FREE CONSULTANT

PROFESSIONAL PRACTICAL GUIDE

Methodologies for Determining

Risk Appetite and Risk Tolerance

A practical guide aligned with **ISO 31000:2018** and **COSO ERM 2017**
referencing the requirements of the Global Internal Audit Standards **(GIAS 2024)**

Document type	Applied professional guide
Domain	Risk governance, enterprise risk management & internal audit
Version	First edition — 1.0
Language	English (with Arabic terms)
Prepared by	**Ahmad Abumanei**
Classification	Public

Free Consultant | free-consultant.com

Contents

Preface: Purpose and Scope of the Guide

This guide sets out a practical methodology for determining risk appetite and risk tolerance, moving them from the level of general statements to numeric limits that bind day-to-day decisions. The need for it stems from a recurring observation in practice: many organizations own a "risk appetite statement" hanging on the wall that changes no one's behaviour, because it was never translated into numbers and never linked to indicators or escalation paths. That is precisely where this guide intervenes.

The content rests on three complementary references: **ISO 31000:2018** as the backbone of the risk management process, the **COSO ERM 2017** framework where the discussion concerns embedding risk into strategy and performance, and the **Global Internal Audit Standards (GIAS 2024)**, effective 9 January 2025, to frame the role of internal audit toward the appetite framework. Wherever relevant, the reference is named by clause or standard, not by a vague appeal to "best practice."

Audience and how to read it

The intended audience comprises boards and their committees, the risk and compliance functions in the second line, and internal auditors concerned with assessing the appetite framework. The sections are arranged to be read sequentially: from concepts, to the normative basis, to methodologies, then building the cascade, calibration and visual representation, linkage to indicators, the role of internal audit, and finally common pitfalls and the roadmap. Each section can also stand alone as a quick reference.

> **How to use this guide in practice**
> The template tables provided (appetite statement by category, indicator card, risk-and-control matrix) serve as ready-to-complete templates, once calibrated to the organization's sector, size and maturity.
> The diagrams are not decoration; each presents a mental model that compresses a lengthy explanation: the exposure axis, the three lines, the cascade, the appetite line on the heat map, and the escalation mechanism.

Section 1: Conceptual Framework and Core Terminology

Confusing the terms is not a linguistic luxury; it is a practical source of failure. When "appetite," "tolerance" and "capacity" are used as synonyms, each loses its function: the appetite statement turns into a slogan, and the limits meant to discipline decisions disappear. We therefore begin with a precise separation of four distinct but interrelated concepts.

Risk Appetite

The amount and type of risk the organization is willing to accept or pursue, voluntarily, in pursuit of its objectives. It is a strategic choice, not an imposed constraint: a conscious decision about how much risk is worth the expected reward. It is articulated at board level and varies by risk category; an organization may have a high appetite in a category such as expansion into new markets, while having no appetite at all in another such as regulatory breaches or worker safety.

Risk Tolerance

The acceptable degree of deviation around objectives; that is, the quantitative limits that translate qualitative appetite into a permissible range before a situation is deemed a breach requiring escalation. If appetite is the “target level,” tolerance is the “acceptable band around it.” When an organization accepts a defined margin of error in a particular financial metric, it is thereby declaring its tolerance for that metric.

Risk Capacity

The absolute maximum amount of risk the organization can bear without threatening its survival, solvency or core obligations. Capacity is governed by resources, capital, liquidity and regulatory constraints, and is relatively fixed in the short term. The governing rule here is categorical: appetite must always sit below capacity, with a sufficient buffer between them to absorb unexpected shocks.

Risk Criteria and Acceptable Deviation

Risk criteria are the explicit measures and thresholds against which the level of risk is measured and evaluated: the likelihood and impact scales with their descriptive anchors, the matrix, the aggregation rules, and the position of the appetite line. Under ISO 31000 these criteria are defined at an early stage (**clause 6.3.4**) before any risk is recorded; beginning assessment before setting the criteria is among the most common methodological errors.

