

ANTI-CORRUPTION TRAINING SERIES

INTEGRITY
TODAY
A STRONGER
TOMORROW

LEVEL 1

LEVEL 2

LEVEL 3

KNOW | ACT | PREVENT | BUILD TRUST

LEVEL 2

Welcome,
Level 1 Recap and
Level 2 Objectives



RECAP

KEY LEARNINGS
FROM LEVEL 1



UNDERSTAND

LEVEL 2
OBJECTIVES



BUILD

ON YOUR
KNOWLEDGE

Together
Against Corruption



ETHICAL
PEOPLE



STRONGER
INSTITUTIONS



BRIGHTER
TOMORROW

Anti-Corruption and Risk Management

LEVEL 2

Training Manual

Risk Identification Assessment and Prioritisation

Contents

1. Welcome Level 1 Recap and Level 2 Objectives
2. Moving from Anti-Corruption Awareness to Risk Management
3. Understanding Risk in an Anti-Corruption Context
4. What Is Corruption Risk Management
5. The Corruption Risk Management Cycle
6. Understanding Inherent and Residual Risk
7. Internal and External Sources of Corruption Risk
8. People Process and System-Based Risks
9. High-Risk Organisational Functions and Activities
10. Identifying Corruption Risk Events
11. Identifying Risk Causes and Possible Consequences
12. Using Process Mapping to Locate Corruption Risks
13. Assessing Risk Likelihood
14. Assessing Risk Impact
15. Using a Corruption Risk Matrix
16. Rating and Prioritising Corruption Risks
17. Creating a Corruption Risk Register
18. Assessing a Workplace Corruption Risk
19. Day 1 Review and Key Takeaways

Copyright Notice

Anti-Corruption and Risk Management

LEVEL 2

© 2026 **KlevafX Technologies**. All Rights Reserved.

This publication is protected by copyright law. No part of this book may be reproduced, stored in a retrieval system, transmitted, distributed, or reproduced in any form or by any means—electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the copyright owner, except for brief quotations used in reviews or scholarly references.

This material has been developed for educational and training purposes. Unauthorized copying, redistribution, resale, or commercial use of this publication, in whole or in part, is strictly prohibited.

Every effort has been made to ensure the accuracy of the information contained in this publication.

However, the author and publisher accept no responsibility for any loss, liability, or damage arising from the use or misuse of the information provided. Readers are encouraged to comply with all applicable laws, regulations, and organizational policies within their respective jurisdictions.

Published by:

KlevafX Technologies

Author:

Korede Olafimihan

08065361826

Edition: First Edition, 2026

All rights reserved.

1. Welcome Level 1 Recap and Level 2 Objectives

Welcome to Anti-Corruption and Risk Management — Level 2.

In Level 1, you learned what corruption means, the major forms it takes and how it affects individuals, organisations and society. You also examined ethics, integrity, accountability, transparency, internal controls, conflicts of interest and responsible reporting.

Level 2 takes you beyond basic awareness. Knowing that corruption exists is not enough. You must be able to identify where it is likely to occur, assess how serious the risk is and establish controls that reduce the opportunity for misconduct.

During this course, you will learn how to:

- Identify corruption risks within people, processes and systems
- Recognise high-risk functions, transactions and relationships
- Assess the likelihood and possible impact of corruption
- Use a risk matrix to rate and prioritise identified risks
- Develop and maintain a corruption risk register
- Design preventive, detective and corrective controls
- Assign responsibility for managing specific risks
- Monitor controls and recognise when they are failing
- Report, escalate and document corruption concerns properly
- Develop practical corruption risk-treatment plans

The central principle of Level 2 is simple: corruption prevention must be systematic. An organisation should not wait until money disappears, evidence is destroyed or public trust is damaged before taking action. It must identify vulnerabilities early and control them deliberately.

Moving from **Anti-Corruption Awareness to Risk Management**



2. Moving from Anti-Corruption Awareness to Risk Management

Knowing what corruption is does not automatically prevent it. Many organisations have codes of conduct, anti-corruption policies and trained employees, yet corruption still occurs because the systems surrounding important decisions remain weak.

Anti-corruption awareness helps people recognise misconduct and understand why it is wrong. Corruption risk management goes further by identifying where corruption could occur, determining how serious the threat is and introducing controls before damage happens.

Awareness asks:

- What is corruption?
- What behaviour is prohibited?
- What are the consequences?

Risk management asks:

- Where could corruption occur in this organisation?
- Who has the opportunity or authority to commit it?
- What weakness could make it possible?
- How likely is it to happen?
- What damage could it cause?
- Which controls can prevent or detect it?

For example, warning employees not to accept bribes creates awareness. Requiring multiple approvals, verifying suppliers, documenting procurement decisions and reviewing unusual payments creates risk management.

Awareness influences behaviour, but risk management strengthens the system. An organisation needs both because ethical employees can still work inside vulnerable systems, while strong controls can still be defeated by people who do not understand or respect integrity.

The objective is to move from simply telling people, “Do not engage in corruption,” to deliberately making corruption difficult to commit, easier to detect and costly to conceal.

Understanding **Risk** in an Anti-Corruption Context



3. Understanding Risk in an Anti-Corruption Context

Risk is the possibility that an uncertain event or behaviour could prevent an organisation from achieving its objectives.

In an anti-corruption context, corruption risk is the possibility that someone may misuse entrusted authority, organisational resources or official processes for private benefit.

A corruption risk does not mean corruption has already happened. It means a weakness, opportunity or situation exists that could allow it to happen.

For example:

- One employee controls supplier selection, approval and payment
- Senior officers can override procedures without explanation
- Cash transactions are poorly documented
- Suppliers are appointed without background checks
- Gifts from contractors are accepted without declaration
- Complaints can be suppressed by the same managers being reported

These situations are risks because they create opportunities for bribery, fraud, favouritism, embezzlement or abuse of authority.

Every corruption risk should be examined through four basic questions:

- What could happen?
- Why could it happen?
- How likely is it to happen?
- What damage could it cause?

The possible damage may include financial loss, legal penalties, service failure, damaged reputation, loss of public confidence and harm to employees or beneficiaries.

Corruption risk management is therefore not based on suspicion alone. It is a structured process for identifying vulnerabilities, assessing their seriousness and introducing controls before those vulnerabilities are exploited.

The key principle is clear: if an organisation understands where corruption could occur, it has a better chance of preventing it before the damage is done.



4. What Is Corruption Risk Management

Let us be practical: telling employees to avoid corruption is important, but it is not a complete prevention strategy. If the organisation's systems are weak, dishonest people will still find opportunities to manipulate them.

Corruption risk management is the organised process of identifying where corruption could occur, assessing how serious each risk is and putting effective controls in place to prevent, detect or respond to it.

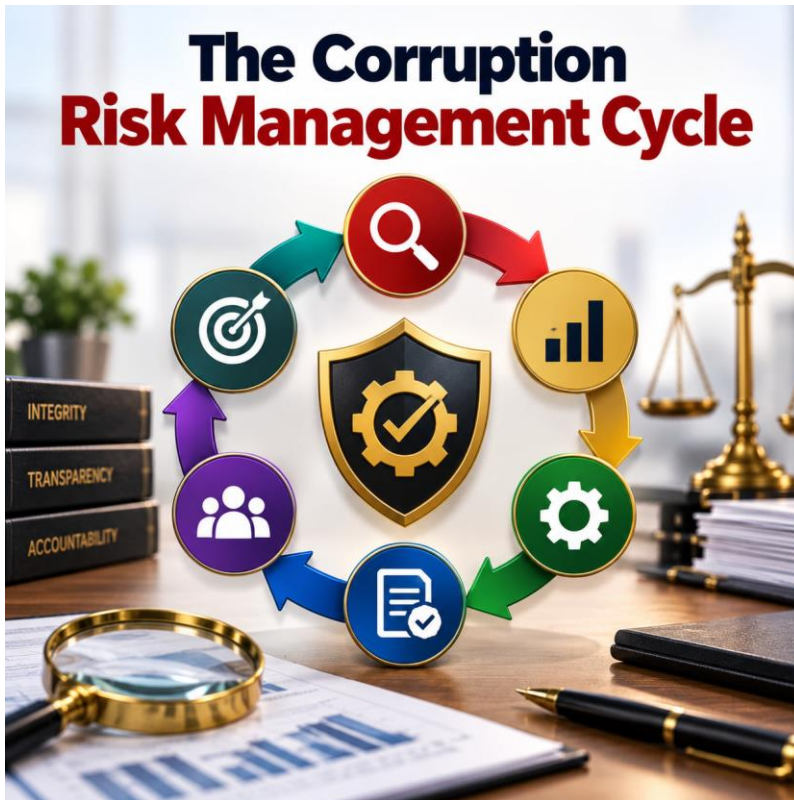
It focuses on five major actions:

- Identify the risk: Determine where bribery, fraud, favouritism, embezzlement or abuse of authority could occur.
- Assess the risk: Examine how likely the misconduct is and how much damage it could cause.
- Prioritise the risk: Address the most serious threats first instead of treating every risk as equal.
- Control the risk: Introduce policies, approvals, checks, monitoring and accountability measures.
- Monitor the risk: Confirm that the controls are working and respond when circumstances change.

For example, an organisation may identify supplier selection as a corruption risk. It could reduce that risk by requiring competitive bidding, declaring conflicts of interest, separating approval responsibilities and independently reviewing procurement decisions.

Corruption risk management is not a one-time exercise completed for documentation. Risks change when personnel, technology, suppliers, regulations or organisational activities change. The assessment must therefore be reviewed regularly.

The purpose is straightforward: identify weaknesses before they are exploited, strengthen controls before money is lost and respond before misconduct becomes an organisational culture.



5. The Corruption Risk Management Cycle

Corruption risk management is not something an organisation does once, files away and forgets. It is a continuous cycle because people, processes, technology, suppliers and operating conditions will keep changing.

