts a customer-facing application and related data	Criticality, recovery, privileged access, assurance period, concentration
Harbour Support Desk	Processes customer queries through a SaaS platform	Personal data, incident handling, access, sub-processing, retention
Oakfield Stationery	Supplies office consumables with no production access	Proportionate classification and lighter due diligence

Exercise instructions

20. Register all three suppliers. State service boundaries and accountable business owners.
21. Rate criticality across the five dimensions. Explain which rating drives the tier.
22. Select a proportionate set of questions from the question bank for each supplier.
23. Create fictional evidence records. Include one outdated assurance reporting period, one strong document and one unsupported supplier response.
24. Assess at least two controls and write two findings, making one an evidence gap and the other a confirmed weakness supported by scenario facts.
25. Create three risk scenarios, including inherent, current residual and target risk, and articulate uncertainty.
26. Record two treatments and demonstrate that "Delivered" is not the same as "Verified".
27. Draft one conditional supplier recommendation and one risk-acceptance case. Mark records as fictional; do not invent an actual authorisation.
28. Document a fourth-party dependency, monitoring plan and an incident fact-versus-unknown note.
29. Select each supplier in the Assessment Report, examine the dashboard, and prepare a one-page management summary.

Self-review rubric

Criterion	Excellent evidence of practice
Traceability	Every material conclusion links to the right supplier, risk, control and evidence.
Reasoning	Scores and severity have credible, documented business rationale.
Evidence quality	Claims, evidence sufficiency and limitations are distinguished.
Decision discipline	Recommendations, appetite breaches and authority are accurately represented.
Lifecycle completeness	Actions, monitoring, incidents, contract and exit questions are considered proportionately.

Communication	Management summary explains exposure, choices, owners and next dates without jargon.

Suggested reflection: Which conclusion changed after you reviewed the evidence? What remained uncertain? What would you escalate, to whom, and why?

12 Workbook limitations

- Protected sheets support filtering, but sorting requires unprotecting the sheet first.
- Dashboard-specific filters are not implemented; use register filters.
- The workbook has fixed capacities (including 60 suppliers and 200 risks). Confirm overflow handling if approaching those limits.
- Some many-to-many evidence links use comma-separated identifiers and a resolved-count check rather than separate relational link tables.
- The report and dashboard do not replace judgement, authority verification, legal review, technical testing, or incident response procedures.

GRC Workshop | Learn the work. Practise the judgement. Document the evidence.