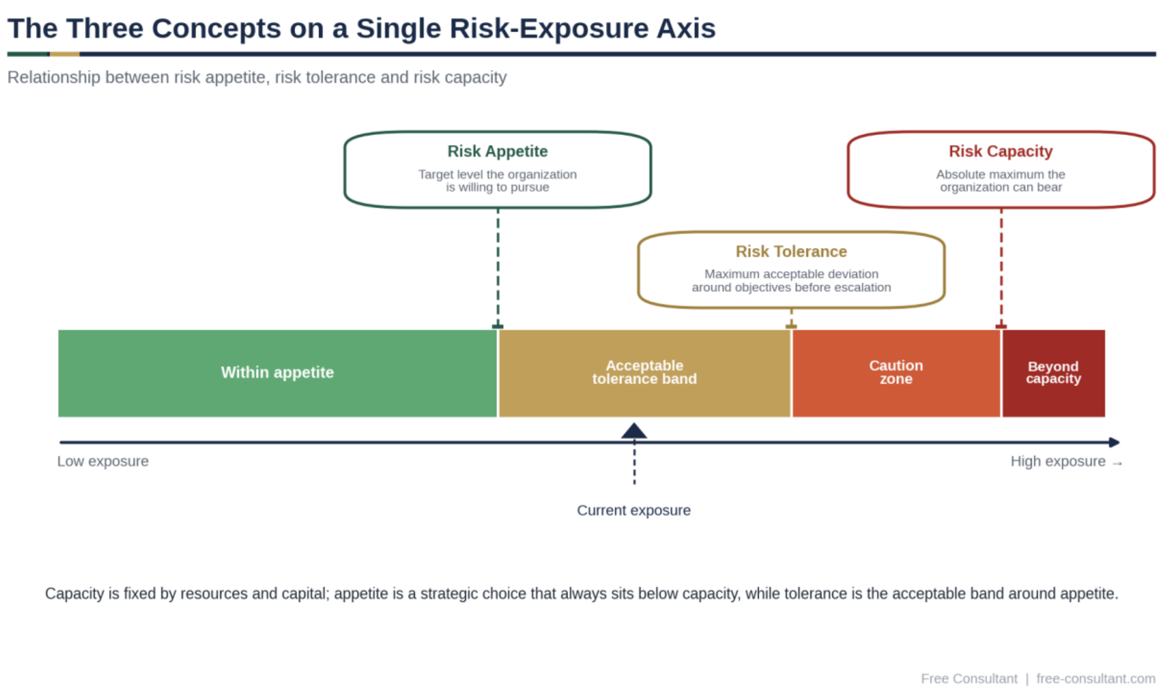

Figure 1: The three concepts on a single risk-exposure axis — appetite below capacity, tolerance a band around appetite

A brief comparison of the four concepts

Concept	Question it answers	Who sets it	Nature	Brief example
Risk Appetite	How much do we want to risk voluntarily?	The board	Qualitative strategic choice	High appetite for growth, none for non-compliance
Risk Tolerance	What deviation is acceptable before escalation?	Second line, approved by the board	Quantitative limits around objectives	Earnings volatility within a defined range
Risk Capacity	What is the most we can bear?	Governed by resources and capital	A fixed, objective ceiling	Maximum loss before solvency is threatened
Risk Criteria	How do we measure and compare risks?	Second line	Scales, thresholds and rules	A 5×5 matrix and the appetite line

Professional note: the practical difference between appetite and tolerance

Appetite expresses the “destination,” and tolerance the “edges of the road.” A board that declares a limited appetite for credit risk without setting a numeric tolerance — such as a maximum acceptable default rate — has drawn a destination without edges; the result is operational decisions that vary with each individual’s judgement. Numeric translation is what makes appetite binding.

Section 2: The Normative and Governance Basis

Risk appetite is not built in a vacuum; it has a normative reference that determines where it sits, who owns it, who monitors it, and who provides assurance over it. Here we review the three governing references and clarify the place of each.

First: ISO 31000:2018 — the backbone of the risk process

The standard places appetite and tolerance within "risk criteria" in **clause 6.3.4** of the risk management process — that is, in the stage of defining scope, context and criteria, before identification and analysis. In the treatment stage (**clause 6.5**), residual risks are compared against these criteria to decide whether they are within the acceptable range or require further treatment. The standard's principles (clause 4) remind us that criteria should be "customized" to the organization and "based on the best available information," not copied from a ready-made template.

Second: COSO ERM 2017 — the strategy lens

When the discussion concerns embedding risk into strategy and performance, the **COSO ERM** framework offers the most precise reference. Its second component, "Strategy and Objective-Setting," explicitly includes **Principle 7 "Defines Risk Appetite"** and Principle 8 "Evaluates Alternative Strategies." **Principle 14** obliges the organization to develop a "portfolio view" of risk, since risks interact with one another, so it is not enough to view them individually but rather to estimate the overall profile at the entity level.

Third: GIAS 2024 — internal audit's role toward appetite

The Global Internal Audit Standards are organized into five domains and fifteen principles. With respect to risk appetite, internal audit's role is established in three principal locations, anchoring a fundamental principle: internal audit does not set appetite, but provides assurance over its existence, adequacy and the effectiveness of compliance with it, thereby preserving its independence.

- **Standard 9.1 "Understanding Governance, Risk Management, and Control Processes":** the chief audit executive must develop an understanding of the organization's objectives, strategies and risks — including its risk appetite — as a basis for building a risk-based plan.
- **Standard 9.4 "Internal Audit Plan":** the plan must rest on a risk-based methodology consistent with the organization's risk appetite and the board's priorities, so that audit effort is directed toward what exceeds or approaches the limits.
- **Domain V — Principle 13 "Plan Engagements Effectively":** at the individual engagement level, the risk of the activity under audit is assessed relative to its objectives and against the organization's appetite and tolerance, from which the engagement's objectives, scope and criteria are derived.

This is complemented by the **Three Lines Model (IIA 2020)**, which distributes the roles: the governing body approves appetite and oversees, the first line owns the risks and applies decisions within the limits, the second line designs the framework and monitors compliance, and the third line provides independent assurance.

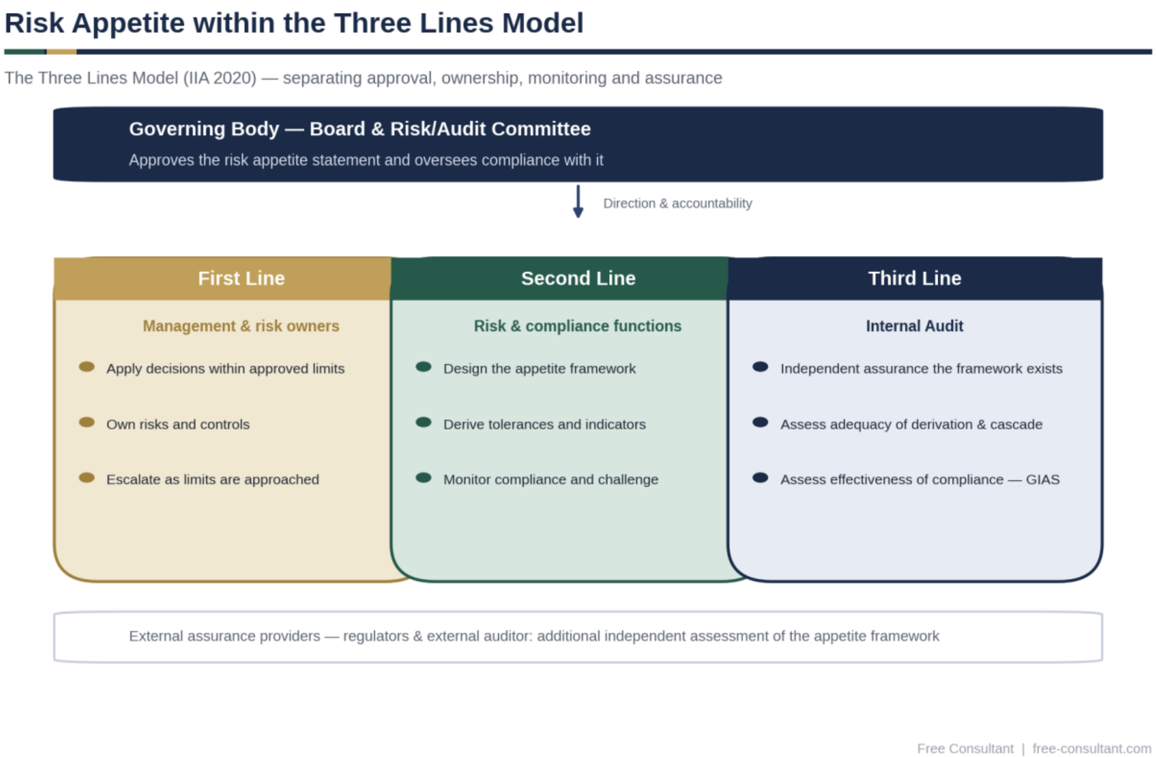

Figure 2: The position of risk appetite within the Three Lines Model — separating approval, ownership, monitoring and assurance

Professional note: internal audit's independence toward appetite

If internal audit undertakes to draft the appetite statement or derive its limits, it later audits its own work, and the objectivity required by Domain II of GIAS collapses. The sound role is advisory at the design stage with explicit disclosure, and assurance at the assessment stage, with separation between them in time and documentation.

Section 3: Methodologies for Determining Risk Appetite

There is no single methodology suitable for every organization. The choice is governed by the maturity of risk management, the nature of the sector, the availability of data, and the materiality of the decision. In practice, two or more methodologies are usually combined. We present six methodologies, then compare them in a single table.

3-1 The qualitative, statement-based (top-down) methodology

It begins from the top: the board drafts qualitative appetite statements for each risk category based on strategic objectives and values, then those statements are decomposed downward into tolerances and indicators. Suitable for organizations in the early stages of maturity, or when quantitative data is scarce. Its strength lies in speed of application and clarity of message; its weakness in the susceptibility of qualitative statements to interpretation unless subsequently tied to numbers.

3-2 The quantitative, capacity- and capital-based (bottom-up) methodology

It begins from the bottom: loss-bearing capacity is estimated from capital, liquidity and the required safety margin, then this capacity is allocated across risk categories as limits. It draws on tools such as **Value at Risk (VaR)** and **Expected Shortfall**, and estimating **Expected Loss** through its components (PD, LGD and EAD). Suitable for financial sectors and data-rich institutions, offering high precision, but requiring modelling capabilities and data that may not be available to every organization.

3-3 The hybrid methodology and dual calibration

It combines the two approaches: the board’s ambition is articulated top-down and tested against what the data and capacity permit bottom-up, so the two converge on a “calibrated” appetite that is applicable and measurable. This is the most mature practice, because it prevents unrealistic ambition on the one hand, and unjustifiably conservative limits on the other.

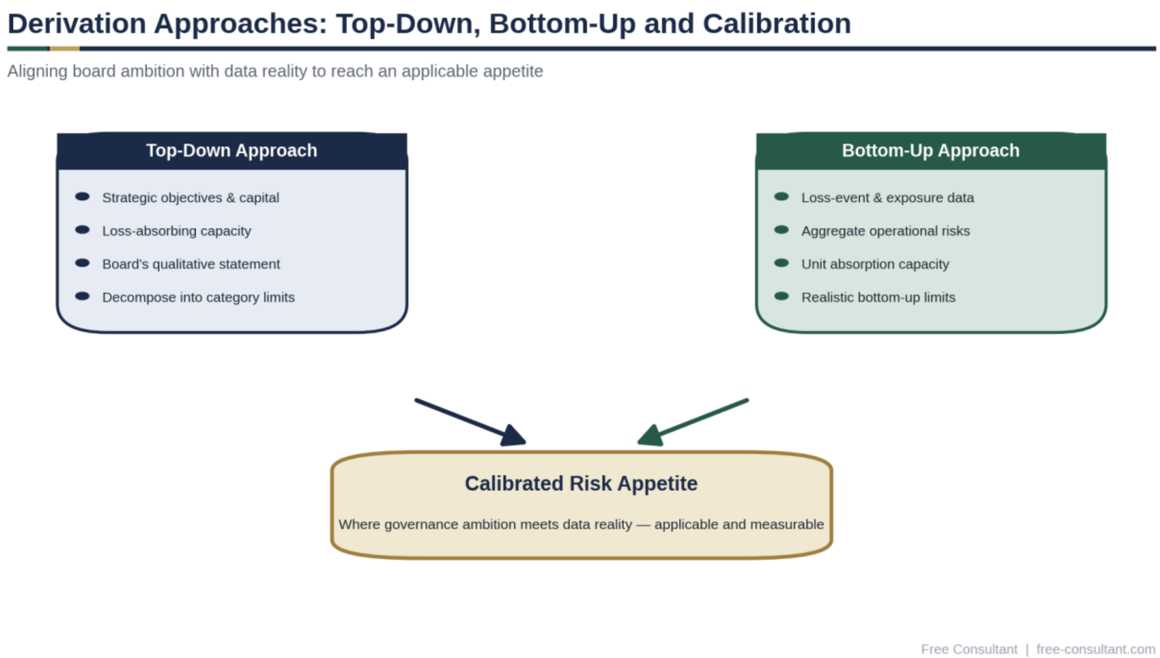

Figure 3: The convergence of the top-down and bottom-up approaches on an applicable, calibrated appetite

3-4 The risk-criteria and matrix methodology

Appetite is determined in practice by calibrating the likelihood and impact measures and drawing an “appetite line” on a 5×5 matrix, such that risks below the line are deemed acceptable with no further action, and those above it require treatment or escalation. This methodology turns appetite from text into a visual limit linked to every risk in the register, and we detail it in Section 5.

3-5 Benchmarking, scenario analysis and stress testing

Appetite is calibrated by reference to peer levels in the sector (benchmarking) — with caution toward differences in size and context — and its robustness is tested through **scenario analysis** and **stress testing**, which reveal whether the limits hold under extreme yet plausible conditions. This is complemented by **reverse stress testing**, which starts from the point of failure and works backward to identify the scenarios leading to it — a powerful tool for calibrating capacity and the maximum tolerance limit.

3-6 Workshops, the Delphi method and structured judgement

When data is scarce or the risk relates to matters hard to quantify, such as reputation or strategy, structured workshops bringing together stakeholders are used, or the Delphi method to reach expert consensus through successive rounds. The condition for success here is discipline: agreed descriptive anchors for the measures, documentation of assumptions, and avoiding the dominance of higher-ranking voices over collective judgement.

Comparison of methodologies

Methodology	When to use	Outputs	Key limitations
Qualitative (top-down)	Early maturity or scarce data	Qualitative appetite statements per category	Open to interpretation unless quantified

Methodology	When to use	Outputs	Key limitations
Quantitative (bottom-up)	Financial sectors, rich data	Limits derived from capital	Requires modelling capability and data
Hybrid	Generally the most mature practice	Calibrated, applicable appetite	Greater coordination effort
Matrix & appetite line	Linking appetite to the register	A visual limit per risk	Sensitive to scale-calibration quality
Scenarios & stress testing	Testing the robustness of limits	Confirmation limits hold, or adjustment	Depends on the quality of scenario assumptions
Workshops & Delphi	Risks hard to quantify	Documented expert consensus	Prone to group bias

Section 4: From Statement to Limit — Building the Cascade

Whatever methodology is chosen, appetite is complete only when it cascades downward from a board-level statement to a limit that governs an operational decision. This cascade is what turns appetite from intent into an effective governance tool.