The cycle usually involves six connected stages:

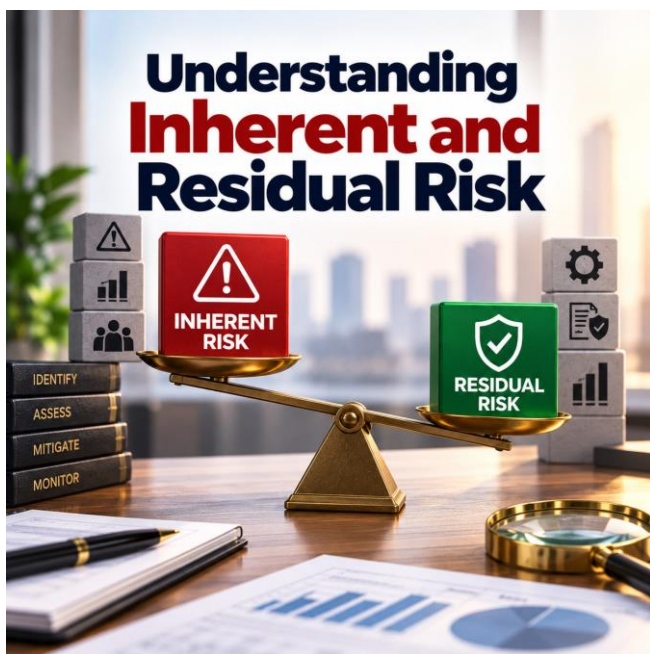
- Establish the context: Understand the organisation's objectives, activities, structure, stakeholders and operating environment.
- Identify corruption risks: Determine where bribery, fraud, favouritism, embezzlement, conflicts of interest or abuse of authority could occur.
- Analyse the risks: Examine the causes, existing controls, likelihood of occurrence and possible consequences.
- Evaluate and prioritise: Compare the risks and decide which ones require immediate attention.
- Treat the risks: Introduce or strengthen controls to prevent, detect or reduce the identified risks.
- Monitor and review: Check whether controls are working and identify new or changing risks.

Communication and documentation should continue throughout the entire cycle. Employees must know their responsibilities, management must receive accurate information and important decisions must be properly recorded.

For example, if procurement is identified as high-risk, the organisation assesses its weaknesses, introduces controls, assigns responsible officers and monitors transactions. If those controls fail or circumstances change, the risk must be reassessed.

The process then begins again.

The main point is simple: identify the risk, assess it, control it and keep watching it. A corruption risk that was low yesterday can become serious tomorrow if the organisation stops paying attention.



6. Understanding Inherent and Residual Risk

Let us make this simple: every activity carries a certain level of corruption risk before any safeguards are applied. Even after controls are introduced, some risk may still remain. These two conditions are known as inherent risk and residual risk.

Inherent risk is the level of corruption risk that exists when you assume there are no controls in place.

For example, an officer who can select suppliers, approve invoices and authorise payments has a high inherent risk of fraud or favouritism because too much control is concentrated in one person.

Residual risk is the level of risk that remains after controls have been introduced.

If the organisation separates supplier selection, invoice verification and payment approval among different officers, the risk will reduce. However, it may not disappear completely because the officers could still cooperate to bypass the controls.

The basic relationship is:

- Inherent risk — the original exposure before controls
- Controls — the measures introduced to reduce the exposure
- Residual risk — the exposure that remains after controls

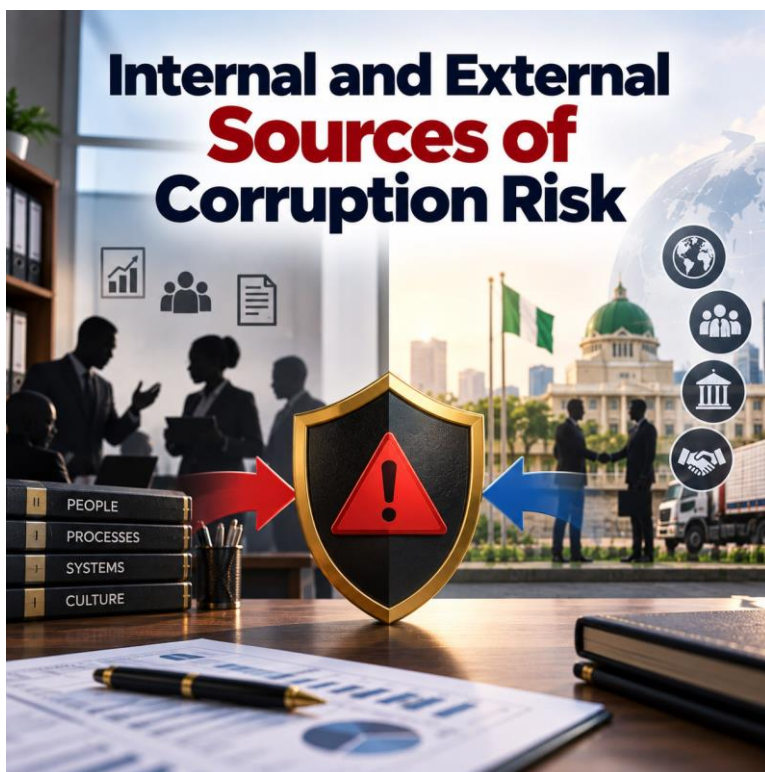
When assessing residual risk, do not merely confirm that a policy or control exists. Ask:

- Is the control properly designed?
- Is it consistently followed?
- Who checks that it is working?
- Can senior officers override it?
- Is there evidence that it reduces the risk?

A control that exists only on paper does not meaningfully reduce corruption risk.

If the residual risk remains above the organisation's acceptable level, stronger controls, closer monitoring or changes to the activity will be required.

The key point is this: inherent risk shows the danger without protection, while residual risk shows the danger that remains after protection has been applied.



7. Internal and External Sources of Corruption Risk

When corruption occurs, people often focus only on the employee who committed the act. But corruption risk can come from inside the organisation, outside it or from cooperation between people on both sides. If you examine only one source, you will miss part of the problem.

Internal sources originate from the organisation's employees, leadership, systems, policies or working practices.

Common internal sources include:

- Too much authority given to one person
- Weak supervision and approval procedures
- Senior management overriding established controls
- Poor record keeping and undocumented decisions
- Undeclared conflicts of interest
- Unethical organisational culture
- Inadequate staff screening or job rotation
- Failure to investigate reported misconduct

External sources come from individuals, organisations or conditions outside the organisation.

Common external sources include:

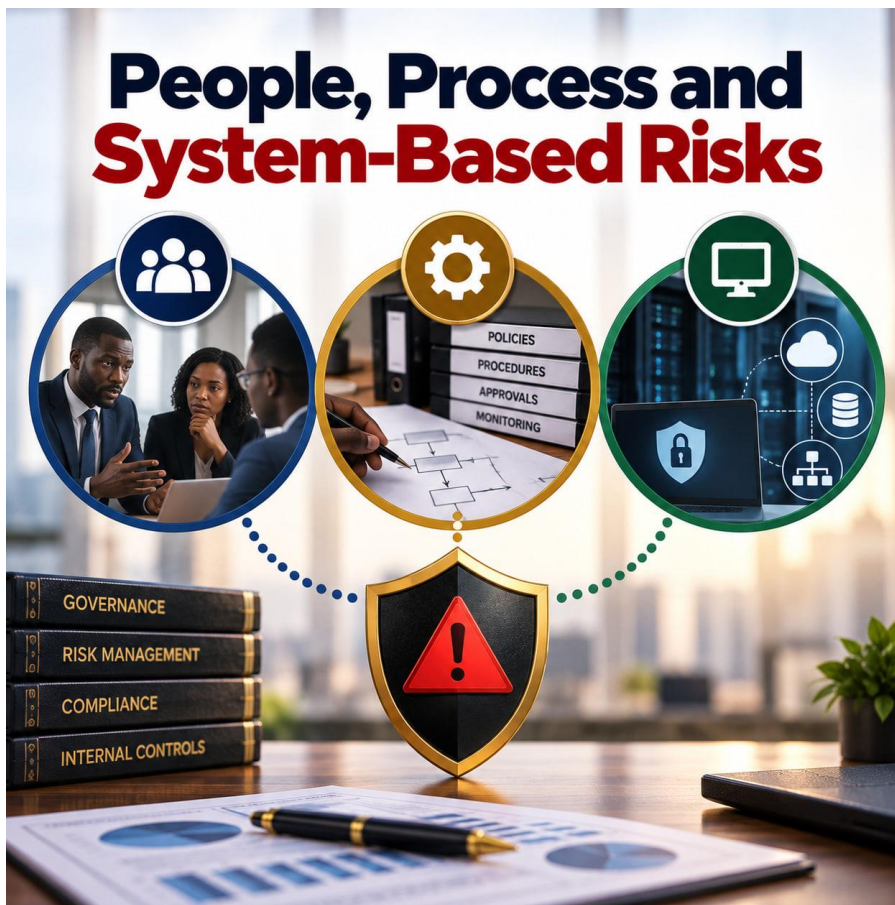
- Suppliers offering bribes or secret commissions
- Contractors submitting false invoices or inflated quotations
- Customers using gifts to obtain special treatment

- Agents or intermediaries making improper payments
- Political interference in appointments or contracts
- Criminal groups attempting to exploit financial systems
- Weak regulatory enforcement
- Operating in sectors or locations with high corruption exposure

Internal and external actors may also work together. For example, a procurement officer may share confidential bidding information with a supplier in exchange for payment. The employee is the internal source, while the supplier is the external source.

A proper assessment must therefore examine employees, leadership, third parties, processes and the wider operating environment.

The lesson is straightforward: corruption risk does not stop at the organisation's gate. Strong internal controls are necessary, but third parties and external pressures must also be properly assessed and monitored.



8. People Process and System-Based Risks

When corruption happens, it is easy to blame one dishonest individual and assume the problem has been solved. But removing one person will not protect the organisation if the same weak processes and systems remain in place.

Corruption risks can generally be examined under three areas: people, processes and systems.

People-based risks arise from the behaviour, authority, relationships or competence of individuals.

Examples include:

- Employees with undeclared conflicts of interest
- Managers who regularly override controls
- Staff members living far beyond their known income
- Individuals controlling several stages of one transaction
- Employees accepting gifts or favours from suppliers
- Staff members who have not received proper ethics training

Process-based risks arise when procedures are weak, unclear, inconsistent or deliberately ignored.

Examples include:

- Contracts awarded without competitive bidding
- Payments approved without supporting documents

- Recruitment decisions made without clear criteria
- Complaints handled by the person being accused
- Cash collected without receipts or reconciliation
- Emergency procedures repeatedly used to bypass normal controls

System-based risks arise from weaknesses in technology, information management and automated controls.

