GRC WORKSHOP

ENTERPRISE RISK MANAGEMENT

Practitioner Handbook

A field guide to practical risk assessment, treatment, oversight and reporting

FREE PRACTITIONER RESOURCE • VERSION 1.1 • OCTOBER 2026

From risk identification to management decisions

Enterprise Risk Management

Practitioner Handbook

GRC Workshop | Version 1.1 | October 2026
A free practical companion to the ERM learning pathway and toolkit

> **Who this is for:** Aspiring and junior GRC analysts, career switchers, and practitioners who need a structured reference for everyday risk work.
> **Prerequisites:** Familiarity with basic organisational objectives and risk terminology is useful but not essential.
> **Scope:** General practitioner education, not legal advice, certification, or an approved methodology for any particular organisation. All organisations and events in the worked example are fictional.

How to use this handbook

Use this as a field reference, not a substitute for your organisation's approved policies. Read Chapters 1–3 for orientation, Chapters 4–8 while performing work, and Chapters 9–10 when preparing reports and reviewing quality. Chapter 11 is a complete case study. Chapter 12 provides reusable checklists and exercises. Use the GRC Workshop ERM Toolkit alongside it: review the sample version before entering information into a clean copy. Field names in this handbook are generic; the exact workbook tabs, validation rules and formulas must be checked against the final released workbook.

Learning outcomes: By the end, you should be able to (1) write and support a clear risk assessment; (2) distinguish risk owners, advisers and approval authorities; (3) compare current exposure against approved appetite and tolerances; (4) develop and monitor a treatment plan; and (5) communicate an actionable risk decision to management.

---

1. The analyst's role in ERM

Enterprise risk management (ERM) connects uncertainty to objectives and decisions. A risk is the effect of uncertainty on objectives; in everyday practice, you need to describe the scenario, potential consequences and what the organisation can do about it. Risk management is not simply maintaining a register. It is a cycle of understanding context, identifying exposures, analysing and evaluating them, selecting responses, monitoring changes and communicating decisions.

A GRC analyst commonly facilitates workshops, requests evidence, challenges assumptions, records assessments, tracks actions, prepares reports and escalates concerns. The analyst does **not** automatically own each business risk or have authority to accept it. The accountable risk owner must understand the exposure and make decisions within delegated authority. The governing body or designated committee typically sets oversight expectations and approves overarching appetite; precise roles vary.

Role	Typical accountability or activity
Board / governing body	Oversight and approval of enterprise appetite, subject to governance arrangements

Role	Typical accountability or activity
Risk committee / executive sponsor	Reviews material exposure and decisions within delegated authority
Risk owner	Accountable for the business risk and recommendations or decisions under delegation
Control owner	Designs and operates a particular control; supplies evidence
Treatment action owner	Implements and evidences an assigned action
GRC analyst / risk function	Advises, challenges, documents, coordinates and monitors
Internal audit	Provides independent assurance; generally does not own management's controls

On the job: When asked to "sign off this risk", establish who is requesting approval, what exact decision they want, the applicable authority, what evidence supports it and whether acceptance is legally and contractually permissible. A GRC analyst's acknowledgement of a record is not the same as formal business acceptance.

2. Understand the business before scoring risk

Start with the organisation's objectives, services, important assets, dependencies, stakeholders and external obligations. A risk may be severe to one business process and marginal to another. Without this context a score is not defensible.

Minimum context record: Business objective; process/service and owner; relevant assets or suppliers; plausible threats or sources of uncertainty; existing commitments; material assumptions; time horizon; scope and reporting period.

Questions to ask stakeholders: Which outcome matters most? What would disruption cost? What customer, legal or safety impacts are possible? What has happened before? Which controls actually operate? What has changed recently? Who can decide if the exposure is acceptable?

Keep the distinction between **risk**, **issue** and **incident**. A risk concerns uncertain future effects; an issue is an identified present problem; an incident is an event that has occurred. A failed control may be a current issue that increases a future risk, and a live incident may require immediate response in addition to risk review. Do not delay incident handling while completing a register.

3. Identify and write a credible risk

Sources include interviews, business process reviews, audit findings, incidents, supplier assessments, change requests, vulnerability results and emerging threats. Invite both business and technical perspectives. A register that only reflects technical vulnerabilities may miss strategic, operational and concentration exposures.