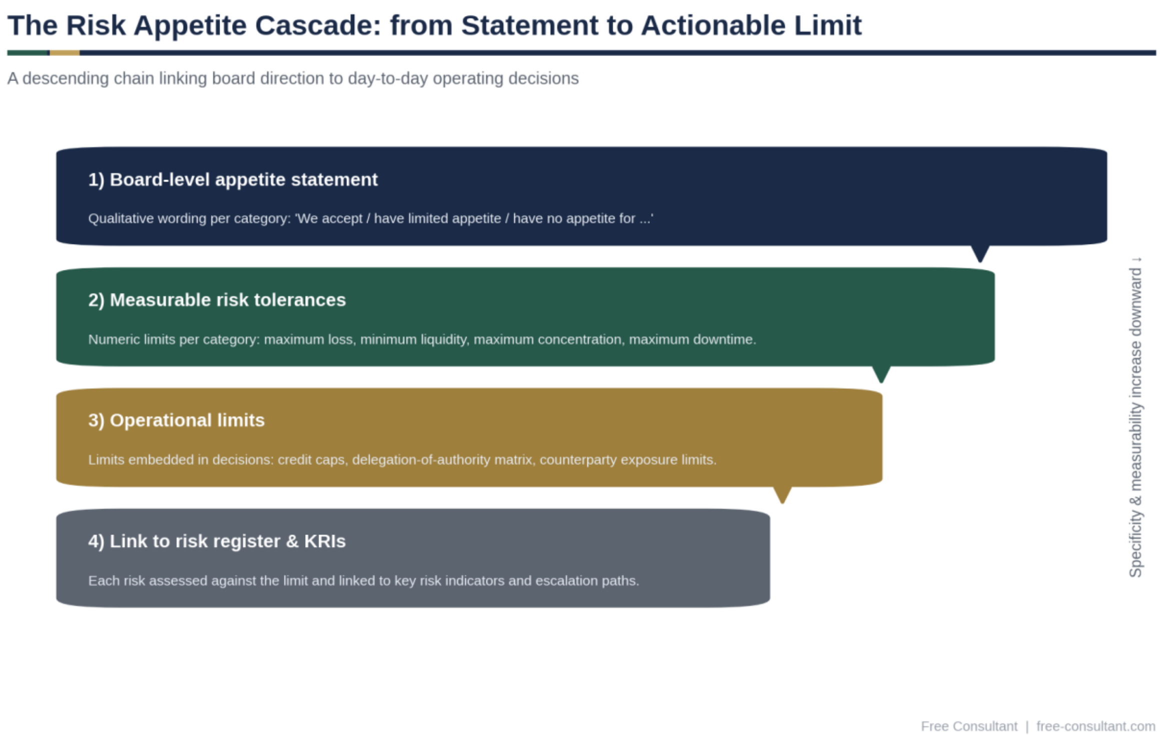

Figure 4: The risk appetite cascade: a descending chain from qualitative statement to actionable limit

1) The board's qualitative statement — correct articulation

For each risk category, an explicit stance is articulated in one of three forms: "We accept risk in …," "We have limited appetite for …," or "We have no appetite for …," coupled with the purpose. A fundamental error is for the statement to be "low appetite for everything"; this is not an appetite statement but **an evasion of it**, since each category requires an independent stance proportionate to its role in creating value.

2) Measurable tolerances

Each qualitative statement is translated into a numeric limit for the category: maximum acceptable loss, minimum liquidity ratio, maximum concentration for a customer or sector, maximum downtime for critical systems, maximum turnover of core staff. These limits are the threshold separating the acceptable situation from the one requiring escalation.

3) Operational limits

Tolerances are broken down into limits embedded in day-to-day decisions: credit caps per segment, a delegation-of-authority matrix linking decision size to the level of approval, counterparty and supplier exposure limits, inventory or market-position caps. At this level appetite becomes tangible in the employee's work, not merely a document held by senior management.

4) The rule of linking to the register and indicators

Each risk in the register is assessed against the relevant limit, and any breach is flagged explicitly with its escalation path. The register thus becomes a living tool for measuring compliance with appetite, not a static list. Key risk indicator thresholds are also derived from the tolerances, as Section 6 will show.

An integrated template for the appetite statement by category

The following table is a practical template linking, in a single row per category: the appetite stance, the quantitative tolerance measure, and the operational limit and associated indicator. It is intended to be calibrated to the organization’s reality.

Risk category	Appetite stance	Tolerance measure (example)	Operational limit / indicator
Strategic	Calculated appetite to support growth	Maximum deviation from the revenue plan within an approved range	Review gates for major initiatives
Financial & liquidity	Limited appetite	Minimum liquidity ratio and maximum leverage	Periodic liquidity reports with alert thresholds
Operational	Low appetite	Maximum downtime for critical systems	Recovery-time indicator against target
Regulatory compliance	No appetite	Zero deliberate material breaches	Breaches and regulatory-findings indicator
Cyber	No appetite for severe risks	Zero breach of critical data	Patch age and response time
Reputation	Very limited appetite	No events affecting public trust	Media monitoring and material complaints

Section 5: Calibration and Visual Representation

The credibility of appetite depends on the quality of calibration of the measures against which it is gauged. A matrix with vague measures yields arbitrary classifications, however elegant it looks. Descriptive anchors are therefore defined for each level of likelihood and impact, then the appetite line is drawn on them.

Calibrating the likelihood and impact measures

For each level on a 1–5 scale, a descriptive anchor is defined to enable consistent application. Impact is not left as an abstract notion but tied to tangible limits across multiple dimensions (financial, operational, compliance, reputation), as in the following table. Likelihood is tied to an expected frequency or a percentage range, not to loose words such as “rare” or “likely” without definition.

Level	Financial dimension (example)	Operational dimension	Regulatory / reputation dimension
5 — Severe	Loss exceeding the critical threshold	Extended outage of critical systems	Material breach and wide reputational damage
4 — Major	Large loss below the critical threshold	Wide disruption but recoverable	Significant regulatory finding
3 — Moderate	Limited, tangible loss	Partial disruption of important services	Recurring complaints of limited impact
2 — Minor	Small loss	Short disruption of limited impact	Limited internal impact
1 — Negligible	Immaterial financial impact	Transient disturbance	No external impact

Drawing the appetite line on the heat map

After calibrating the measures, the value of each cell (likelihood × impact) is computed and coloured according to the five-tier classification. The appetite line is then drawn, separating the acceptance zone below it from the breach zone above it. The position of the line is a visual embodiment of the board’s decision: the higher the line, the wider the accepted area — i.e. the greater the appetite. This line is linked to a response rule: what is below it is monitored, and what is above it requires treatment or escalation per the tolerance.

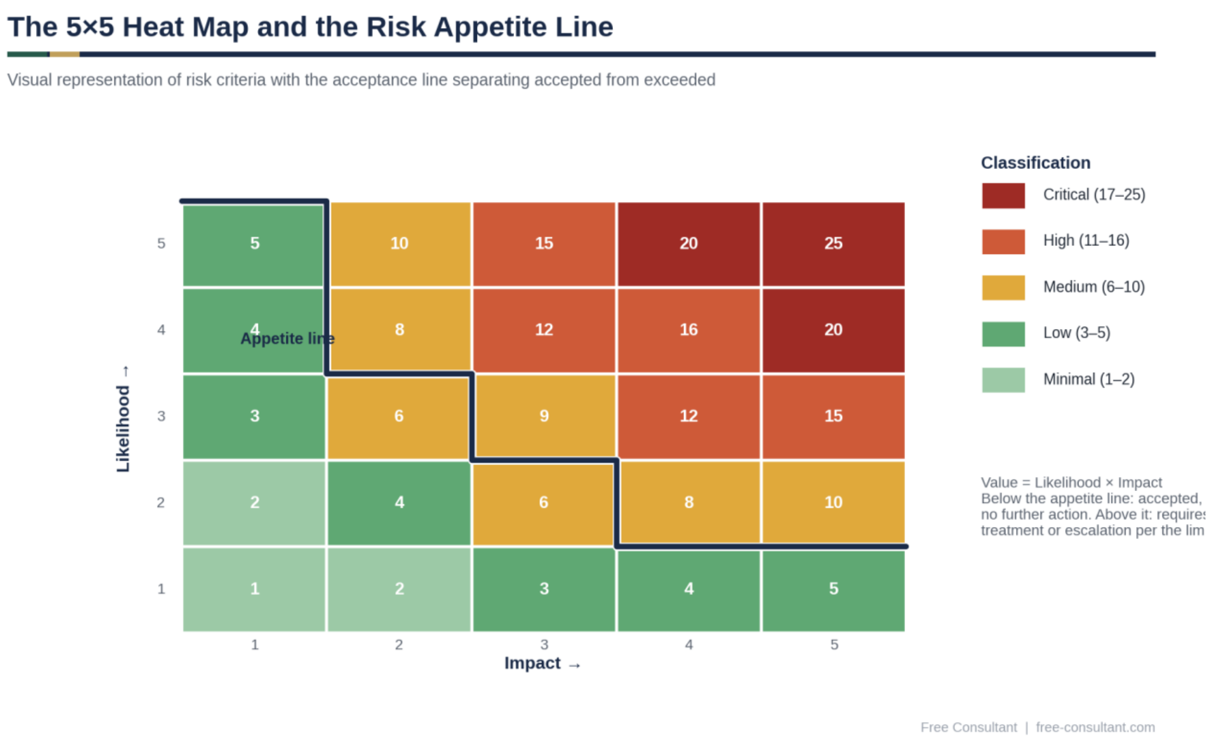

Figure 5: The 5×5 heat map and the appetite line separating the accepted from the exceeded

A note on calibration

The items of the treatment plan and the indicator thresholds must correspond to the same scale anchors used in the matrix; using different anchors in different places robs the framework of its consistency and renders the classifications incomparable.

Section 6: Linking to Key Risk Indicators and Escalation Paths

Appetite that is not monitored is not managed. Tolerances are therefore translated into **key risk indicators (KRIs)** with green/amber/red thresholds derived directly from the limit, coupled with a clear escalation path: who is notified at amber, who acts at red, and within what timeframe.

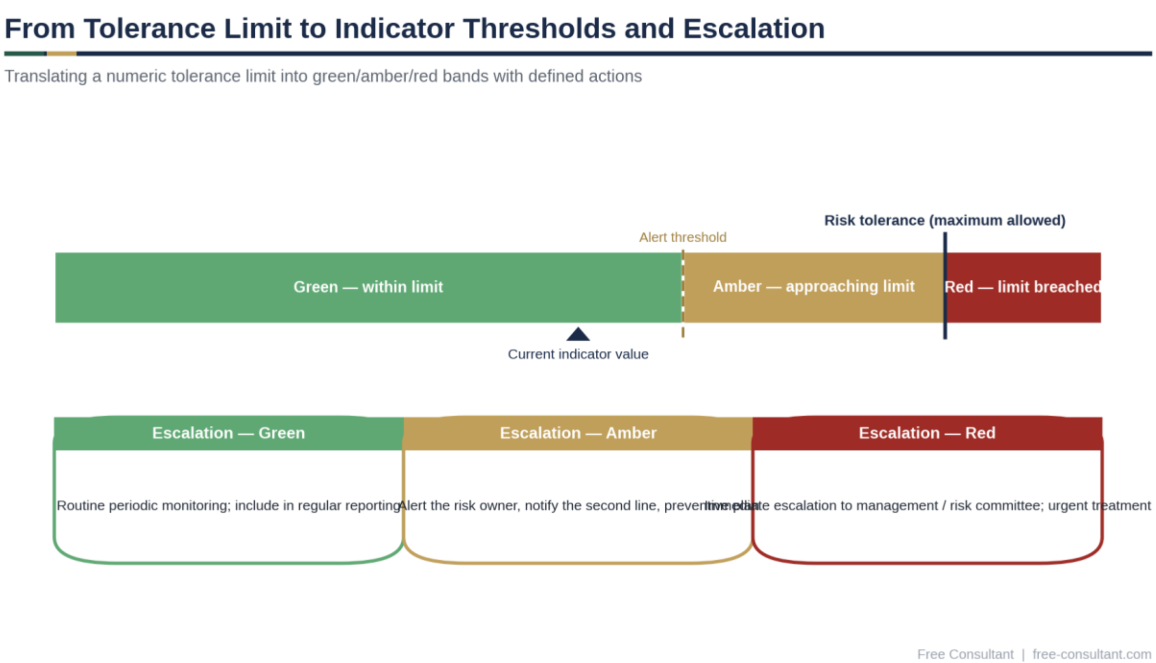

Figure 6: Deriving indicator thresholds from the tolerance limit and linking them to escalation actions

Indicator definition card

No indicator is adopted without a complete definition card that ensures it is applicable and reviewable. The following table sets out the mandatory fields for each indicator.

Field	Required content
Indicator name	Specific and, where possible, leading — predicting the risk, not merely recording it
Associated risk	The number(s) of the risk in the register
Definition & formula	The precise equation for computing the indicator
Data source & owner	The system or report and the responsible person
Frequency	Daily / weekly / monthly / quarterly
Thresholds	Green/amber/red in numbers, derived from the tolerance
Escalation path	Who is notified, who acts, and within what timeframe

A limited number of decision-relevant indicators is preferred — around 5–10 per major category — over dashboards crowded with token indicators, combining lagging indicators such as incident counts and losses with leading indicators such as overdue maintenance, vacancy rates, near-misses and patch age.

Section 7: The Role of Internal Audit in Assuring the Appetite Framework

As the third line, internal audit provides independent assurance over the appetite framework through five integrated assessment axes, from which the key assurance questions and the engagement programme are derived.

1. **Existence:** Is there a board-approved appetite statement covering the material risk categories?
2. **Derivation:** Have the qualitative statements been translated into quantitative tolerances with a clear basis in capacity, capital and scenarios?
3. **Cascade:** Have the limits descended into operational limits embedded in authorities and day-to-day decisions?
4. **Compliance:** Are breaches actually monitored and escalated per the approved paths, or do they remain on paper?
5. **Review governance:** Is the framework reviewed periodically and updated upon material changes in strategy or market?

A mini risk-and-control matrix on appetite governance

The following table is a miniature template of a risk-and-control matrix focused on the governance of the appetite framework itself, with a reference to the relevant GIAS standard for each item — a template that can be expanded into a full audit programme.

Risk	Root cause	Expected control	GIAS ref.
Absence of an approved appetite statement	Weak board oversight of risk	Documented approval of the appetite statement and periodic review	Principle 9 / 9.1
A qualitative statement without quantitative limits	Failure to derive tolerances	Documented tolerances linked to each category	9.4
Limits disconnected from decisions	Limits not cascaded operationally	Delegation-of-authority matrix and embedded caps	Principle 13
Breaches not escalated	Absence of a monitoring and escalation mechanism	Indicators with thresholds and effective escalation paths	Principle 13 / 14
An out-of-date framework	Absence of periodic review	Annual review and upon material change	Principle 9 / 12

Linking working papers to the standards

When documenting this engagement, each observation in 5C form (Criteria / Condition / Cause / Consequence / Recommendation) is mapped to its assessment axis and the corresponding GIAS standard, making the report defensible before the audit committee and the external quality reviewer, and consistent with Principle 15 on communicating results and following up action plans.

Section 8: Common Pitfalls and Leading Practices

Specific errors recur in practice that hollow out the appetite framework. The following table pairs each common error with the corresponding leading practice, in practical wording ready for direct application.

Common error	Corresponding leading practice
“Low appetite for everything” to evade the choice	An explicit, differentiated stance per category according to its role in creating value
A qualitative statement on the wall with no numeric limits	Deriving measurable tolerances for each category
Limits that never reach day-to-day decisions	Cascading limits into operational caps and a delegation-of-authority matrix
An elegant matrix with vague measures	Defined descriptive anchors for each level across multiple dimensions
Breaches monitored but not escalated	Thresholds and escalation paths with defined responsibilities and timeframes
A framework written once then forgotten	Periodic review and upon every material change in strategy or market
Internal audit drafting appetite and deriving its limits	An independent assurance role with a clear separation of duties
Copying an appetite statement from another organization	Calibration to the organization’s context, capacity and sector

Section 9: Implementation Roadmap

Embedding the appetite framework is a phased process, not a single event. The following roadmap presents a logical sequence from establishment to embedding and independent assurance, to be calibrated in time to the organization's size and maturity.

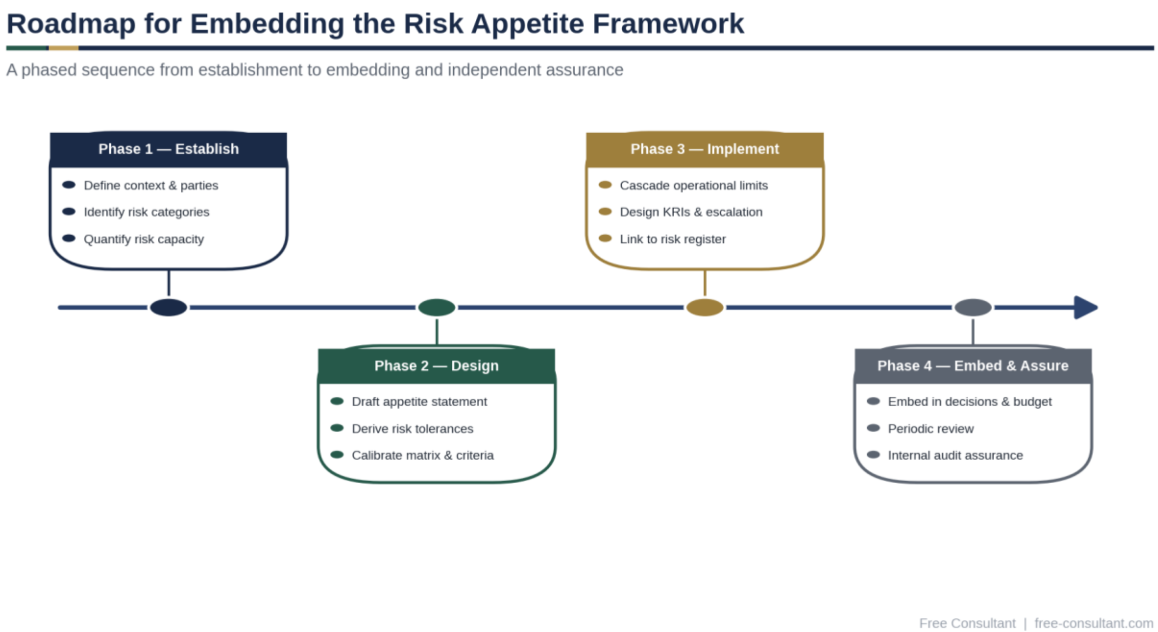

Figure 7: A roadmap for embedding the risk appetite framework across four phases

- **Phase 1 — Establish:** Define the internal and external context and the stakeholders, fix the material risk categories, and quantify capacity from resources and capital.
- **Phase 2 — Design:** Draft the appetite statement per category, derive the quantitative tolerances, and calibrate the matrix, risk criteria and the appetite line.
- **Phase 3 — Implement:** Translate limits into operational caps and authorities, design indicators with their thresholds and escalation paths, and link to the risk register.
- **Phase 4 — Embed & Assure:** Embed the framework in decisions and the budget, review periodically, and subject it to independent internal-audit assurance per GIAS.

Conclusion

The true value of risk appetite lies not in the existence of a document but in its capacity to change decisions. When appetite cascades from a board-level qualitative statement to a measured tolerance, to an operational cap embedded in authorities, to an indicator with a threshold and an escalation path, it becomes a living tool that directs resources, disciplines boldness and protects value. At that point internal audit finds a framework it can assess, rather than a slogan that is hard to grasp.

This guide has been careful to tie each step to its normative reference — ISO 31000 in building the process, COSO ERM in connecting it to strategy, and GIAS in defining the role of the third line — because normative discipline is what separates a framework that withstands audit from one that collapses at the first test. The key to success remains calibration to each organization's reality: its sector, size, maturity and capacity; no ready-made template substitutes for that effort.

Appendix (A): Bilingual Glossary of Terms

English Term	المصطلح بالعربية
Risk Appetite	الرغبة في المخاطرة
Risk Tolerance	حدود تحمّل المخاطر
Risk Capacity	القدرة على تحمّل المخاطر
Risk Criteria	معايير المخاطر
Inherent Risk	الخطر الكامن
Residual Risk	الخطر المتبقي
Likelihood	الاحتمالية
Impact / Consequence	الأثر
Risk Heat Map	الخريطة الحرارية للمخاطر
Risk Matrix	مصفوفة المخاطر
Key Risk Indicator (KRI)	مؤشر المخاطر الرئيسي
Threshold / Trigger	الحد / المحفّز
Escalation	التصعيد
Scenario Analysis	تحليل السيناريوهات
Stress Testing	اختبارات الضغط
Value at Risk (VaR)	القيمة المعرضة للخطر
Three Lines Model	نموذج الخطوط الثلاثة
Portfolio View of Risk	النظرة الشمولية لمحفظة المخاطر
Global Internal Audit Standards (GIAS)	المعايير الدولية للتدقيق الداخلي

Appendix (B): Normative References

1. ISO 31000:2018 — Risk management — Guidelines.
2. ISO Guide 73:2009 — Risk management — Vocabulary.
3. ISO/IEC 31010:2019 — Risk management — Risk assessment techniques.
4. COSO (2017) — Enterprise Risk Management: Integrating with Strategy and Performance.
5. COSO (2013) — Internal Control — Integrated Framework.
6. The Institute of Internal Auditors (2024) — Global Internal Audit Standards (effective 9 January 2025).
7. The Institute of Internal Auditors (2020) — The Three Lines Model.
8. The Institute of Internal Auditors — Guidance on Risk Appetite and Risk Tolerance.

About the Author

Ahmad Abumanei

Ahmad Abumanei
CIA · FMVA · CBCA · CFM · CRCM · FTIP

Ahmad has built extensive practical experience in corporate governance, enterprise risk management, internal control, and regulatory compliance, across a range of organizations in the Gulf and Jordan. His focus is on turning theoretical frameworks into practical, applicable tools, and on producing high-quality professional deliverables that genuinely serve the decision-maker rather than tick a box.

He combines depth in governance, risk, and compliance (GRC) and enterprise risk management (ERM) with experience in information systems auditing and regulatory reviews before supervisory authorities in the region. His work draws on the recognized international standards and frameworks, from ISO 31000 and the COSO framework to the Global Internal Audit Standards issued by The Institute of Internal Auditors, with care to align them with the local regulatory environment in each country.

He holds a number of international professional certifications, among them the Certified Internal Auditor (CIA), the Financial Modeling and Valuation Analyst (FMVA), and the Commercial Banking and Credit Analyst (CBCA), alongside qualifications in financial management, risk, and compliance. This breadth gives his perspective an integrative angle that connects risk to finance and to governance at once.

Contact info

Email: Ahmad.abumanie@outlook.com

About the Free Consultant platform

A professional platform founded to act as an intermediary connecting certified specialists in internal audit and risk management with consulting firms and small and medium-sized enterprises, particularly in the GCC market. The platform enables access to specialized expertise in governance, risk and compliance with flexibility and efficiency.

Website: free-consultant.com

FREE CONSULTANT · Professional knowledge within reach of those who seek it