Examples include:

- Shared passwords and unrestricted system access
- Transactions that can be edited without an audit trail
- Former employees retaining access after leaving
- Weak protection of confidential procurement information
- Poor separation of user and approval permissions
- Alerts being disabled or ignored

These three risk areas are connected. A dishonest employee may exploit a weak process through an unprotected system. That is why installing new software alone will not solve a corruption problem, just as creating a policy will not help if employees can ignore it without consequences.

An effective assessment must examine who is involved, how the work is performed and which systems support it. Corruption usually succeeds where weaknesses in all three areas meet.



9. High-Risk Organisational Functions and Activities

Let us be clear: corruption can occur anywhere, but the risk is not equal across every department or activity. It becomes higher wherever people control money, contracts, employment, confidential information, valuable assets or important decisions.

Common high-risk functions and activities include:

- Procurement and contracting: Bid manipulation, inflated prices, kickbacks, favouritism and false suppliers may occur.
- Finance and payments: False invoices, duplicate payments, unauthorised transfers, expense manipulation and embezzlement may occur.
- Recruitment and promotion: Nepotism, favouritism, bribery and manipulation of selection results may influence decisions.
- Licensing and approvals: Officers may demand or accept payments to approve, delay, ignore or accelerate applications.
- Cash collection: Money may be diverted, receipts altered or collections deliberately underreported.
- Asset and inventory management: Organisational property may be stolen, undervalued, misallocated or sold improperly.
- Sales and customer management: Discounts, credit approvals, refunds and account decisions may be manipulated for personal benefit.
- Donations and sponsorships: Funds may be redirected to connected individuals, political interests or false beneficiaries.

- Regulatory and inspection activities: Inspectors may accept bribes to ignore violations or produce favourable reports.
- Third-party engagement: Agents, consultants, contractors and suppliers may make improper payments on the organisation's behalf.
- Access to confidential information: Employees may leak tender prices, customer data or investigation details for personal gain.

An activity becomes especially dangerous when it combines high financial value, individual discretion, urgency, secrecy and weak supervision.

The organisation should therefore direct stronger controls, monitoring and independent review towards its highest-risk activities. Treating every department as equally risky wastes resources and may leave the most vulnerable areas poorly protected.

The point is simple: follow the money, follow the authority and follow the decisions. That is usually where serious corruption risks are found.



10. Identifying Corruption Risk Events

It is not enough to write, “There is a risk of corruption.” That statement is too broad to assess or control. You must describe the specific event that could occur, how it could happen and what it could affect.

A corruption risk event is a possible incident in which entrusted authority, organisational processes or resources may be abused for personal or improper benefit.

A clear risk event should answer:

- Who could be involved?
- What could they do?
- Where could it occur?
- How could the process be manipulated?
- What benefit could be obtained?

For example, instead of writing:

“Procurement corruption may occur.”

Write:

“A procurement officer may disclose confidential bid information to a preferred supplier in exchange for money, gifts or future employment.”

Other corruption risk events include:

- A finance officer may create a false supplier and authorise payments to a personal account.
- A recruitment panel member may manipulate interview scores to favour a relative.

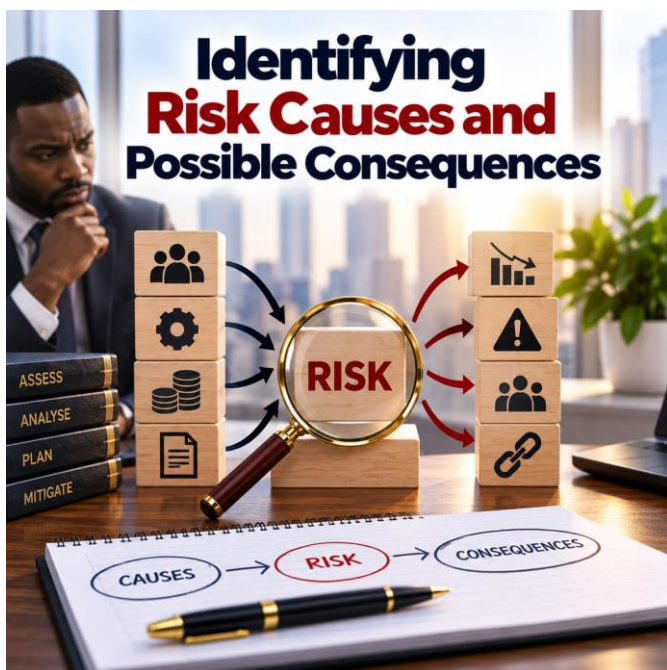
- An inspector may accept payment to ignore a serious regulatory violation.
- A manager may divide one large transaction into smaller amounts to avoid higher approval requirements.
- An employee may approve an inflated invoice submitted by a cooperating contractor.
- A senior officer may pressure staff to award a contract without competitive bidding.

Useful sources for identifying these events include:

- Previous audit findings and investigation reports
- Employee complaints and whistleblower reports
- Transaction records and unusual payment patterns
- Interviews with staff who understand the process
- Changes in personnel, technology or operating conditions
- Corruption cases from similar organisations or industries

A properly written risk event makes it easier to identify causes, assess likelihood, estimate impact and choose the right controls.

The key principle is straightforward: do not identify corruption as a vague possibility—describe the specific event that could happen.



11. Identifying Risk Causes and Possible Consequences

Once you identify a corruption risk event, do not stop there. You need to understand why it could happen and what damage it could cause. Otherwise, you may introduce a control that treats the visible problem but leaves the real weakness untouched.

A risk cause is the condition, weakness or pressure that makes a corruption event possible.

Common causes include:

- Too much authority concentrated in one person
- Weak supervision or independent review
- Poorly defined procedures and responsibilities
- Inadequate background checks on employees or suppliers
- Undeclared conflicts of interest
- Management override of established controls
- Poor record keeping and missing audit trails
- Unrealistic targets or financial pressure
- A workplace culture that protects powerful offenders
- Weak disciplinary action for misconduct

A risk consequence is the damage that may occur if the corruption event takes place.

Possible consequences include:

- Financial loss or theft of organisational resources
- Legal penalties, prosecution or regulatory sanctions
- Poor-quality goods, services or projects
- Injury, service failure or harm to beneficiaries

- Damaged reputation and loss of public confidence
- Loss of customers, investors, donors or business partners
- Unfair recruitment, promotion or contract decisions
- Reduced employee morale and increased misconduct
- Destruction or concealment of important evidence

Consider this example:

Risk event: A procurement officer awards a contract to a related company at an inflated price.

Possible causes:

- The conflict of interest was not declared
- Supplier ownership was not verified
- One officer controlled the selection process
- Management did not independently review the award

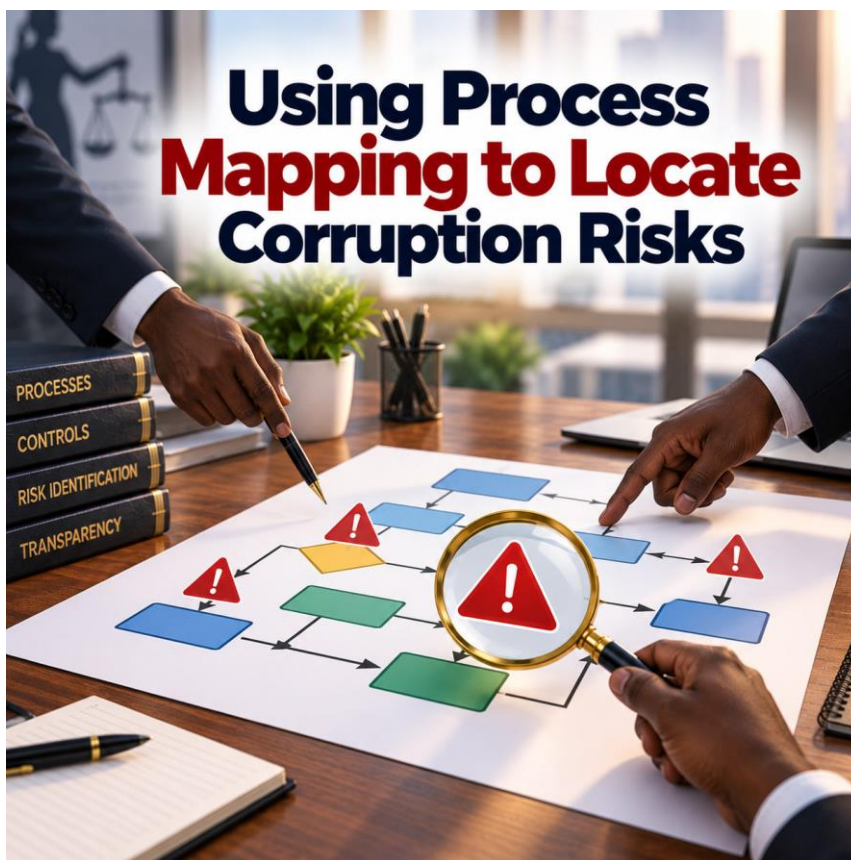
Possible consequences:

- The organisation pays more than necessary
- An unqualified supplier delivers poor-quality work
- The organisation faces investigation and reputational damage
- Public or organisational resources are diverted for private benefit

Strong risk management connects all three elements:

- Cause: Why could it happen?
- Risk event: What could happen?
- Consequence: What damage could follow?

The practical lesson is simple: control the cause before it produces the event, and understand the consequence before deciding how urgently to act.



12. Using Process Mapping to Locate Corruption Risks

Sometimes corruption is difficult to see because people focus only on the final transaction. Process mapping forces you to examine every step that happens before the final decision, approval or payment.

A process map is a clear, step-by-step representation of how an activity is supposed to move from beginning to completion.

For example, a procurement process may involve:

- A department identifies a need
- A purchase request is prepared
- Management approves the request
- Suppliers submit quotations
- Bids are evaluated
- A supplier is selected
- Goods or services are delivered
- An invoice is verified
- Payment is authorised
- Records are reviewed and stored

At each step, ask:

- Who performs this activity?
- Who approves or reviews it?

- What information or document is required?
- Can one person control several stages?
- Can the procedure be bypassed or altered?
- Is there a reliable record of the decision?
- Could an employee or third party obtain an improper benefit?