A practical risk statement follows **cause or condition → uncertain event → consequence for objective**:

> Because privileged access is not consistently protected with MFA, an unauthorised party may obtain administrative access to production services, potentially causing customer-service interruption and unauthorised disclosure of information.

Avoid entries such as “cyber risk”, “lack of MFA” or “non-compliance” without describing what could happen and why it matters. Record the cause separately from the consequence where the template permits.

Evidence pack: Affected systems/processes, findings and dates, configuration evidence, logs or incidents, stakeholder confirmation, assumptions and evidence limitations. Distinguish facts, expert judgement and unverified claims. Do not paste confidential organisational information into public training tools.

Example initial fields: Risk ID CYB-014; process Customer payment services; category Cybersecurity; owner Head of Technology; assessment date; statement; existing controls; inherent assessment; current residual assessment; appetite position; actions; review date.

4. Assess likelihood, impact and uncertainty

Use the organisation’s approved scoring methodology. This handbook illustrates a five-by-five matrix with likelihood and impact each rated from 1 to 5, and a score equal to likelihood multiplied by impact. That method is **illustrative**, not mandated by ISO 31000 and not a precise statistical measurement.

Value	Example likelihood label	Example impact label
1	Rare	Insignificant
2	Unlikely	Minor
3	Possible	Moderate
4	Likely	Major
5	Almost certain	Severe

Operational use requires approved descriptions for each label, including time horizon and relevant financial, service, regulatory, customer or safety consequences. The impact dimension may be multidimensional; do not simply average unlike impacts without an agreed method.

Inherent risk is the assessment before considering the relevant controls, as defined by the organisation’s methodology. **Current residual risk** accounts for currently implemented controls and evidence of their effectiveness. **Target risk** is the anticipated position *after* planned treatment and is not the present assessment.

Example: inherent likelihood 4 and impact 5 yields 20. Existing controls lead the assessment team to judge current residual likelihood 3 and impact 4, yielding 12. The figures require written rationale; “controls in place” alone is insufficient. Never deduct an invented “control score” from inherent risk unless your methodology explicitly requires and defines it.

Challenge questions: Is the scenario specific? Does the time horizon match the criteria? Is the evidence representative? Do we know whether the control works? Are the consequences plausible? Has the business changed? Would a qualitative scenario description be clearer than the numeric label? A score of 12 is not necessarily twice as risky as a score of 6.

5. Evaluate controls and evidence

A control may prevent, detect or correct a problem. **Design effectiveness** asks whether it is capable of addressing the risk if it operates as intended. **Operating effectiveness** asks whether it has actually worked during the relevant period or at the tested point in time.

Typical assurance approach: identify the control objective; map it to the risk; name the owner; understand the population, frequency and period; inspect policy/configuration and actual records; test a sample where appropriate; document exceptions; conclude with limitations. Be cautious about claiming continuous effectiveness from a single screenshot.

Claim	Evidence that may support it	Important limitation
Privileged MFA is enforced	Policy/configuration export and reconciled privileged account inventory	Newly created or excluded accounts may be missed
Offboarding is timely	Sample of leavers, termination dates, access revocation records	A small sample may not represent all departures
Supplier recovery is credible	Test results, incident records, contract and recovery reports	Supplier assertion alone is weaker evidence
Vulnerabilities are managed	Validated scan scope, tickets, age and exception records	Missing assets can distort the metric

When controls are deficient, record the finding and business implication; discuss practical compensating measures, their coverage and expiry; and reassess exposure only when evidence warrants it.

6. Interpret appetite, tolerance and breaches

Risk appetite is the kind and amount of risk the organisation is willing to pursue or retain in achieving objectives. **Tolerance** defines acceptable variation or more specific boundaries. **Capacity** concerns what it could withstand. **Monitoring thresholds** trigger warning, investigation or escalation. Different frameworks use these terms somewhat differently; always follow local approved definitions.

Fictional policy example: a customer-facing service has low appetite for disruption; maximum cumulative unplanned downtime is four hours per calendar month. Warning is triggered at two hours, escalation at three, and a confirmed tolerance breach above four. Reaching the warning threshold does not necessarily mean breaching the final tolerance.

Breach handling sequence: (1) validate data, scope and policy; (2) establish exposure and business impact; (3) alert risk owner; (4) invoke urgent incident/compliance processes if needed; (5) develop treatment or exception options; (6) escalate to designated authority; (7) document decision, interim safeguards and expiry; (8) monitor and close only with evidence.

Management's desire to accept a risk does not make it acceptable under policy. A time-limited exception, where permitted, needs delegated authority, rationale, conditions and expiry. Management cannot waive law or mandatory regulatory obligations merely by documenting acceptance.

7. Choose and authorise risk treatment

Four familiar responses are **avoid**, **reduce or mitigate**, **share or transfer**, and **accept or retain**. They are not interchangeable, and treatments may be combined.

Response	When considered	Critical limitation
Avoid	Stop or change an activity creating unacceptable exposure	Can sacrifice business benefits; evaluate feasibility

Response	When considered	Critical limitation
Reduce	Introduce or improve controls to lower likelihood or consequences	Benefits must be verified, not assumed
Share / transfer	Contractual allocation, outsourcing or insurance	Accountability and residual exposure often remain
Accept	Retain exposure within approved authority and obligations	Requires documented, informed authorisation

A treatment decision should compare expected benefit, cost, time, feasibility, dependencies, secondary risks and effect on objectives. The cheapest option is not automatically best. Where business continuity or safety could be affected, include relevant specialist stakeholders.

Treatment plan minimum: risk ID, selected approach and rationale, alternatives considered, accountable risk owner, named action owner, milestones, resources, due date, interim measures, expected evidence, target exposure, approval/exception, review date and closure criteria.

Important: Target risk is an expectation. The *current* residual risk should not decrease until changed controls are implemented and evaluated. Risk acceptance is not the same as remediation, and a ticket marked “done” is not proof that the treatment worked.

8. Monitor risks, KRIs and action plans

Monitoring is necessary because businesses, threats and control performance change. **KRIs** indicate conditions or exposure associated with risk. **KPIs** measure performance against objectives. **KCIs** assess control operation. One indicator can serve more than one purpose depending on its use.

Example KRI: percentage of open validated critical vulnerabilities overdue for treatment. Define the numerator, denominator, in-scope population, timestamp, system of record, frequency, warning/escalation bands and owner. If nine of thirty open validated critical vulnerabilities are overdue, the rate is 30%. Interpret this with asset criticality, exploitability, compensating controls and scanning coverage; it is not a 30% probability of compromise.

A well-designed indicator supports decisions and has a clear action path. Combine values with trends, sample limitations and qualitative analysis. A green dashboard is not proof that no serious individual risk exists.

For action tracking, record status and evidence separately. Completion may mean implementation ended; closure means required verification and governance checks passed. A delayed treatment may itself require escalation under the agreed rules.

9. Maintain the risk register and report to management

Use consistent naming, IDs, dates, status definitions and a traceable audit trail. Avoid silently overwriting historic rationale or approved decisions. A register should answer: what might happen; why; who owns it; how significant; what controls operate; what action/decision is needed; when will it be revisited?

Suggested reporting structure: overall exposure and trends; top out-of-appetite risks; changes since prior period; breaches/exceptions; overdue treatments; important assumptions; decisions requested, with authority and deadline. Executive reporting should translate technical conditions into business impact without exaggeration.

Example management brief:

> *CYB-014: Unauthorised privileged access.* Current residual score 12 against an approved maximum of 10 for this category. MFA coverage is incomplete on a confirmed subset of privileged accounts. The Head of Technology proposes full coverage and inventory reconciliation within 30 days, with restricted administrative network access as an interim measure. Approval is requested for the plan and any necessary time-limited exception through the designated risk authority. GRC will review evidence and reassess at the next checkpoint.

Do not present unverified target scores as achievements. Name the required decision and the decision-maker. If a live incident or likely regulatory notification arises, use the relevant process immediately rather than relying only on monthly reporting.

10. Operate the toolkit safely and consistently

The GRC Workshop ERM Toolkit is intended for learning and adaptation. The **sample workbook** demonstrates a populated example; the **clean workbook** supports independent practice. Use local copies with fictional data for exercises. Avoid uploading live customer, employee, supplier or vulnerability data to a public website.

Suggested workflow: (1) read workbook instructions; (2) review the example and scoring definitions; (3) make a working copy; (4) confirm organisational scope, owners and thresholds; (5) enter clear risk statements; (6) document assessments and control evidence; (7) record appetite and treatment; (8) assign review dates; (9) check dashboards and source fields; (10) verify formulas, input validation and record consistency before distributing a report.

Workbook-specific acceptance checks: the final release should confirm actual tab names, input cells, locked/formula cells, rating bands, appetite flags, action-tracker relationships and dashboard refresh behaviour. This handbook does not claim those exact mechanics have been inspected. If a calculated result conflicts with source evidence, investigate instead of adjusting a score merely to achieve the desired status.

Quality gate: all material risks have owners, assessments have rationale, exceptions have decision authority, treatments have evidence and dates, and dashboards are traceable to underlying records.

11. Full worked case: a critical supplier dependency

Organisation: Alderbridge Payments Ltd (fictional). **Objective:** provide reliable online payment processing to merchant customers. **Scenario:** a cloud-based payment routing supplier has experienced repeated unplanned outages; Alderbridge currently has no tested failover provider. The service is business-critical.

11.1 Initial identification

> Because payment routing depends on a single cloud supplier without proven failover, an extended supplier outage may prevent merchant transactions, resulting in lost revenue, customer dissatisfaction and potential contractual consequences.

Risk ID TPR-007; owner Chief Operating Officer; control owner Technology Operations Lead; assessment date 28 October 2026. Evidence: supplier incident timeline, internal transaction failure logs,

contract, continuity plan and architecture review. Assumptions: outage data is complete; revenue impacts are estimates pending Finance validation.

11.2 Assessment

Under the fictional 5×5 methodology, the team judges inherent likelihood 4 and impact 5 = **20**. Existing monitoring, contractual escalation and limited manual recovery reduce the assessed current residual likelihood to 3 while impact remains 5 = **15**. Record why each control is considered effective or weak. These values illustrate judgement, not independently estimated event probabilities.

Approved category acceptance boundary: residual score **10 or below**. The current score of 15 is outside appetite. Management must not lower the score to fit the boundary.

11.3 Treatment alternatives

Avoid: stop using the supplier immediately. Potentially severe service impact; unsuitable without tested replacement. **Reduce:** test alternate routing, improve failover, monitor supplier recovery and strengthen contractual incident obligations. **Share/transfer:** review service credits or insurance; these may compensate some losses but do not restore transactions. **Accept:** only via authorised exception if permitted, with expiry and interim controls; this is not automatic.

Recommendation: Prioritise a tested fallback routing option, enhanced monitoring and an interim manual continuity procedure. Obtain Finance and Operations estimates of business impact, and involve Legal/procurement in supplier remedies.

11.4 Treatment record

Element	Fictional entry
Action	Test secondary routing and documented failover procedure
Action owner	Technology Operations Lead
Risk owner	Chief Operating Officer
Target completion	30 November 2026
Evidence	Test report, recovery logs, updated architecture and signed operational procedure
Interim measure	Heightened monitoring and merchant communications plan
Target risk	Score 8, subject to evidence-based reassessment
Governance	Escalate current out-of-appetite position to authorised committee
Review	Weekly while outside appetite

11.5 Monitoring and outcome

Alderbridge tracks cumulative downtime, failed transaction counts, time to restore service and completion of failover tests. Illustratively, three outage events of 45, 75 and 150 minutes total **270 minutes (4.5 hours)**. If its approved monthly tolerance is four hours, a confirmed breach of **30 minutes** requires the documented escalation

response. Check whether downtime periods overlap and whether all incidents are in scope before confirming the figure.

The risk remains scored at 15 while treatment is in progress. If testing later supports improved recovery, stakeholders reassess likelihood and impact using the approved criteria. Do not assert target score 8 is achieved merely because the action is marked complete.

11.6 Risk committee briefing

> **Decision requested:** Endorse the proposed supplier resilience treatment plan, allocate engineering capacity and determine whether a time-limited exception is permissible while current exposure remains above appetite. **Evidence:** Three outages totalling 4.5 hours this month; no tested secondary route; supplier incident reports awaiting full root-cause confirmation. **Accountability:** COO owns the risk, Technology implements recovery measures, GRC monitors and challenges evidence. **Follow-up:** Weekly progress and reassessment after an evidenced failover test.

12. Practical exercises, checklists and model criteria

Exercise A — Write a risk statement

Scenario: A UK online retailer uses an API integration with excessively broad permissions and a long-lived secret. **Deliverable:** a cause–event–consequence risk statement, business objective and named risk owner. **Quality check:** avoid claiming an actual breach without evidence; identify potential impact and uncertainty.

Illustrative answer: Because the inventory integration uses excessive API permissions and a poorly governed credential, compromise or misuse of that credential may allow unauthorised access to order information and disrupt order processing. The Head of E-commerce Operations is the proposed risk owner, subject to confirmation of local accountability.

Exercise B — Evaluate an appetite breach

Fictional policy: Critical vulnerabilities must be remediated within seven calendar days after validation; a warning triggers at day five, and a formal breach occurs *after* day seven. **Data:** Findings A=3 days, B=6, C=10, D=7. **Deliverable:** warning/breach classification and escalation note.

Model interpretation: A normal; B warning requiring stated escalation; C confirmed overdue breach requiring risk-owner escalation and treatment/exception decision; D at the boundary, not strictly beyond it. Verify exact validation timestamps and local wording. An exception is not automatically granted by an IT manager without delegated authority.

Exercise C — Report a KRI

Data: Eight of 32 validated open critical vulnerabilities are overdue this month; previous period 12%. Organisation’s fictional escalation threshold is 20% or more. **Deliverable:** calculate the rate, report its movement and request a specific action.

Model interpretation: 25%, a 13-percentage-point increase over the prior period and above escalation threshold. Validate scope, duplicates, affected services and exceptions; ask the risk owner for prioritised remediation and near-term reporting. The observed rate is not a probability of a security incident.

Reusable analyst checklist

- ☐ Objective and risk scenario are clear and scoped.
- ☐ Risk owner and control/action owners are distinguished.
- ☐ Evidence, assumptions and missing information are documented.
- ☐ Approved rating method, time horizon and definitions are used.
- ☐ Inherent, current residual and target assessments are separate.
- ☐ Control design and actual operation are considered.
- ☐ Appetite, tolerance and applicable requirements are checked.
- ☐ Treatment alternatives, costs, dependencies and rationale are recorded.
- ☐ Approvals and exceptions use the correct delegated authority.
- ☐ Action owners, due dates, evidence and review frequency are assigned.
- ☐ Monitoring records trigger action when needed.
- ☐ Reports explain impact, trends and requested decisions.
- ☐ Closure is supported by evidence, not solely by a completed ticket.

Suggested exercise review rubric

Criterion	Weight	What to look for
Accuracy	25%	Correct terminology, calculations and evidence
Governance	25%	Owner, approval and escalation correctly differentiated
Reasoning	25%	Business impact, alternatives, uncertainty and proportionate action
Documentation	15%	Complete, traceable record and follow-up
Communication	10%	Clear decision request for intended stakeholder

Self-review against this rubric is a learning aid, not an independently verified competence assessment.

13. Quick reference and glossary

Term	Practical meaning
Risk	Effect of uncertainty on objectives
Risk owner	Accountable decision-maker for a business risk
Inherent risk	Exposure before considering relevant controls under the chosen methodology

Term	Practical meaning
Current residual risk	Exposure after considering currently operating controls
Target risk	Anticipated future exposure after planned treatment
Risk appetite	Type and amount of risk an organisation is willing to pursue or retain
Risk tolerance	Acceptable variation or particular exposure boundary
Risk capacity	Amount of exposure an organisation can withstand
KRI	Metric signalling risk exposure or relevant conditions
Control effectiveness	Assessment of whether a control is suitably designed and operates
Exception	Authorised, documented departure from a defined requirement, if permitted
Treatment	Action chosen to modify or deliberately retain exposure

14. References and continued learning

This handbook is practitioner education informed by established risk-management guidance; it does not reproduce or certify any standard. Consult the authoritative versions and your organisation's approved requirements when making real decisions.

1. **ISO 31000:2018**, *Risk management — Guidelines*, ISO: https://www.iso.org/standard/65694.html
2. **NIST Cybersecurity Framework 2.0**, particularly Govern (GV), 2024: https://www.nist.gov/cyberframework
3. **NIST SP 1303**, *CSF 2.0 Enterprise Risk Management Quick-Start Guide*: https://doi.org/10.6028/NIST.SP.1303
4. **NIST IR 8286 series**, cybersecurity risk and enterprise risk management: https://csrc.nist.gov/projects/cybersecurity-risk-management
5. **UK Government Orange Book**, *Management of Risk — Principles and Concepts*: https://www.gov.uk/government/publications/orange-book

Recommended GRC Workshop sequence: Enterprise Risk Management Explained → Risk Identification and Assessment → Inherent and Residual Risk → Risk Appetite vs Risk Tolerance → Risk Treatment and Acceptance → Risk Monitoring, KRIs and Reporting → ERM Toolkit Guide → ERM Pathway Assessment.

Version note: v1.0, 28 October 2026. Editorial draft for review. Workbook-specific tab names, formulas and instructions must be reconciled against the final released toolkit before publication. Any internal company case should remain fictional or fully authorised and sanitised.

Workbook-specific operating guide

Published companion: ERM Toolkit v4.1.1 — Clean Template. This section supplements the general handbook and takes precedence where workbook functions are more specific. The workbook must be configured before organisational use.

1. Read and configure the workbook

README — Start here for intended use, limitations, editable-cell legend and required setup order.

Methodology — Review the as-of date, likelihood/impact scales, rating bands, assessment validity, due-soon window, acceptance period and snapshot frequency.

Appetite — Define risk categories and approved appetite and tolerance scores, with statement, approver, approval date, effective date, review date and threshold version. The clean template is not preapproved for an organisation.

Checks — Confirm whether setup is complete and review data integrity issues. The release gate can show SETUP REQUIRED until appetite settings are approved.

2. Create an authoritative risk record

Risk Register A:E — Enter risk ID, title, cause-event-consequence description, category and risk owner. The register accommodates 100 records (rows 6–105).

Risk Register F:I — Enter inherent likelihood and impact (1–5); the inherent score and rating are calculated.

Risk Register J:P — The control-effectiveness entry is indicative only. For an authoritative residual score, provide evidence-based residual likelihood and impact in K/L and complete evidence reference, assessor, assessment date, approval and manual decision fields AE:AI and AL. If evidence or approval is invalid, the workbook may use the inherent basis.

Risk Register Q:AA — Track target score, gap, applicable appetite/tolerance, breach and governance statuses, review dates. Formula fields should not be overwritten.

3. Record decisions and control treatment

Risk Acceptance Register — Formal acceptance decisions belong here, not in an informal note on the Risk Register. Record decision, delegated authority, date, expiry, and justification; expired or insufficiently authorised acceptances do not make a breach disappear.

Breach Monitor — Review all risks exceeding appetite, including accepted risks. The monitor separately identifies tolerance breaches, acceptance expiry and required next actions.

Treatment Tracker — Use one row per mitigation action, linked by Risk ID. Record action owner, start/due dates, status, completion, evidence and reassessment information.

Risk-Control Matrix / RCM Summary — Map risks to controls and assess control effectiveness. The RCM suggested assessment is not a substitute for the evidence-approved residual rating on the Risk Register.

4. Monitor and report

KRI Tracker — Record indicators, risk link, measures and monitoring signals according to the sheet definition.

Emerging Risks — Flag material emerging exposures and escalation needs.

Scenario Analysis / Risk Aggregation / Aggregation Map — Use these for illustrative loss scenarios and concentration screening. Indicative annualised loss estimates are not financial forecasts, and ordinal risk scores must not be added.

Dashboard — Review risk counts, ratings, breaches, treatment actions, reviews, KRIs, emerging risks and scenario estimates. Ensure setup and data checks are valid before treating figures as decision-ready.

5. Preserve history and validate

Snapshot Capture — Set a fixed reporting date in Methodology. Check source data and control totals, then copy the specified capture range.

Snapshot History — Append captured records with Paste Special > Values. The history is manually maintained, not immutable.

Snapshot Trends — Select snapshot periods, enter required control totals and inspect reconciliations and like-for-like comparability.

Change Log — A voluntary log, not a tamper-resistant audit trail. Keep separately controlled evidence for formal approvals and change history.

Exception Register / Checks — Only exactly scoped and independently authorised exceptions affect the specified checks; they do not excuse unrelated defects.

Critical use rules

• Blue text on cream fill indicates editable input cells; black text on grey indicates calculated cells.

• Default bands: Low 1–4, Medium 5–9, High 10–16, Critical 17–25; confirm these and their interpretation for the intended organisation.

• Do not treat a numeric score as an objective probability or sum ordinal scores.

• Do not mark treatment closed or report a reduced residual score without evidence and the required approval.

• Recalculate and test the workbook in desktop Excel before using its results operationally; the workbook notes that Excel for web is unverified.

Workbook cross-check: ERM_Toolkit_v4_1_1_Clean_Template.xlsx, worksheet README, Methodology, Risk Register, Appetite, Risk Acceptance Register, Snapshot Capture, Checks and v4.1 Validation Guide.