THE CHARTERED INSTITUTE OF LOAN & RISK MANAGEMENT OF NIGERIA

PAPER PRESENTATION

BY

DR. TARI OGOLA

Risk Management Consultant

EMPOWERING RISK MANAGEMENT PROFESSIONALS: A CLOSER LOOK AT THE BASICS OF RISK MANAGEMENT

@

16TH ANNUAL RISK PROFESSIONAL INTERNATIONAL CONFERENCE

NICON LUXURY HOTEL,

AREA 11, GARKI

ABUJA.

NOVEMBER 27, 2026.

INTRODUCTION

Risk management is not simply the identification of things that might go wrong. It is a disciplined way of understanding uncertainty, making informed choices and ensuring that the organisation takes risks deliberately, within agreed boundaries and with appropriate safeguards. Effective risk management supports the achievement of business objectives; it does not exist merely to prevent activity or produce compliance paperwork.

This guide develops five practical themes for risk management professionals: setting risk appetite, establishing an effective control framework, understanding the business and its transactions, maintaining independent risk oversight, and using artificial intelligence responsibly. A case study on the collapse of Barings Bank brings these themes together by showing how weak controls, ignored warnings and compromised challenge can combine to produce a catastrophic outcome.

1. RISK APPETITE: SETTING THE BOUNDARIES

A Risk Appetite Statement (RAS) is a formally approved document that describes the amount and types of risk an organisation is willing to accept in pursuit of its objectives. It translates strategy into practical boundaries. These boundaries may be qualitative—for example, stating that certain conduct or activities are unacceptable—or quantitative, expressed through measurable limits, thresholds and tolerances. Risk appetite is not a declaration that the organisation wants to take risk indiscriminately. It is a statement of the level of exposure leadership is prepared to accept, having considered the organisation's objectives, capacity, resources and operating environment. It gives management and employees a common reference point when evaluating decisions and emerging exposures.

How the RAS guides core risk tools

- Risk and Control Self-Assessment (RCSA): The RAS provides a benchmark for deciding whether inherent and residual risks are acceptable. Where residual exposure exceeds the approved appetite, teams should consider strengthening controls, changing the activity or implementing an action plan.
- Key Risk Indicators (KRIs): Appetite is translated into thresholds and escalation triggers. KRIs help the organisation identify increasing exposure early, before it becomes a material breach or loss.
- Risk register: The RAS helps teams rate and prioritise risks, identify appetite breaches, assign clear owners and monitor treatment plans.
- Loss database: Actual incidents and losses provide evidence about where exposures or controls may have fallen outside expectations. Patterns in loss data can inform improvements to controls and a review of the organisation's appetite.

THE CONNECTION RAS → RCSA → KRIs and Risk Register → Loss Data → Review and refine appetite. The tools generate evidence; the RAS provides the benchmark for judging whether risk is acceptable. A useful RAS must be understood and used, not merely approved and filed. It should inform business planning, product decisions, risk assessments, monitoring and escalation. It should also be reviewed when the organisation's strategy, products, markets or risk environment materially change.

TOPIC 2

WHY A CONTROL FRAMEWORK MATTERS

Risk management works best when controls are clear, consistent, proportionate and supported by accountable ownership.

A control framework is a structured set of policies, procedures, controls, responsibilities and monitoring arrangements that helps an organisation manage risk consistently and effectively. It establishes how risks are addressed in practice: who is responsible, what safeguards must operate, how performance is monitored and what happens when a control fails. Without a coherent framework, control activities can become fragmented. Different teams may apply different standards, responsibilities may be unclear, important risks may fall between departments, and management may receive inconsistent information. A framework connects individual controls to the organisation's broader risk objectives.

2.1 Clear roles and ownership

An effective framework distinguishes between the people who own and manage risks, those who set standards and provide oversight, and those who provide independent assurance. Each material risk should have an identifiable owner. Each key control should have an accountable operator, a defined purpose and a way of demonstrating that it is working. Clear ownership reduces duplicated effort and prevents gaps in responsibility. It also makes remediation more effective: when a weakness is identified, the organisation knows who must act, who monitors progress and who receives an escalation if the issue remains unresolved.

2.2 Risk-informed decisions

Controls should produce information that helps decision-makers understand the exposure they are accepting. Monitoring results, exceptions, incidents and KRI movements should be reported in a way that supports timely action. Escalation points should be clear so that a developing problem is not left unresolved because staff are uncertain about when or to whom it should be reported.

The purpose is not to create reports for their own sake. Risk information should influence decisions—whether to proceed with an activity, impose additional conditions, reduce exposure, allocate resources to remediation or escalate a matter to senior management.

2.3 The danger of too little or too much control

UNDER-CONTROL	OVER-CONTROL
Gaps in checks, weak supervision and unmanaged exposure can allow errors, misconduct or losses to occur.	Duplicated checks, unnecessary approvals and excessive procedures can cause delay, cost and operational frustration.

A good framework avoids both extremes. The strength of a control should be proportionate to the nature, likelihood and potential impact of the risk. A high-impact activity may require stronger authorisation, segregation of duties and closer monitoring. A lower-risk activity may be managed through simpler checks. Applying the same level of control to every activity can waste resources and weaken attention to the risks that matter most.

2.4 What makes a control effective?

- Purpose: the control addresses a clearly identified risk and has a defined expected outcome.
- Ownership: a named role or team is responsible for operating it.
- Design: the control is capable of preventing, detecting or correcting the relevant failure.

- Operation: it is performed consistently, at the required frequency, and evidence is retained.
- Monitoring: exceptions and failures are identified, reported and remediated.

KEY TAKEAWAY The right control, with the right owner, at the right level of intensity. A control framework is effective when it supports accountability and sound decisions without unnecessarily obstructing the business.

TOPIC 3
RISK MANAGERS MUST UNDERSTAND THE BUSINESS

You cannot manage a risk properly if you do not understand it in its commercial and transactional context.

Risk management becomes meaningful when the risk professional understands how the organisation creates value, how its activities are carried out and where losses or failures can arise. A risk assessment that is disconnected from the business may identify generic risks but miss the actual points at which exposure is created. The risk manager should therefore understand the business model, follow transactions from beginning to end and challenge the assumptions on which decisions are based. This requires curiosity, commercial awareness and the ability to translate operational detail into practical risk advice.

3.1 Understand the business model

Start with the organisation's strategy and how it earns revenue. Understand its customers, products, markets, key processes, dependencies and measures of success. Consider which activities are most important to revenue generation and which relationships or resources the organisation relies on to deliver its objectives. This knowledge helps the risk manager identify where strategic, concentration, conduct and reputational risks may arise. For example, dependence on a limited number of customers, suppliers, products or markets may create vulnerabilities that are not obvious when individual transactions are considered in isolation.

3.2 Understand the transaction end-to-end

For a specific transaction, understand its purpose, the parties involved, the flow of funds, contractual terms, collateral, approval process, settlement arrangements and the expected exit or repayment. Do not stop at the proposal or the headline commercial terms. Follow the transaction through each stage and identify who performs each action. This end-to-end view can reveal hidden obligations, conflicting incentives, weak documentation, opportunities for fraud and points where a transaction could fail. It also helps the risk manager determine whether the controls proposed are relevant to the actual process.

3.3 Test the real risk

The risk professional should go beyond accepting descriptions supplied by the business. Ask what can fail, why it might fail, when failure could occur, how much could be lost, who ultimately bears the loss and whether the assumptions are realistic. Consider both the normal operating conditions and circumstances in which the transaction or process comes under pressure. These questions improve the quality of inherent and residual risk assessments. They also help determine whether controls are sufficient, whether pricing and limits reflect the exposure, and whether the recommendation to approve, decline or condition a proposal is properly supported.

3.4 Connect risk analysis to action

Risk analysis should lead to practical measures. Depending on the exposure, these may include specific controls, contractual covenants, KRIs, monitoring requirements, escalation triggers,

approval conditions and named responsibility for follow-up. The measures should address the risks identified and be capable of implementation by the people responsible. A risk report that identifies a weakness but does not explain what should happen next is incomplete. The risk manager's contribution is strongest when the analysis is translated into clear, timely and proportionate action.

THE RISK MANAGER'S TEST "How does this business make money—and what could make it lose money?" The answer should shape the assessment, the controls proposed and the advice given to decision-makers.

TOPIC 4
WHY RISK MANAGEMENT MUST BE INDEPENDENT

Close enough to understand the business. Independent enough to challenge it.

The business owns and manages the risks arising from its day-to-day activities. Risk Management provides independent oversight and challenge. This distinction is fundamental to effective governance because the people responsible for delivering business targets should not be the only people assessing whether the risks taken to achieve those targets are acceptable.

4.1 The business: first-line responsibility

The business or first line is responsible for managing risk as part of normal operations. It makes decisions within approved risk appetite, operates the controls assigned to it, identifies and reports issues, and takes action to remediate weaknesses. Risk ownership cannot be transferred to the Risk Management function simply because a risk team reviews or challenges an activity.

4.2 Risk Management: second-line oversight

The Risk Management function establishes or supports the methods and frameworks used to identify, assess and monitor risk. It independently challenges business assessments, monitors the organisation's exposure against appetite and escalates material concerns. It should be sufficiently informed about business activity to provide relevant challenge, while retaining the objectivity needed to question decisions.

4.3 Why separation matters

- Objectivity: independence reduces conflicts of interest and pressure to approve business activity at any cost in order to meet targets.
- Early warning: an independent function can identify breaches, weak controls and emerging exposures before they develop into larger problems.
- Accountability: separation prevents self-review. The business remains responsible for execution, while Risk Management challenges and oversees.
- Better decisions: leaders receive candid advice and a clearer view of the balance between risk and reward.

4.4 Independence must be supported by authority

Independence is not meaningful if risk professionals are unable to communicate concerns, obtain relevant information or escalate issues to the appropriate level. The function must have a recognised mandate and access to decision-makers. Where significant risks are identified, the organisation should have clear escalation arrangements and a process for ensuring that concerns receive proper consideration. At the same time, independence does not mean isolation. Risk Management should maintain constructive working relationships with business teams, understand commercial realities

and engage early in decisions. The objective is not to oppose every proposal. It is to ensure that decisions are made with a clear understanding of the risks and within approved boundaries.

IMPORTANT DISTINCTION Partner with the business, but never become the business. Risk Management should help the organisation take informed risks—not assume the first line's responsibility for managing them.

4.5 Practical signs of weakened independence

- Risk concerns are routinely set aside because a business unit is profitable or commercially influential.
- Risk staff are expected to approve or operate controls for activities they are meant to oversee.
- Material issues cannot be escalated without the permission of the business area being challenged.
- Risk assessments are changed to support a preferred decision rather than to reflect the evidence.

These conditions can weaken governance and make it difficult for leaders to receive an accurate picture of exposure. Independence must therefore be reflected in reporting lines, responsibilities, access, escalation arrangements and organisational culture.

TOPIC 5

ARTIFICIAL INTELLIGENCE: A RISK MANAGER'S ADVANTAGE

Faster insight. Wider visibility. Better-informed decisions—with human judgement firmly in control.

Artificial intelligence can help risk teams analyse large volumes of information, identify patterns and focus attention on issues that may require investigation. Used responsibly, it can improve the speed and breadth of risk analysis. It should be treated as a decision-support capability, not as a substitute for professional judgement, accountability or appropriate control.

5.1 Earlier warning

AI tools can help examine transaction information and KRI movements to identify unusual activity, emerging patterns or changes that may not be immediately visible through manual review. This can help risk teams direct attention to areas where exposure appears to be increasing. Any alert should still be investigated and interpreted in context; an unusual pattern is a prompt for review, not automatic proof of wrongdoing or loss.

5.2 Faster analysis of risk information

AI can assist with reviewing RCSAs, risk registers, policies and incident reports. It may help organise large volumes of material, summarise recurring themes, compare entries and flag possible omissions or inconsistencies. This can reduce time spent on repetitive review and allow professionals to devote more attention to interpretation, challenge and follow-up.

5.3 Deeper insight from loss data

Loss events often contain information about weaknesses in processes, controls or supervision. AI can help group incidents, identify anomalies and highlight recurring causes across products, processes and teams. By bringing related events together, it can help the organisation see patterns that may be difficult to detect when incidents are reviewed separately.

5.4 Stronger decision support

AI can support scenario exploration, summarise complex evidence and help management compare possible responses. For example, it may help organise the likely implications of alternative control measures or present a concise summary of information for review. The decision-maker must still

test the assumptions, consider what information may be missing and determine whether the proposed response is appropriate.

5.5 The critical caution: AI output must be verified

AI can produce an answer quickly and confidently while still being wrong, incomplete or misleading. It may misunderstand context, reproduce errors in source information, overlook important exceptions or generate conclusions that are not supported by the evidence. If its output is accepted without checking, the speed of analysis can amplify rather than reduce risk.

- Validate facts: check important figures, dates, references and statements against reliable source material.
- Challenge assumptions: ask whether the analysis reflects the actual business process and the relevant risk context.
- Check for bias: consider whether the information or method may produce unfair or distorted outcomes.
- Protect data: use AI only in ways consistent with the organisation's data protection, confidentiality and information-security requirements.
- Retain human accountability: a qualified person must review material outputs and remain responsible for decisions.

CORE PRINCIPLE AI should accelerate risk insight—not replace risk judgement. The professional remains responsible for verifying the output and deciding what action is appropriate.

CASE STUDY

THE COST OF SILENCING RISK: THE COLLAPSE OF BARINGS BANK (1995)

A classic failure of governance, control and organisational challenge.

The Barings Bank case illustrates how serious control weaknesses can remain concealed when responsibilities are poorly separated and warning signals are not acted upon. The presentation records a final loss of approximately £827 million. The collapse is a reminder that risk governance depends not only on written policies but also on the willingness and authority to enforce them.

CASE AT A GLANCE Barings Bank was founded in 1762. In 1995, losses associated with trading activities in Singapore culminated in the bank's collapse, with a reported final loss of approximately £827 million.

6.1 The control breakdown: trading and settlement in one hand

Nick Leeson, a 28-year-old trader operating from Barings Futures Singapore, held responsibilities that should have been separated. He executed trades in the front office and also controlled clearing and settlement in the back office. This concentration of responsibility created a fundamental segregation-of-duties failure. Because there was no effective independent check, Leeson was able to conceal substantial speculative losses in a secret account identified as Account 88888. The same individual could initiate transactions and influence the records and processes through which those transactions were checked and settled. This defeated a basic internal control principle: no single individual should be able to carry out and conceal a transaction without independent scrutiny.

6.2 Warning signals that were not acted upon

The presentation identifies several warning signs. Risk managers and auditors in London noticed repeated large requests for funds described as client margins. Reported trading profits did not align with the actual cash inflows into the bank. Requests for independent oversight were deferred to

local management or dismissed. An internal audit in December 1994 recommended removing Leeson from back-office duties. Management rejected the warning. In effect, risk concerns were subordinated to local authority and short-term reported profitability. The issue was not simply that warning signs existed; it was that the organisation did not respond to them with the level of independent investigation and action they required.

6.3 Lessons for modern risk management

1. Authority must match responsibility. A risk manager who can identify a serious concern but has no effective route to escalate it—or no organisational backing for appropriate intervention—may be unable to prevent losses. Risk oversight requires a recognised mandate and access to decision-makers.
2. Separation of duties is essential. Front-office trading and back-office settlement should not be combined in a way that allows one person to initiate, record and conceal transactions. Independent checks must be designed into important processes.
3. Profits do not equal safety. Strong reported performance should never be treated as proof that controls are effective. Profitable business units must remain subject to scrutiny, and unusual results or funding demands should be investigated.

6.4 Connecting the case to the five themes

- Risk appetite: exposures and activities must remain within approved boundaries; unusual or unexplained exposure should prompt review.
- Control framework: responsibilities, segregation of duties, monitoring and escalation must work in practice, not merely exist on paper.
- Business understanding: risk professionals must understand the trading and settlement process well enough to recognise where control failures can occur.
- Independence: risk and audit concerns must be considered objectively, even when they challenge influential managers or profitable activities.
- Use of information and technology: monitoring and analysis can help identify inconsistencies and patterns, but people must investigate alerts and act on verified findings.

FINAL LESSON A control framework is only as strong as the leadership willing to enforce it. Effective risk management requires clear boundaries, sound controls, business understanding, independent challenge and the courage to act on warning signs.

CLOSING REFLECTION

Risk management is most valuable when it improves the quality of decisions before problems become losses. The risk professional must understand the organisation’s objectives, test the assumptions behind business activity, ensure that controls are proportionate, preserve independent challenge and use available tools responsibly. The ultimate measure of effective risk management is not the volume of reports produced, but whether the organisation is better able to recognise, understand and manage the risks it takes.

THANK YOU