This examination may reveal corruption risks such as:

- A staff member creating an unnecessary purchase request
- Confidential bidding information being leaked
- Evaluation scores being manipulated
- A related supplier being selected without disclosure
- Poor-quality goods being accepted in exchange for payment
- An invoice being inflated or paid twice
- Records being changed to conceal the transaction

A process map should show both the official procedure and what employees actually do in practice. A perfectly written procedure is useless if staff members regularly bypass it.

The purpose is not to create a beautiful diagram. It is to identify where authority is concentrated, oversight is missing and manipulation could occur.

The key principle is clear: when you follow a process step by step, hidden corruption opportunities become easier to identify.



13. Assessing Risk Likelihood

After identifying a corruption risk, the next question is practical: how likely is this event to happen? You cannot treat every possible risk as an emergency, so likelihood helps you determine where attention is needed most.

Risk likelihood is the estimated probability that a corruption event will occur within a particular period.

Likelihood should not be based on personal opinion alone. It should be supported by available evidence, past experience and current conditions.

Factors that may increase likelihood include:

- Similar incidents have happened before
- One person controls several stages of a transaction
- Senior officers frequently override controls
- Employees or suppliers have undeclared relationships
- Transactions involve large amounts of money
- Cash payments are common
- Records are incomplete or easily altered
- Monitoring and supervision are weak
- Employees can bypass procedures without consequences
- The activity involves urgency, secrecy or excessive discretion

A simple likelihood scale may be used:

- Rare: The event is highly unusual and has little opportunity to occur

- Unlikely: The event could occur, but existing conditions make it difficult
- Possible: The event may occur under current circumstances
- Likely: The event is expected to occur or has happened repeatedly
- Almost certain: The event is occurring frequently or conditions strongly support it

For example, supplier favouritism may be rated likely where one manager selects suppliers, no conflict-of-interest declarations are required and previous complaints have been ignored.

Evidence for assessing likelihood may come from:

- Audit and investigation reports
- Previous incidents and complaints
- Interviews with employees
- Transaction records and unusual patterns
- Control-testing results
- Industry or country risk information

A risk should not be rated low simply because no incident has been officially reported. Poor reporting systems may hide misconduct rather than prove that it is absent.

The main point is this: assess likelihood according to the opportunity, history and effectiveness of controls—not according to how comfortable management feels.



14. Assessing Risk Impact

A corruption incident does not have to involve millions of naira before it becomes serious. A single dishonest decision can damage finances, public confidence, employee safety or the organisation's ability to operate. That is why impact must be assessed beyond the amount of money involved.

Risk impact is the level of harm the organisation may suffer if a corruption event occurs.

When assessing impact, consider several areas:

- Financial impact: Loss of money, assets, revenue, contracts or funding
- Legal impact: Investigation, prosecution, fines, sanctions or civil claims
- Operational impact: Delays, disrupted services, failed projects or reduced productivity
- Reputational impact: Loss of trust among customers, regulators, employees and the public
- Human impact: Injury, exploitation, unfair treatment or denial of essential services
- Strategic impact: Failure to achieve organisational goals or maintain important partnerships

A simple impact scale may be used:

- Insignificant: Limited damage that can be corrected through routine action
- Minor: Small loss or disruption requiring management attention
- Moderate: Noticeable financial, operational or reputational damage
- Major: Serious loss, legal exposure or disruption affecting key activities
- Severe: Organisational failure, major prosecution, widespread harm or lasting reputational damage

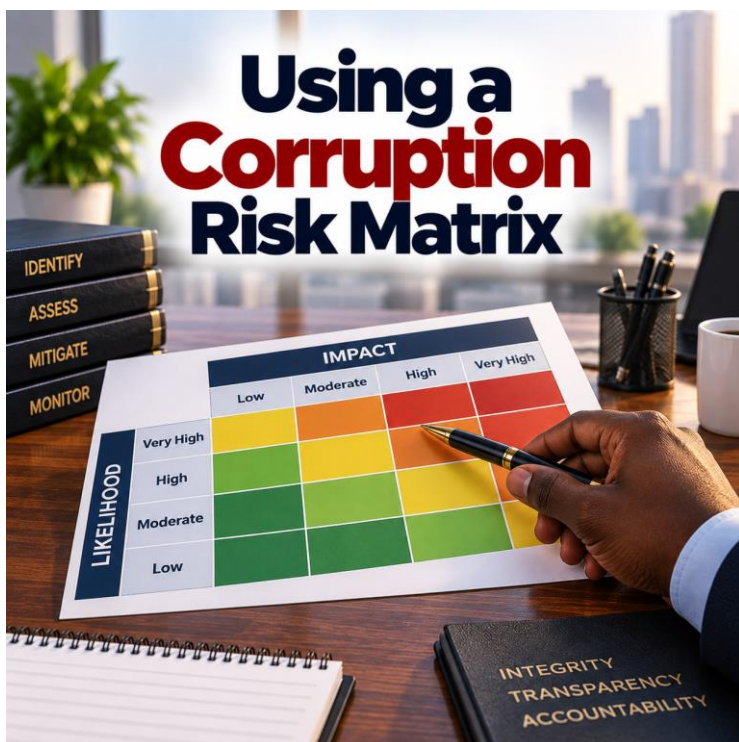
For example, bribery involving a safety inspector may appear financially small, but the impact could be severe if an unsafe facility remains open and people are injured.

Impact assessments should be based on the worst credible consequence, not an exaggerated imaginary disaster or the most comfortable outcome management prefers.

Ask:

- Who could be harmed?
- How much could be lost?
- Which laws, contracts or policies could be violated?
- How long could the damage continue?
- Could the organisation recover?
- Would the incident attract regulatory, media or public attention?

The key principle is simple: do not measure corruption only by the money exchanged; measure the full damage the corrupt decision could cause.



15. Using a Corruption Risk Matrix

Now that you can assess likelihood and impact, you need a consistent way to combine them. This is where a corruption risk matrix becomes useful. It helps an organisation compare risks and decide which ones require urgent attention.

A corruption risk matrix measures two factors:

- Likelihood: How probable is the corruption event?
- Impact: How serious would the damage be?

Each factor may be scored from 1 to 5:

LIKELIHOOD

- 1 — Rare
- 2 — Unlikely
- 3 — Possible
- 4 — Likely
- 5 — Almost certain

IMPACT

- 1 — Insignificant
- 2 — Minor
- 3 — Moderate
- 4 — Major
- 5 — Severe

The risk score is calculated as follows:

Likelihood × Impact = Risk Score

For example, if supplier bribery is rated Likely (4) and its impact would be Major (4):

4 × 4 = 16

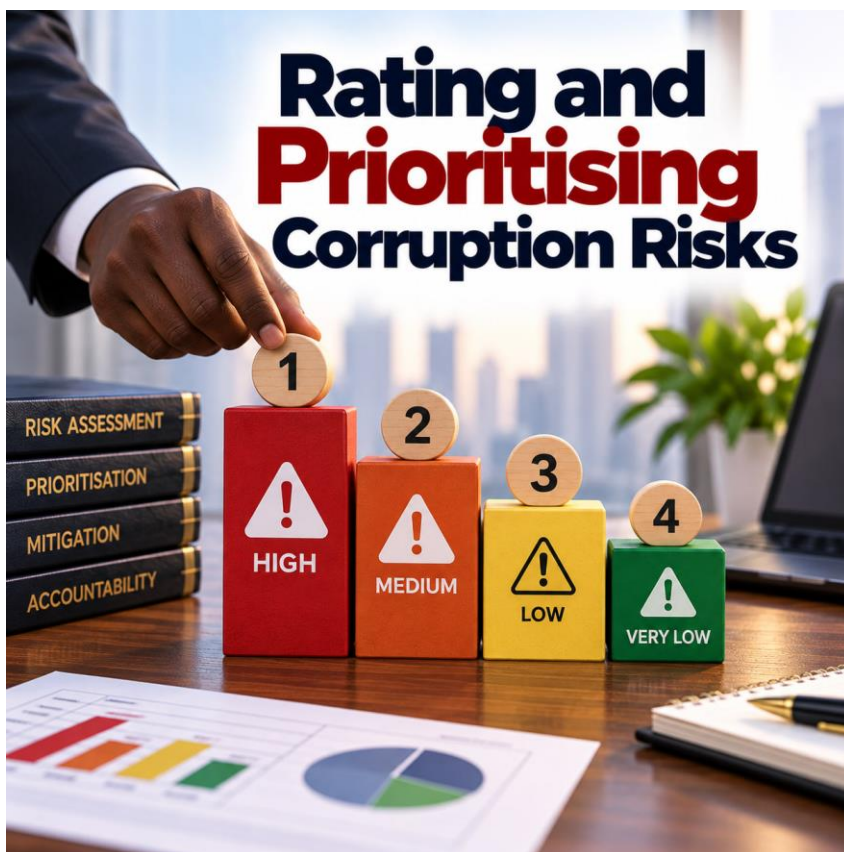
The organisation may classify the scores as:

- 1–4: Low risk — Maintain routine controls and monitoring
- 5–9: Moderate risk — Review controls and assign responsibility
- 10–16: High risk — Take prompt action and strengthen controls
- 17–25: Critical risk — Escalate immediately and involve senior leadership

A matrix supports consistent decision-making, but it does not replace professional judgement. Two risks with the same score may require different responses because one involves vulnerable people, legal violations or senior-management misconduct.

Ratings must also be supported by evidence. Managers should not reduce a score simply to make a department appear safer or avoid taking corrective action.

The risk matrix answers one important question: which corruption risks require attention first? It turns general concern into a clear and prioritised basis for action.



16. Rating and Prioritising Corruption Risks

Let us be realistic: an organisation may identify dozens of corruption risks, but it cannot address all of them with the same urgency. Rating and prioritisation help management focus limited time, money and attention on the risks that could cause the greatest harm.

A risk rating is usually determined by combining:

- The likelihood of the corruption event occurring
- The potential impact if it occurs
- The strength of existing controls
- The level of risk remaining after those controls

The basic calculation may be:

Likelihood × Impact = Risk Score

However, the numerical score should guide judgement—not replace it.

When prioritising risks, consider:

- Whether the risk threatens lives, safety or essential services
- Whether it could cause major financial loss
- Whether senior officials or organised groups may be involved
- Whether it could lead to prosecution or regulatory sanctions
- Whether the activity involves public funds or vulnerable people

- Whether the misconduct could continue for a long time undetected
- Whether current controls are weak or regularly bypassed
- Whether the incident could seriously damage public confidence

For example, two risks may both score 12. One concerns minor inventory theft, while the other involves bribery during safety inspections. The second risk may deserve higher priority because its consequences could include injury or loss of life.

Risks may be prioritised as:

- Low: Accept and monitor through routine controls
- Moderate: Assign responsibility and improve selected controls
- High: Develop an immediate treatment plan and increase monitoring
- Critical: Escalate to senior leadership and take urgent protective action

Each priority risk should have:

- A named risk owner
- A clear treatment action
- A completion deadline
- Required resources
- A monitoring and reporting method

A high-risk rating without action is just documentation. The purpose of prioritisation is to direct responsibility and resources towards the organisation's most serious exposures.

The principle is straightforward: deal first with the risks most likely to occur, most capable of causing serious harm and least protected by effective controls.



17. Creating a Corruption Risk Register

Once corruption risks have been identified and rated, they should not remain scattered across meeting notes, audit reports or people's memories. They must be recorded in one organised document called a corruption risk register.

A corruption risk register is a working document used to record, assess, assign and monitor corruption risks across an organisation.

For each risk, the register should include:

- Risk area: The department, process or activity exposed to corruption
- Risk event: A clear description of what could happen
- Risk causes: The weaknesses or conditions that could make it happen
- Possible consequences: The financial, legal, operational, human or reputational damage
- Existing controls: Measures already being used to manage the risk
- Likelihood rating: How probable the event is
- Impact rating: How serious the damage could be
- Overall risk rating: The calculated risk level
- Required treatment: Additional action needed to reduce the risk
- Risk owner: The person responsible for managing it
- Completion date: When the agreed action should be implemented
- Review status: Whether the risk is improving, unchanged or increasing

For example:

Risk area: Procurement

Risk event: A procurement officer may manipulate supplier evaluation scores to favour a related company.

Causes: Undeclared conflicts of interest, weak review and excessive individual discretion.

Consequences: Inflated costs, poor-quality delivery, investigation and reputational damage.

Existing controls: Evaluation committee and conflict-of-interest declaration.

Risk rating: High

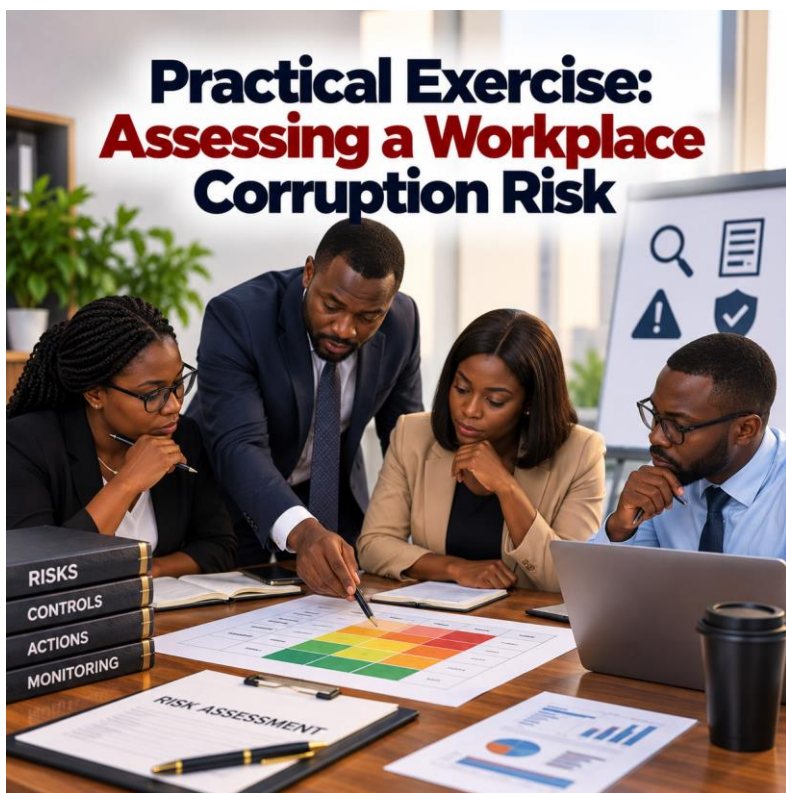
Required treatment: Verify supplier ownership and introduce an independent review of evaluation scores.

Risk owner: Head of Procurement

A risk register must be updated when controls change, incidents occur, responsibilities shift or new risks emerge. It should also be reviewed regularly by management.

Do not create a register simply to satisfy auditors. If no one owns the risks, deadlines are ignored and updates are never made, the document has no practical value.

The key point is clear: a corruption risk register turns identified concerns into documented responsibilities, deadlines and actions that can be monitored.



18. Assessing a Workplace Corruption Risk

Let us apply what we have learned to a realistic workplace situation. Identifying suspicious behaviour is only the beginning. A proper assessment must connect the risk event, its causes, possible consequences, existing controls and overall risk rating.

WORKPLACE SCENARIO

A procurement manager is responsible for inviting suppliers, evaluating quotations and recommending the successful bidder. The same manager regularly awards contracts to one company.

Further checks reveal that:

- The company was registered by the manager's relative
- The relationship was never declared
- Competing quotations appear to have been prepared by the same person
- Prices are consistently higher than market rates
- Senior management approves the recommendations without independent review

RISK ASSESSMENT

Risk area: Procurement and contracting

Risk event: The procurement manager may manipulate supplier selection to award inflated contracts to a related company for personal or family benefit.

Risk causes:

- Undeclared conflict of interest

- Excessive authority concentrated in one person
- No verification of supplier ownership
- Weak review of quotations and market prices
- Automatic approval by senior management

Possible consequences:

- Financial loss through inflated contract prices
- Poor-quality goods or services
- Unfair exclusion of legitimate suppliers
- Legal or regulatory action
- Damage to organisational reputation
- Loss of employee and stakeholder confidence

Existing controls: Management approval and submission of multiple quotations

Control weakness: The approval is not independent, and the quotations may have been falsified. The controls exist but are ineffective.

Likelihood rating: 4 — Likely

Impact rating: 4 — Major

Risk score: $4 \times 4 = 16$

Overall rating: High risk

Required treatment:

- Remove supplier selection from the manager's sole control
- Require conflict-of-interest declarations
- Verify the beneficial ownership of suppliers
- Confirm quotations directly with competing suppliers
- Compare proposed prices with independent market data
- Introduce an independent procurement review
- Investigate previous contracts awarded to the company

This example shows why risk assessment must go beyond identifying a suspicious relationship. The objective is to establish what could happen, why it could happen, how serious it is and what must be done about it.

Day 1

Review and Key Takeaways



19. Day 1 Review and Key Takeaways

Today, we moved beyond basic anti-corruption awareness and examined how corruption risks can be identified, assessed and prioritised before serious damage occurs.

The major lessons from Day 1 are:

- Awareness explains what corruption is, but risk management identifies where and how it could happen.
- Corruption risk management is a continuous cycle of identifying, analysing, evaluating, treating and monitoring risks.
- Inherent risk is the level of exposure before controls are applied.
- Residual risk is the level of exposure remaining after controls are applied.
- Corruption risks may come from employees, leadership, third parties, systems or the wider operating environment.
- People, processes and systems must be examined together because weaknesses in one area can expose the others.
- High-risk activities usually involve money, contracts, employment, valuable assets, confidential information or discretionary authority.
- A corruption risk event must clearly describe the specific misconduct that could occur.
- Risk causes explain why the event could happen, while consequences describe the damage that may follow.

- Process mapping helps reveal where authority is concentrated, supervision is missing or procedures can be bypassed.
- Likelihood measures how probable the event is.
- Impact measures the financial, legal, operational, human, strategic and reputational harm it could cause.
- A risk matrix combines likelihood and impact to determine the level of risk.
- Risks must be prioritised so that urgent attention and resources are directed towards the most serious exposures.
- A corruption risk register records each risk, its causes, consequences, controls, rating, required action, owner and deadline.

The central lesson is simple: an organisation should not wait for corruption to happen before taking action. It must identify vulnerabilities early, assess them honestly and assign responsibility for controlling them.



ANTI-CORRUPTION RISK MANAGEMENT

CONTROLS MONITORING AND RESPONSE

LEVEL 2 •

PROFESSIONAL TRAINING MANUAL

Day 1 Recap and Day 2 Overview



DAY 1 RECAP AND DAY 2 OVERVIEW

Welcome back. Yesterday, we focused on finding and assessing corruption risks. Today, we move to the part that determines whether risk management produces results: **controlling the risks, monitoring the controls and responding when something goes wrong.**

In Day 1, we established that:

- Corruption risk management goes beyond awareness and policy statements
- Risks can arise from people, processes, systems and external relationships
- Process mapping helps locate vulnerable points in organisational activities
- Risk events must be linked to their causes and possible consequences
- Likelihood and impact are combined to determine the level of risk

- High and critical risks must receive greater attention and faster action
- A corruption risk register documents responsibilities, controls and deadlines

Day 2 will focus on how organisations reduce identified risks through practical and measurable action.

You will learn how to:

- Distinguish between preventive, detective and corrective controls
- Design controls that address specific corruption risks
- Use segregation of duties and approval procedures properly
- Strengthen financial, procurement and transaction controls
- Conduct due diligence on suppliers, agents and other third parties
- Manage gifts, hospitality and conflicts of interest
- Assign risk ownership and develop treatment plans
- Monitor control performance and recognise control failure
- Use warning indicators to identify changing risks
- Report, escalate and document corruption concerns
- Respond to suspected incidents and preserve relevant evidence

The key shift today is from **identifying the problem** to **doing something effective about it**. A risk assessment that does not lead to action is only paperwork.

Understanding Anti-Corruption Risk Controls



UNDERSTANDING ANTI-CORRUPTION RISK CONTROLS

Identifying and rating a corruption risk is not the final achievement. The real work begins when the organisation decides what must be done to reduce that risk. This is where anti-corruption risk controls come in.

An **anti-corruption risk control** is any policy, procedure, responsibility, system or practical action designed to prevent corruption, detect it early or reduce the damage it causes.

Examples include:

- Separating purchasing, approval and payment responsibilities
- Requiring employees to declare conflicts of interest
- Conducting background checks on suppliers and contractors

- Setting clear approval limits for transactions
- Restricting access to financial systems and confidential information
- Reviewing unusual payments and transaction patterns
- Providing confidential reporting channels
- Conducting independent audits and compliance checks
- Investigating misconduct and applying appropriate sanctions

A strong control should answer five questions:

- **Which specific risk does it address?**
- **Who is responsible for operating it?**
- **When and how should it be performed?**
- **What evidence proves that it was performed?**
- **Who checks whether it is working?**

For example, requiring three quotations is not enough if one employee can produce false quotations. The control becomes stronger when quotations are verified independently, supplier ownership is checked and the evaluation process is documented.

Controls may fail because they are poorly designed, inconsistently applied, easily overridden or never monitored. A policy that exists only on paper is not an effective control.

Organisations must also balance controls with operations. A control should reduce risk without creating unnecessary delays or making legitimate work impossible.

The central principle is clear: **a control is effective only when it addresses a specific risk, is consistently applied and can be proven to work.**

Preventive, Detective and Corrective Controls



PREVENTIVE, DETECTIVE AND CORRECTIVE CONTROLS

Let us be practical: no single control can completely eliminate corruption risk. An organisation needs controls that stop misconduct before it happens, expose it when it occurs and address the damage afterwards.

Anti-corruption controls are generally divided into three categories:

1. PREVENTIVE CONTROLS

These are designed to stop corruption before it occurs.

Examples include:

→ Segregation of duties

- Approval limits and authorisation procedures
- Conflict-of-interest declarations
- Employee and supplier background checks
- Competitive procurement procedures
- Restricted access to money, records and systems
- Anti-corruption policies and staff training

Preventive controls reduce opportunity, but dishonest individuals may still attempt to bypass them.

2. DETECTIVE CONTROLS

These are designed to identify suspicious activity during or after it occurs.

Examples include:

- Internal and external audits
- Transaction monitoring
- Bank and account reconciliations
- Inventory checks
- Whistleblowing and complaint channels
- Exception reports and system alerts
- Independent review of contracts and payments

A detective control is useful only when identified warning signs are reviewed and acted upon promptly.

3. CORRECTIVE CONTROLS

These are applied after misconduct or control failure has been discovered. Their purpose is to stop further damage, address the consequences and prevent recurrence.

Examples include:

- Suspending a suspicious payment
- Recovering stolen funds or assets
- Investigating the incident
- Applying disciplinary or legal action
- Correcting inaccurate records
- Closing the weakness that allowed the misconduct
- Revising policies, procedures or system permissions

Consider procurement fraud:

- Requiring competitive bidding is a **preventive control**
- Reviewing unusual supplier-payment patterns is a **detective control**
- Investigating the transaction and recovering the funds are **corrective controls**

The strongest approach combines all three. Prevention reduces opportunity, detection exposes misconduct and correction deals with the damage.

The principle is straightforward: **try to stop corruption, be prepared to detect what escapes prevention and act decisively when it is discovered.**

Designing Controls That Address Specific Risks



DESIGNING CONTROLS THAT ADDRESS SPECIFIC RISKS

A control should never be introduced simply because it sounds professional or appears in another organisation's policy. It must address the specific way corruption could occur in your own process.

Start with a clearly defined risk event.

For example:

Risk event: A procurement officer may leak confidential bid prices to a preferred supplier in exchange for a personal benefit.

The organisation should then ask:

→ What allows this event to happen?

- Who has access to the information?
- At what stage could it be disclosed?
- Which control could prevent or detect it?
- Who will operate and monitor the control?

Suitable controls may include:

- Restricting access to bid information
- Recording everyone who opens or downloads bid documents
- Requiring confidentiality declarations
- Separating bid receipt from bid evaluation
- Investigating unusual similarities between competing quotations
- Applying sanctions for unauthorised disclosure

A properly designed control should be:

- **Relevant:** It must address the identified risk and its causes.
- **Clear:** Employees must understand what to do, when to do it and who is responsible.
- **Practical:** It should work within the organisation's actual operations.
- **Proportionate:** Stronger risks should receive stronger controls.
- **Documented:** There must be evidence that the control was performed.
- **Monitored:** Someone independent should confirm that it is working.

Avoid weak controls such as “staff should act with integrity” or “management should be careful.” These statements express expectations, but they do not explain the action, responsibility, timing or evidence required.

Every control should answer:

- Who performs it?
- What action must be completed?
- When must it be completed?
- What evidence will be retained?
- Who reviews its effectiveness?

The key principle is simple: **do not attach general controls to specific risks.** Understand how the misconduct could occur, then design controls that directly block, expose or correct that particular route.

Segregation of Duties and Approval Controls



SEGREGATION OF DUTIES AND APPROVAL CONTROLS

One person should not control an important transaction from beginning to end. When the same individual can initiate, approve, execute and record an activity, corruption becomes easier to commit and harder to detect.

Segregation of duties means dividing key responsibilities among different people so that no individual has complete control over the entire process.

The main duties that should be separated are:

- **Initiation:** Requesting or starting the transaction
- **Authorisation:** Approving the transaction
- **Execution:** Carrying out the approved activity

- **Recording:** Entering it into the organisation's records
- **Custody:** Holding the money, assets or sensitive information
- **Review:** Independently checking what was done

For example, in procurement:

- One officer prepares the purchase request
- Another officer approves the request
- A committee evaluates suppliers
- A different employee confirms delivery
- Finance verifies the documents
- An authorised officer approves payment

Approval controls require designated officers to review and authorise transactions before they proceed.

Effective approval controls should include:

- Clearly documented approval limits
- Supporting documents for every decision
- Verification of prices, quantities and beneficiaries
- Additional approval for high-value or unusual transactions
- Electronic or written evidence showing who approved and when
- Restrictions preventing people from approving their own transactions

However, adding more signatures does not automatically create stronger control. If approvers sign documents without reviewing them, the approval becomes a formality rather than protection.

Smaller organisations may not have enough employees to separate every duty. In that situation, compensating controls should be introduced, such as:

- Regular owner or senior-management review
- Independent bank reconciliation
- Surprise cash and inventory checks
- Automated transaction alerts
- Periodic external review

Segregation of duties reduces individual opportunity, while approval controls ensure that important decisions receive proper scrutiny.

The rule is simple: **the person requesting, approving, executing and reviewing a transaction should not be the same person.**

Financial Controls and Transaction Monitoring



FINANCIAL CONTROLS AND TRANSACTION MONITORING

Money usually leaves an organisation through an approved transaction. The important question is whether that approval is legitimate, properly supported and given to the correct beneficiary. Without strong financial controls, fraud can look like ordinary business activity.

Financial controls are the procedures used to protect money and assets, ensure accurate records and prevent unauthorised transactions.

Important financial controls include:

- Approved budgets and spending limits
- Separation of payment preparation and approval
- Supporting documents for every transaction

- Independent verification of invoices and beneficiaries
- Bank and account reconciliations
- Restricted access to banking and accounting systems
- Dual authorisation for high-value payments
- Regular cash, payroll and expense reviews
- Independent review of changes to supplier bank details

Transaction monitoring means reviewing financial activity to identify unusual patterns, exceptions or warning signs.

Red flags may include:

- Duplicate or repeated invoice numbers
- Payments just below an approval limit
- One large payment divided into smaller amounts
- Repeated payments to one supplier
- Round-number invoices without adequate explanation
- Payments made outside normal working hours
- Sudden changes to supplier bank accounts
- Transactions without contracts, receipts or delivery evidence
- Payments to personal or unrelated accounts
- Refunds, discounts or write-offs approved by one employee
- New suppliers receiving large payments immediately

Automated systems can identify unusual transactions, but alerts must be reviewed by competent and independent officers. A warning that no one investigates is not an effective control.

Monitoring should be risk-based. High-value transactions, emergency purchases, cash payments, politically exposed relationships and high-risk suppliers require closer attention.

Suspicious activity does not automatically prove corruption. It signals the need for verification, documentation and possible escalation.

The principle is straightforward: **do not monitor only whether money was paid; examine who received it, why it was paid, who approved it and whether the transaction makes sense.**

Procurement and Contracting Risk Controls



PROCUREMENT AND CONTRACTING RISK CONTROLS

Procurement is one of the highest-risk areas in any organisation because it combines money, discretion, suppliers and important decisions. If the controls are weak, contracts can be manipulated long before payment is made.

Common procurement risks include:

- Specifications designed to favour one supplier
- Confidential bid information leaked to competitors
- False or coordinated quotations
- Undeclared relationships with suppliers
- Inflated prices and secret commissions

- Unqualified companies receiving contracts
- Contract values divided to avoid approval limits
- Poor-quality goods being accepted as satisfactory
- Payments made for work not completed

Effective procurement controls should cover the entire contracting process.

Before supplier selection:

- Confirm that the purchase is necessary and budgeted
- Develop clear, objective specifications
- Conduct background and beneficial-ownership checks
- Require conflict-of-interest declarations
- Use competitive bidding unless an exception is properly justified

During evaluation and award:

- Use an independent evaluation committee
- Apply predetermined scoring criteria
- Protect confidential bidding information
- Document scores, decisions and reasons for selection
- Compare prices with reliable market information
- Obtain higher approval for large or unusual contracts

During delivery and payment:

- Verify that goods or services were received
- Separate contract management from payment approval
- Match the purchase order, delivery evidence and invoice
- Inspect quality before accepting delivery
- Monitor contract changes, extensions and additional costs
- Pay only into verified supplier accounts

Emergency procurement requires particular attention. Urgency may justify a faster process, but it should not eliminate documentation, price checks, approval and independent review.

The organisation should also monitor warning signs such as repeated awards to one supplier, identical quotations, unexplained price increases, frequent contract variations and close relationships between employees and contractors.

The key point is simple: **procurement control does not end when a supplier is selected.** Every stage—from identifying the need to approving the final payment—must remain transparent, documented and independently reviewed.

Third-Party, Agent and Supplier Due Diligence



THIRD-PARTY, AGENT AND SUPPLIER DUE DILIGENCE

An organisation can be exposed to corruption through people who are not on its payroll. Agents, consultants, suppliers, contractors and business partners may offer bribes, conceal ownership or make improper payments while claiming to act on the organisation's behalf.

Due diligence means checking a third party's identity, ownership, reputation, capability and risk level before entering or continuing a business relationship.

Before appointing a third party, verify:

- The legal name, address and registration details
- The identities of directors and beneficial owners
- Relevant qualifications and operational capacity

- Previous contracts and business experience
- Connections to employees, public officials or decision-makers
- History of fraud, corruption, sanctions or legal violations
- Bank-account ownership and payment details
- The reason for using an agent or intermediary
- Whether the proposed fees are reasonable for the work

Warning signs may include:

- Refusal to disclose the real owners of the business
- A recently registered company seeking a major contract
- No physical office, staff or relevant experience
- Unusually high commissions or vague consultancy fees
- Requests for payment in cash or into a personal account
- Requests for payment in another country without justification
- Close relationships with officials or employees
- Insistence that the third party can “guarantee” an approval
- Negative reports involving dishonesty or misconduct

Due diligence should be proportionate to the risk. A high-value agent dealing with government officials requires more investigation than a low-risk supplier providing routine items.

The contract should also include:

- Anti-bribery and ethical-conduct requirements
- Accurate record-keeping obligations
- Rights to inspect or audit relevant records
- Immediate reporting of conflicts or suspicious demands
- Termination rights for corruption or false information

Due diligence does not end after appointment. Third parties must be monitored throughout the relationship, particularly when ownership, bank details, payment patterns or responsibilities change.

The key principle is clear: **you cannot outsource a service and assume you have outsourced the corruption risk.** Know who represents your organisation, how they operate and who ultimately benefits.

Managing Gifts, Hospitality and Conflict-of-Interest Risks



MANAGING GIFTS, HOSPITALITY AND CONFLICT-OF-INTEREST RISKS

Not every gift is a bribe, and not every personal relationship is corrupt. But once a gift, favour or private interest can influence—or appear to influence—a professional decision, the organisation has a risk that must be managed.

Gifts and hospitality may include:

- Cash or gift cards
- Meals and entertainment
- Travel and accommodation
- Event tickets
- Discounts and free services

→ Personal favours

→ Donations made on someone's behalf

A gift or hospitality becomes particularly risky when it:

→ Is offered during bidding, inspection or contract renewal

→ Is unusually valuable, frequent or secret

→ Is given to a decision-maker or family member

→ Creates an expectation of favourable treatment

→ Is provided in cash or cash equivalent

→ Would embarrass the organisation if publicly disclosed

Clear controls should require:

→ Defined value limits and prohibited items

→ Prior approval for high-risk hospitality

→ Declaration and recording in a gifts register

→ Refusal or return of inappropriate gifts

→ Independent review of repeated gifts from one source

→ Consistent sanctions for violations

A **conflict of interest** exists when personal, family, financial or outside interests could interfere with an employee's professional judgement.

Examples include:

→ Evaluating a company owned by a relative

→ Recruiting a close friend without disclosure

→ Holding shares in a supplier

→ Running a private business that competes with the employer

→ Supervising or approving payments to a partner's company

Having a conflict is not automatically corruption. **Concealing it and participating in the decision** creates the serious risk.

Employees should therefore:

→ Declare actual, potential and perceived conflicts

→ Withdraw from affected decisions

→ Avoid accessing confidential information related to the matter

→ Allow an independent person to manage the process

→ Update declarations when circumstances change

The key principle is simple: **if a gift, favour or personal interest could affect—or appear to affect—your judgement, declare it before taking part in the decision.**



ASSIGNING RISK OWNERSHIP AND ACCOUNTABILITY

A corruption risk that belongs to “everybody” usually ends up being managed by nobody. Every significant risk must have a named person who is responsible for ensuring that it is properly controlled and monitored.

A **risk owner** is the person with enough authority and knowledge to manage a specific risk. This person does not personally perform every control, but remains accountable for ensuring that the necessary actions are completed.

The risk owner should:

- Understand the risk, its causes and possible consequences
- Confirm that appropriate controls are in place

- Assign control activities to competent employees
- Monitor whether the controls are working
- Ensure weaknesses are corrected within agreed deadlines
- Escalate serious issues to senior management
- Update the corruption risk register
- Report changes in the risk level

For example, the Head of Procurement may own the risk of supplier favouritism, while procurement officers, evaluation committee members and compliance staff perform different controls.

It is important to distinguish between two responsibilities:

- **Risk owner:** Accountable for managing the overall risk
- **Control owner:** Responsible for performing or supervising a particular control

Clear accountability should state:

- Who owns the risk
- Who performs each control
- What action is required
- When it must be completed
- What evidence must be retained
- Who receives reports when problems occur

The risk owner must have sufficient authority and access to information. Assigning responsibility to a junior employee who cannot challenge senior management or enforce corrective action is not genuine accountability.

Senior leadership also remains responsible for oversight. Management cannot assign risk ownership and then ignore whether the risk is being properly managed.

The principle is simple: **every major corruption risk must have a named owner, every control must have a responsible person and every failure must have a clear route for escalation.**



DEVELOPING A CORRUPTION RISK TREATMENT PLAN

Once a corruption risk has been identified and rated, management must decide exactly what will be done about it. Writing “improve controls” is not a treatment plan. It is a vague intention with no clear action, owner or deadline.

A **corruption risk treatment plan** is a documented programme of actions designed to reduce a risk to an acceptable level.

An organisation generally has four treatment options:

- **Avoid the risk:** Stop or redesign the activity creating unacceptable exposure.
- **Reduce the risk:** Introduce stronger preventive, detective or corrective controls.

- **Transfer or share the risk:** Use insurance, contractual protection or qualified external providers where appropriate.
- **Accept the risk:** Retain a low or unavoidable risk with documented approval and continued monitoring. Acceptance must never be used to ignore illegal conduct. An organisation cannot “accept” bribery, fraud or other criminal behaviour.

A proper treatment plan should state:

- The specific corruption risk being treated
- The current risk rating
- Weaknesses in existing controls
- The additional controls required
- The person responsible for each action
- The resources needed
- The implementation deadline
- The expected residual risk
- How progress and effectiveness will be monitored

For example:

Risk: A procurement officer may favour a related supplier.

Treatment actions:

- Introduce mandatory conflict-of-interest declarations
- Verify supplier beneficial ownership
- Establish an independent evaluation committee
- Rotate procurement responsibilities periodically
- Review previous awards involving connected suppliers

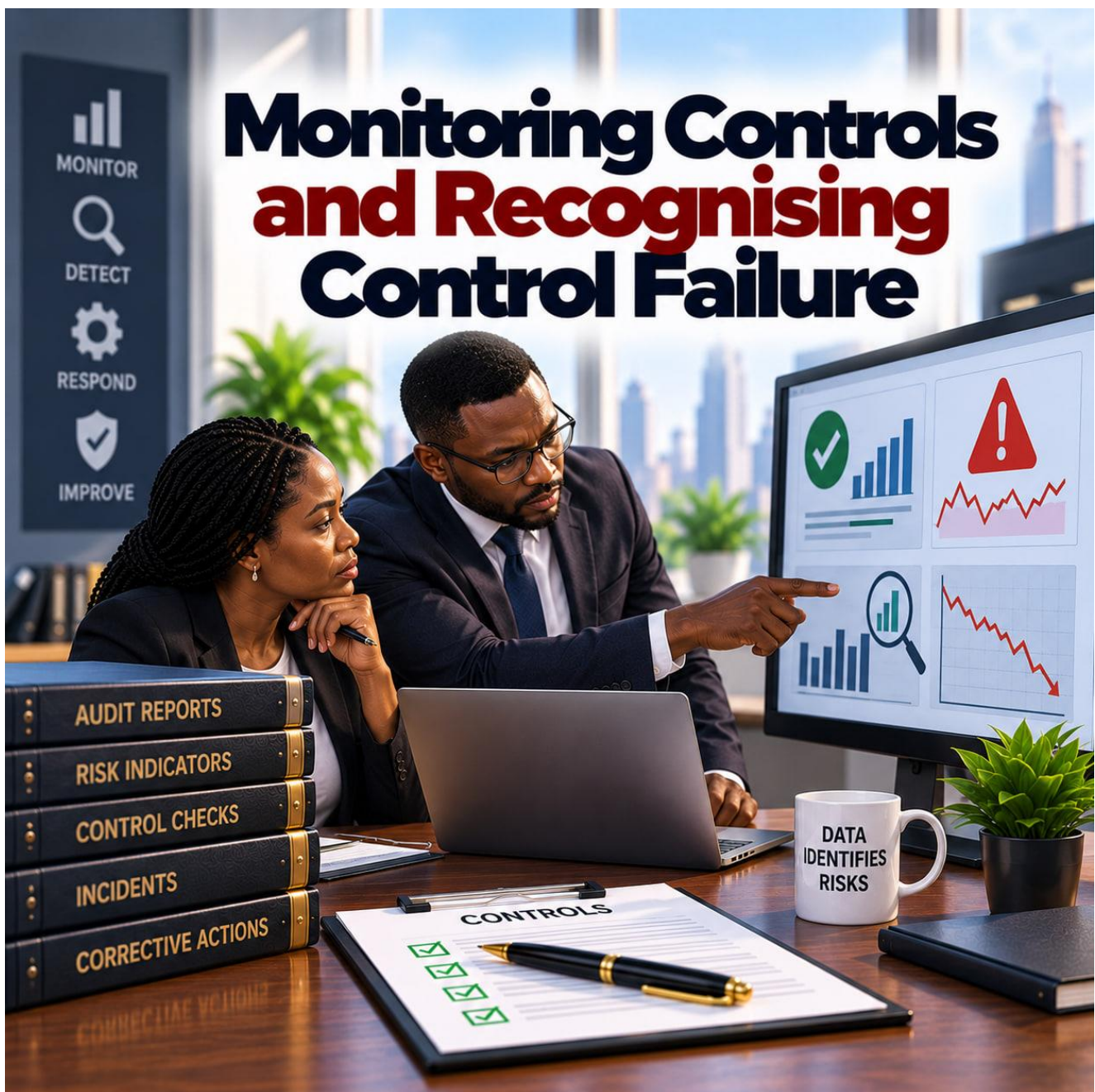
Risk owner: Head of Procurement

Deadline: Within 30 days

Expected result: Reduce the risk from high to moderate

Treatment actions should be specific, realistic and measurable. After implementation, the organisation must test whether the controls actually reduced the risk. If the residual risk remains too high, additional action is required.

The key principle is clear: **every serious corruption risk needs a defined response, a responsible owner, a firm deadline and evidence that the treatment worked.**



MONITORING CONTROLS AND RECOGNISING CONTROL FAILURE

Putting a control in place does not mean the risk is permanently managed. A control can look impressive in a policy document and still fail completely in practice. That is why controls must be monitored, tested and improved.

Control monitoring means checking whether a control:

- Is properly designed for the identified risk
- Is being performed as required
- Is consistently applied to every relevant transaction
- Produces reliable evidence
- Cannot be easily bypassed or overridden

→ Is actually reducing the risk

Monitoring methods may include:

- Reviewing approvals and supporting documents
- Testing a sample of transactions
- Examining system logs and exception reports
- Conducting surprise cash or inventory checks
- Comparing supplier prices with market rates
- Following up on complaints and whistleblower reports
- Interviewing employees who operate the controls
- Tracking corrective actions and missed deadlines

Warning signs of control failure include:

- Documents signed without proper review
- Repeated exceptions treated as normal
- Missing records or unexplained alterations
- One person regularly bypassing established procedures
- System alerts being ignored or disabled
- The same irregularity appearing in several audits
- Senior managers overriding controls without justification
- Employees performing incompatible duties
- Corrective actions remaining incomplete after deadlines

Control failure can happen in two main ways:

- **Design failure:** The control is not capable of addressing the risk.
- **Operating failure:** The control is suitable, but people do not perform it correctly or consistently.

For example, requiring three quotations may be a reasonable control. However, it fails if employees submit fabricated quotations and approvers never verify them.

When failure is identified, the organisation should determine the cause, strengthen or replace the control, assign responsibility and reassess the residual risk.

The principle is straightforward: **do not ask only whether a control exists—ask whether it is working, whether there is evidence and whether it is actually reducing the risk.**

Key Risk Indicators and Early-Warning Signs



KEY RISK INDICATORS AND EARLY-WARNING SIGNS

Corruption rarely begins with a complete confession or a clearly labelled fraudulent payment. It usually produces small warning signs first. The organisation must know what to watch before those signs develop into serious losses.

A **Key Risk Indicator (KRI)** is a measurable signal showing that corruption exposure may be increasing or that a control may be weakening.

Examples of KRIs include:

- A rising number of contracts awarded without competition
- Repeated purchases just below approval limits
- Increasing use of emergency procurement

- Frequent changes to supplier bank details
- Unusual growth in payments to one supplier
- High numbers of missing receipts or supporting documents
- Repeated control overrides by the same manager
- Increasing unresolved whistleblower complaints
- Employees failing to submit conflict-of-interest declarations
- Large contract variations after the original award

Other early-warning signs may include:

- An employee refusing to take leave or share responsibilities
- A supplier receiving favourable treatment without explanation
- Employees and contractors having undisclosed personal relationships
- Records being altered, backdated or removed
- Staff members becoming defensive during routine reviews
- Payments made to personal or unrelated accounts
- Lifestyle changes inconsistent with known income
- Audit findings recurring without corrective action

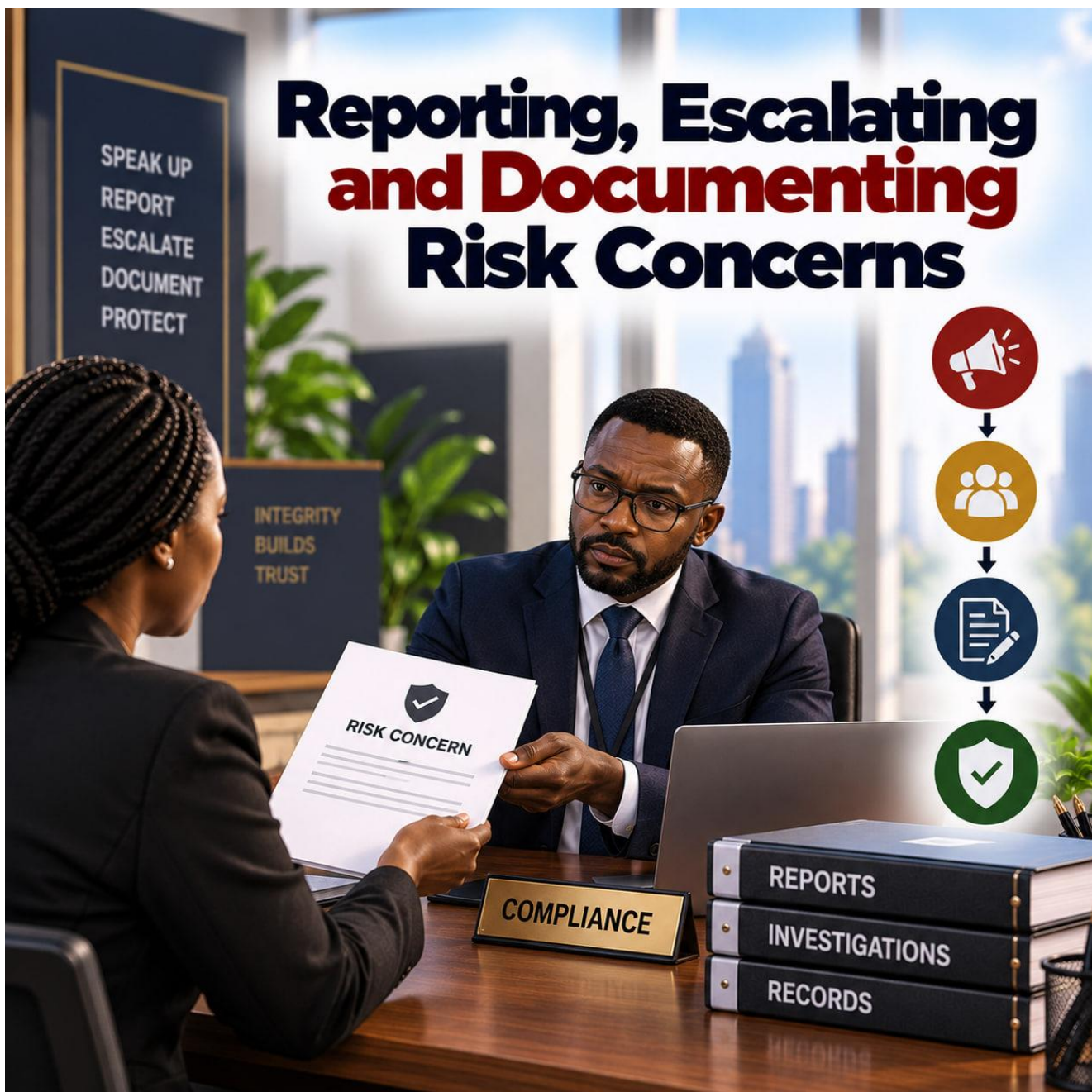
A useful KRI should have:

- A clear definition
- A reliable source of information
- A person responsible for monitoring it
- A threshold that triggers investigation or escalation
- A defined reporting frequency

For example, an organisation may decide that more than three non-competitive contracts in one month will trigger an independent procurement review.

A warning sign is not automatic proof of corruption. It is a reason to examine the transaction, verify the facts and determine whether controls are failing.

The main principle is simple: **do not wait for confirmed corruption before paying attention. Monitor the signals that show the risk is increasing.**



REPORTING, ESCALATING AND DOCUMENTING RISK CONCERNS

Spotting a corruption risk is useful only if the concern reaches someone who can act. Silence, delay and poor documentation can allow a manageable warning sign to become a serious incident.

Reporting means communicating the concern through an approved channel.

Escalation means referring the matter to a higher or more independent authority because of its seriousness, urgency or the people involved.

Documentation means creating an accurate record of what was observed, reported and done.

A risk concern should clearly state:

→ What was observed or discovered

- When and where it occurred
- Which people, transactions or processes were involved
- Which documents or records may support the concern
- What risk or possible violation was identified
- Whether immediate action is required
- Who received the report and when

Reports should be based on facts rather than rumours, insults or unsupported conclusions. If something is uncertain, clearly describe it as a concern requiring verification.

Available reporting channels may include:

- A direct supervisor
- Compliance or risk-management personnel
- Internal audit
- A confidential whistleblowing channel
- Senior management or the board
- An authorised external regulator or law-enforcement body

Normal reporting lines should not be used when the person receiving the report may be involved. The concern must be escalated to an independent authority.

Immediate escalation may be necessary when:

- Senior management may be involved
- Evidence could be destroyed
- Funds may be transferred or removed
- People may face threats or retaliation
- Public safety or essential services are at risk
- The misconduct may continue if action is delayed

Documentation should be factual, dated, secure and confidential. Original records must not be altered, and access should be limited to authorised persons.

The reporter should not conduct an unauthorised investigation, confront suspected individuals or circulate allegations publicly. These actions may expose the reporter, damage evidence or compromise a legitimate investigation.

The key principle is clear: **report facts promptly, escalate according to the seriousness of the risk and preserve an accurate record of every action taken.**



RESPONDING TO SUSPECTED CORRUPTION INCIDENTS

When corruption is suspected, the organisation must act quickly—but not recklessly. A careless response can destroy evidence, expose whistleblowers, damage innocent people or allow those involved to conceal what happened.

A suspicion is not the same as proven guilt. The immediate objective is to protect people, records, funds and the integrity of the investigation.

The organisation should:

- Record the allegation or warning signs accurately
- Assess the seriousness and urgency of the situation
- Notify the appropriate authorised personnel

- Protect the identity of the reporter where possible
- Secure relevant documents, devices and transaction records
- Prevent suspicious payments or activities from continuing
- Manage conflicts involving investigators or decision-makers
- Decide whether external authorities must be notified
- Begin a fair and properly authorised investigation

Immediate protective action may include:

- Temporarily restricting access to financial systems
- Suspending a payment or contract approval
- Preserving emails, system logs and CCTV records
- