RUKN ERM

Enterprise Risk Management

USER GUIDE

The 10-Step Risk Management Cycle, From Objectives to Continuous Monitoring

Aligned to the COSO ERM (2017) and ISO 31000 frameworks
Prepared for Rukn ERM users
Version 1.1 — September 2026, written against Rukn ERM 1.0.1

Introduction

Risk management is not a form you fill in once. It is a cycle: an organization sets objectives, works out what could threaten them, decides how much of that risk it is willing to live with, builds defenses, and then watches those defenses continuously so it can adjust before small problems become large ones.

Rukn ERM is built around that cycle. This guide walks you through all ten steps in order, from setting objectives through to continuous monitoring, so that whichever step you are working on, you know what it is for, what you do inside the app, and what should come out the other end.

The cycle at a glance

#	Step	In one line
1	**Objectives**	Define what the organization is trying to achieve, at every level.
2	**Risk Identification**	Surface the events that could help or hinder those objectives.
3	**Risk Assessment**	Score each risk's likelihood and impact before any controls.
4	**Board Sets Appetite**	Governance defines how much risk is acceptable, and where the lines sit.
5	**Treatment Decision**	Choose how to respond to each risk that sits outside appetite.
6	**Control Design**	Design the specific controls that carry out the treatment decision.
7	**Residual Risk Check**	See where the risk lands once controls are counted, and test it against appetite.
8	**KRI Design**	Build early-warning indicators that watch the risk going forward.
9	**Implementation & Testing**	Roll controls out, and prove they exist and work as designed.
10	**Continuous Monitoring**	Track KRIs and controls over time, report up, and feed learnings back to Step 1.

Two things to notice before you start. First, the cycle has a built-in feedback loop: if the Residual Risk Check (Step 7) shows a risk is still outside appetite once controls are considered, the process loops back to Step 5 for a stronger treatment decision, rather than moving forward. Second, the cycle never really ends — Continuous Monitoring (Step 10) is what feeds new information back into Step 1, so objectives, risks, and appetite are revisited on a regular rhythm rather than only when something goes wrong.

Screen names in this guide are the names the app uses. On the web the menu is grouped into Risk — Dashboard, Risk register, Risk appetite, Simulation, AI assistant, Actions, Incidents, KRIs, Controls — and Governance — Committees, Policies, Compliance, Audits, Reports, Organization. The iPhone and Android apps carry the same modules, the first five on tabs and the rest under More. Everything below works identically in Arabic, where the whole interface lays out right to left.

One caveat before you start: Step 1 is the only step of the ten that Rukn ERM does not hold. There is no objectives register in the product today, and the step below says what to do instead rather than pointing you at a screen that is not there. Simulation, Governance, Compliance and Audits are on the Growth and Enterprise plans; the rest of the cycle is on every plan, including the free trial.

STEP 1 Objectives

PURPOSE

Every risk only matters in relation to something you are trying to achieve. Before you can identify risks meaningfully, the organization needs a clear, current statement of its objectives — strategic, operational, reporting, and compliance — at the entity level and cascaded down to department or process level.

WHAT YOU'LL DO

- Agree the objectives outside Rukn ERM — in the strategy document, business plan or scorecard your organisation already keeps. This is the one step of the ten the app does not hold, so nothing here is lost by writing it down where your board already looks.
- Tag each objective by level (entity, department, or process) and by type (strategic, operational, reporting, compliance). Give each one an owner — the person accountable if it is missed — and a time horizon, so later risk assessments know what period they are protecting.
- Then build the matching structure inside Rukn ERM, under Organization → Structure: the business units and the departments inside them. Every risk must belong to a business unit, so this tree is what carries objectives into the register in practice, and it is what every report rolls up through.
- Keep the wording of each objective to hand. Step 2 asks you to name it in the risk's description, which is where the link between a risk and what it threatens is recorded today.

WHAT COMES OUT OF THIS STEP

- An approved objectives register, held outside Rukn ERM, and a business unit and department tree inside it that mirrors how those objectives are owned.

TIPS & COMMON PITFALLS

- Keep objectives specific enough to test. "Grow the business" cannot be risk-assessed; "increase government-sector contract revenue by X% this year" can.
- Revisit the objectives whenever strategy changes — a new tender, a new market, a reorganization — not only at the start of the annual cycle.
- Do not leave them implicit because the app has no field for them. A register whose risks cannot be traced back to anything is the most common reason a risk programme fails its first audit.

STEP 2 Risk Identification

PURPOSE

With objectives set, the next question is: what could happen — internally or externally — that would help or hurt each one? This step is deliberately broad. The goal is coverage, not judgment; scoring comes in Step 3.

WHAT YOU'LL DO IN RUKN ERM

- In the Risk register, create an entry for each risk. Rukn ERM assigns the code (RISK-0001, RISK-0002 …) so two people cannot pick the same one.
- Describe the risk in cause → event → consequence form, and name the objective it threatens in the same description (for example: "reliance on a single supplier [cause] could lead to a service outage [event], delaying contract delivery and triggering penalty clauses [consequence] — threatens the on-time delivery objective").
- Choose the category from your organisation's risk taxonomy, set up once under Organization → Taxonomy. The taxonomy is what the register filters by, what appetite is set against in Step 4, and what every roll-up report groups on.
- Set the business unit, and the department where the risk sits inside one. Business unit is required — it is how the register is filtered and reported by part of the organisation.
- Assign a risk owner — the person best placed to manage it day to day, not necessarily the objective owner. They are notified as soon as the risk is theirs.
- Draw on more than one source. Incidents and near misses are their own module in Rukn ERM, and anyone can report one from their phone in seconds; audit findings are raised in Audits; add workshops, contract and tender review, and external scanning of regulatory, market and geopolitical change.

WHAT COMES OUT OF THIS STEP

- A populated risk register, each entry categorised, owned, and placed in the organisation's structure, ready for assessment.

TIPS & COMMON PITFALLS

- One risk per entry. "IT and staffing issues" is two risks wearing a trench coat — split them so they can be owned and scored separately.
- Don't filter out risks that feel unlikely at this stage — likelihood is scored next, in Step 3.
- A risk owner must be a Risk owner, Risk manager, Support staff, Executive or Administrator. Auditors cannot own records they may later have to examine, and Rukn ERM will refuse the assignment.

STEP 3 Risk Assessment

PURPOSE

Now each identified risk is scored for likelihood and impact before considering any controls currently in place. This is the risk's inherent (gross) level, and it is what lets the organization prioritize attention rather than treat every risk the same.

WHAT YOU'LL DO IN RUKN ERM

- For each risk, score Likelihood and Impact from 1 to 5. Rukn ERM multiplies the two into the inherent score, so the scale runs 1 to 25.
- Those scores place the risk on the heat map on the Dashboard, and set its level: 1–4 is Low, 5–9 Medium, 10–16 High, 17–25 Critical.
- Record the basis for each score — data, expert judgment, historical incidents — in the description. Rukn ERM carries a single impact score rather than a set of dimensions, so the reasoning belongs in the text, where the next person to review it can read it.
- Where a risk can be quantified, fill in the four simulation inputs as well: annual probability, and the minimum, most likely and maximum loss. A risk with all four set is included in Simulation, which models the organisation's total annual loss and value-at-risk across the whole register.

WHAT COMES OUT OF THIS STEP

- An inherent risk rating and heat-map position for every risk, ranking them by priority.

TIPS & COMMON PITFALLS

- Score consistently across teams — run a short calibration session so "high" means the same thing in finance as it does in IT.
- Resist scoring in the residual (post-control) sense here. In Rukn ERM you never re-score for residual at all: the app calculates it from control effectiveness in Step 7, and a likelihood already discounted for controls quietly double-counts them.

This is the point where the board's risk appetite (Step 4) becomes the yardstick everything else is measured against — so it's worth having at least a draft appetite statement before assessment begins, even if the board hasn't formally signed off yet.

STEP 4 Board Sets Risk Appetite

PURPOSE

This is a governance step, not a risk-team step: the board (or equivalent governing body) decides how much risk the organization is willing to accept in pursuit of its objectives, and how much variation around that is tolerable. Everything downstream — treatment decisions, control intensity, KRI thresholds — is calibrated against this line.

WHAT YOU'LL DO IN RUKN ERM

- Open Risk appetite. For each category in your taxonomy, record the appetite statement in words ("low appetite for compliance risk, moderate appetite for growth-related operational risk"), then set two numbers: the appetite threshold and the tolerance threshold, both expressed as a residual score out of 25.
- Only an Executive or an Administrator can set appetite. That is deliberate: the people who draw the line should not be the same people working inside it.
- Rukn ERM then watches the line without being asked. When a risk's residual score crosses it, the executives and the risk owner are notified — the breach does not wait for someone to open the screen.
- Record the board's approval — date, attendees, version — in your own minutes. Rukn ERM stores the statement and the thresholds, not the approval; what it does keep is the activity log, which shows who changed appetite and when, and that is what an auditor will want alongside the minutes.

WHAT COMES OUT OF THIS STEP

- An approved, dated appetite statement per risk category, with the thresholds that Steps 5, 7 and 8 are all calibrated against.

TIPS & COMMON PITFALLS

- Appetite is not one number for the whole organization — a Kuwaiti government client, for example, will typically show near-zero appetite for compliance and reputational risk but a higher appetite for strategic/growth risk. Rukn ERM sets it per category for exactly this reason.
- Appetite is set once per category and applies across the organisation; there are no separate departmental thresholds. Where a department needs a tighter line, say so in the statement and hold it through KRI thresholds in Step 8.
- Revisit the appetite statement at least annually, and immediately after any major change in strategy, regulation, or market conditions.

STEP 5 Treatment Decision

PURPOSE

For every risk that sits outside the board's appetite, someone has to decide what to do about it. The decision is one of five: treat it (reduce it with controls), tolerate it (accept it as it stands), transfer it (insurance, contract, outsourcing), terminate it (stop the activity that creates it), or — where the risk carries an upside — take more of it deliberately in pursuit of a strategic gain.

WHAT YOU'LL DO IN RUKN ERM

- Record the decision as an Action on the risk. Rukn ERM has no separate treatment field: Actions is the treatment tracker, and an action raised from a risk stays attached to it.
- Give the action a title that states the decision, an owner, a due date and a priority. Put the rationale, the expected cost and the expected effect on the rating in the description — this is the record that has to stand up later.
- The owner is notified when the action is assigned to them, again as the due date approaches, and again if it passes. The register shows what is being done about each risk; Actions shows the whole programme of work in one list.
- Where the decision is to tolerate, raise the action anyway and complete it. That leaves a dated record of who accepted the risk, which an undocumented decision never does.
- Preventive, detective, corrective and directive are not treatment options in Rukn ERM — they are the four control types you choose from in Step 6, and they describe what a control does, not which response you picked.

WHAT COMES OUT OF THIS STEP

- A documented treatment decision and owner for every risk outside appetite, tracked in Actions and feeding directly into control design.

TIPS & COMMON PITFALLS

- "Tolerate" is a legitimate decision — but only when it is explicit, dated, and made by someone with the authority to accept that level of risk. An undocumented "we'll live with it" is not the same thing.
- Transferring a risk (e.g. insurance) moves the financial impact, not the accountability — governance and reputational responsibility stay with the organization.

STEP 6 Control Design

PURPOSE

Where the treatment decision is to treat/reduce a risk, this step turns that decision into specific, assignable controls — the actual mechanisms that will lower likelihood, lower impact, or both.

WHAT YOU'LL DO IN RUKN ERM

- In Controls, define each control: what it does, its type — preventive (stops the event), detective (catches it after it starts), corrective (puts it right afterwards) or directive (requires the behaviour that avoids it) — and which risk cause it addresses.
- Assign a control owner: the person who performs or is accountable for the control, which may differ from the risk owner.
- Rukn ERM does not carry separate fields for how often a control runs or whether a person or the system performs it. Put both in the description — the tester in Step 9 will look for them there, and a control whose frequency nobody wrote down cannot be sampled.
- Map each control to every risk it addresses. The mapping runs both ways: a control can cover several risks, and a risk can have several controls. This is also what makes the register show which risks have coverage and which have none.

WHAT COMES OUT OF THIS STEP

- A control library mapped to risks, with an owner and a stated frequency for each control, ready to be tested in Step 9.

TIPS & COMMON PITFALLS

- Design controls around the specific cause identified in Step 2, not the risk category in general — a vague control ("improve oversight") is hard to test and easy to skip.
- Favor a smaller number of well-owned controls over many loosely defined ones; each additional control is something someone has to keep proving works.

STEP 7 Residual Risk Check

PURPOSE

Once controls are in place, the question is where the risk actually sits now — the residual (net) risk — and whether the treatment has brought it back inside the board's appetite. Rukn ERM works differently from a spreadsheet here, and it is worth understanding before you trust the number.

WHAT YOU'LL DO IN RUKN ERM

- You do not re-score likelihood and impact. Rukn ERM calculates the residual from the inherent score and one figure — control effectiveness, from 1 to 5. Each point takes 15% off, so a risk scored 16 with fully effective controls lands at 4.
- That figure normally comes from the controls themselves. Map controls to the risk, record a test rating on each of them in Step 9, and Rukn ERM averages those ratings into the risk's control effectiveness and recalculates the residual on the spot. The risk screen says when the figure was derived this way rather than typed.
- Before anything has been tested you can enter control effectiveness yourself. Rukn ERM keeps the two apart deliberately: a figure you typed is yours and stays, while a derived one is cleared if the last rated control is unmapped — so the register never keeps discounting exposure on the strength of controls that are no longer there.
- Compare the residual against the appetite and tolerance thresholds for the risk's category. Crossing the line raises an appetite breach to the executives automatically.
- If the residual is still outside appetite, go back to Step 5 — a stronger treatment, more or better controls — or escalate to the board for an explicit, documented exception where no further cost-effective treatment exists.

WHAT COMES OUT OF THIS STEP

- A residual risk rating for every treated risk, resting on tested controls, and a clear pass or escalate position against appetite.

TIPS & COMMON PITFALLS

- Because the residual moves on its own here, the trap is different from the usual one: it is easy to accept the number without asking whether the control ratings behind it are current. A residual of 4 resting on a control last tested eighteen months ago is a number, not an assurance.
- Be honest about control effectiveness before testing starts. A control that exists on paper but has never been tested is not a 5, and typing one there discounts real exposure on the strength of a plan.

STEP 8 KRI Design

PURPOSE

Key Risk Indicators are early-warning, forward-looking metrics that tell you a risk is drifting toward its threshold before it actually breaches it — distinct from KPIs, which measure whether you're hitting performance targets after the fact.

WHAT YOU'LL DO IN RUKN ERM

- For each significant residual risk, define one or more KRIs that track a driver of that risk (for example "percentage of critical suppliers with a single point of failure" for a supply-chain risk). Give each one a name, a unit and an owner.
- Set two thresholds — yellow and red — and say which direction is bad. Rukn ERM colours each reading green, amber or red from those two numbers and the direction, so "higher is worse" and "lower is worse" indicators both read correctly. Calibrate them to the appetite bands from Step 4, leaving enough space between yellow and red to act.
- Set a measurement cycle — daily, weekly, monthly, quarterly, every six months or annually — and Rukn ERM tells the owner when a reading is due and chases them when it is overdue. Leave the cycle off for event-driven indicators and nothing is ever reported as late.
- Link the KRI to its risk, and to the control it watches where there is one. That second link is what lets a red reading say which control degraded, rather than only that exposure moved.
- Record readings as they arrive, with a note. Each reading is kept, so the indicator shows its history rather than only its latest value.

WHAT COMES OUT OF THIS STEP

- A set of owned, thresholded KRIs on a measurement cycle, feeding the dashboard used in Continuous Monitoring.

TIPS & COMMON PITFALLS

- Choose leading indicators where possible (backup-test failures) over purely lagging ones (system downtime) — the point of a KRI is to give you time to react.
- Fewer, well-chosen KRIs beat a long list nobody reviews. If a KRI never moves and nobody acts on its breaches, retire it.

STEP 9 Implementation & Testing

PURPOSE

Designing a control is not the same as having one. This step rolls the designed controls out into daily operation and proves — through testing — that they exist as designed (design effectiveness) and are actually being performed (operating effectiveness).

WHAT YOU'LL DO IN RUKN ERM

- Raise an Action for each new or changed control, with an owner and a due date. Actions is the tracker for implementation work as well as for treatment decisions.
- Perform a design walkthrough — confirm the control, as written, would actually address the risk cause it is mapped to.
- Test operating effectiveness on a sample of instances — a sample of approvals, reconciliations or access reviews — then record the test on the control itself: the rating out of 5, the date it was tested, and what you found. Rukn ERM keeps every test, so the control shows its trend and not just its latest number.
- Attach the evidence to the control: the sample sheet, the screenshot, the sign-off. A rating of 5 with nothing attached is an assertion; with the evidence attached it is something an auditor can check.
- The latest rating becomes the control's effectiveness, which flows straight into the residual score of every risk it is mapped to. A control rated 1 also notifies the risk owners, the risk manager and internal audit.
- Where the testing is internal audit work rather than management's own, run it through Audits: plan the audit with a lead auditor and a scope, raise findings against it with a severity and an owner, and raise remediation actions from each finding. When the remediation holds, verify the finding — Rukn ERM records who concluded it, when, and on what basis, and closes it. A finding closed too early can be reopened.

WHAT COMES OUT OF THIS STEP

- Evidence-backed confirmation that each control is in place and working, or a tracked remediation plan for the ones that aren't.

TIPS & COMMON PITFALLS

- Don't let a control sit as implemented in the register until it has actually been tested — an untested control is still a plan, not a control, and in Rukn ERM its rating is silently discounting a residual score.
- Reuse this evidence for internal and external audit — a well-kept testing log with files attached is most of what an auditor will ask for, and an Administrator can export every attachment in the organisation as a single zip.

STEP 10 Continuous Monitoring

PURPOSE

Risk management doesn't stop once controls are tested — objectives, threats, and the operating environment keep changing. This step keeps the whole cycle honest: it watches KRIs and controls over time, reports up to management and the board, and feeds what's learned back into Step 1.

WHAT YOU'LL DO IN RUKN ERM

- Review the Dashboard on a set rhythm — monthly for KRIs, quarterly for the full register — rather than only when something breaks.
- Let Rukn ERM do the watching between reviews. It notifies on assignment, on actions due soon and overdue, on incidents reported, on KRI breaches and overdue readings, on appetite breaches, on controls rated ineffective, on requirements found non-compliant, and on audit findings raised. Each person chooses which of those reach them by push and by email under Account security; the in-app list always keeps everything, so nothing is lost by muting a channel.
- Investigate and act on any KRI breach or failed control test, and log the response — a new action, a re-test, or a finding.
- Produce management and board reports from Reports: the risk register and action tracker as CSV, an executive summary as PDF, and — on the Growth and Enterprise plans — a full risk workbook as Excel and a board deck as PowerPoint, in English or Arabic.
- When monitoring surfaces a new risk, a changed objective, or a shift in what is tolerable, route it back into the cycle — to Step 1 or Step 2 as appropriate — rather than treating it as a one-off.

WHAT COMES OUT OF THIS STEP

- A live, current risk position, a track record of board and management reporting, and a steady stream of updates back into the start of the cycle.

TIPS & COMMON PITFALLS

- Treat this step as the connective tissue of the whole system, not an afterthought — a register that is never revisited after Step 9 goes stale within a quarter.
- Calendar the review cadence (who reviews what, and how often) as deliberately as you calendared the initial workshops in Step 2.

What Else Is in Rukn ERM

The ten steps are the spine of the product, but several modules sit alongside them and are easy to miss if you only follow the cycle.

- Incidents. What actually happened, as opposed to what might. Anyone can report one in seconds, link it to a risk, attach evidence and raise remediation actions from it. Incident history is one of the strongest inputs to Step 2.
- Governance — Committees and Policies. The bodies that oversee the programme, who sits on them and how often they meet; and the policy register, with approval dates, review dates and owners, which chases its own reviews before they fall due.
- Compliance. Frameworks and the requirements inside them, each owned, assessed and mapped to the risks and policies that address it — so "which risks cover this clause" has an answer.
- Simulation. Monte Carlo over the quantified risks from Step 3, producing expected annual loss, value-at-risk and a loss distribution for the whole register or by category.
- AI assistant. A risk-analysis assistant that works against your own register, within a monthly allowance set by your plan.
- Evidence. Files attach to risks, incidents, controls, policies and audit findings, and an Administrator can export every attachment at once.
- The activity log, under Organization. Who changed what, and when, across the whole organisation.
- The startup import. An Excel workbook that creates business units, departments, users, appetite, committees, policies, risks, KRIs and controls in one pass — the fastest way to go from a spreadsheet to a populated register on day one.
- Everything above is on the phone as well as the desk, in English and Arabic, and the mobile apps keep working through a poor connection.

Who Does What

Rukn ERM has six roles, and they follow the Three Lines Model rather than a seniority ladder. Permissions are fixed and enforced on the server, so a role cannot be talked into doing something it should not.

- Administrator — the account holder, set when the organisation registers. Manages people, roles, the taxonomy, the subscription and imports, and can reach every module. There is one at a time, and the role is handed over rather than granted.
- Executive — sets appetite and tolerance in Step 4 and reads everything. Owns no records: drawing the line and then working inside it would be the same hands doing both.
- Internal Auditor — the third line. Plans audits, raises findings, attaches the evidence behind them, and verifies or reopens them in Step 9. Cannot create or own risks, actions, incidents, controls or indicators, because a finding written by someone who could also edit the record it concerns is not independent.
- Risk Manager — the second line. Runs the programme: risks, actions, incidents, controls, indicators, governance and compliance, and the activity log. Cannot set appetite or raise audit findings.
- Risk Owner — the first line. Creates and owns risks, actions and incidents, records readings for their own indicators, and attaches evidence to their own records.
- Support Staff — also the first line. Reports incidents, completes the actions assigned to them, and attaches evidence to what they work on. Cannot create or own risks, which is what separates the role from a Risk Owner.

Keeping the Cycle Turning

The ten steps in this guide are written in sequence because that is how a risk moves through the system the first time. In practice, once a risk register is established, you will spend most of your time in Steps 9 and 10 — testing controls and monitoring — with occasional trips back to earlier steps when monitoring surfaces something new, appetite changes, or objectives shift.

That feedback — Step 7 back to Step 5 when a treatment isn't enough, and Step 10 back to Step 1 when the environment changes — is what makes this a cycle rather than a checklist. Rukn ERM keeps every step's data linked, so a change at any point shows up wherever else it matters: rate a control and the residual score of every risk it covers moves, and if that crosses the appetite line the executives hear about it without anyone sending an email.

Quick Reference

#	Step	Typically owned by	Key artifact produced
1	**Objectives**	Objective owner (outside Rukn ERM)	Objectives register, held outside the app
2	**Risk Identification**	Risk owner	Risk register entry
3	**Risk Assessment**	Risk owner / Risk manager	Inherent score, 1–25
4	**Board Sets Appetite**	Executive	Appetite statement per category
5	**Treatment Decision**	Action owner	Action on the risk
6	**Control Design**	Control owner	Control, typed and mapped to risks
7	**Residual Risk Check**	Risk owner / Risk manager	Residual score, derived from controls
8	**KRI Design**	Risk owner	Thresholded KRI
9	**Implementation & Testing**	Control owner / Internal auditor	Control test, rating and attached evidence
10	**Continuous Monitoring**	Risk manager / Executive	Dashboard, notifications and reports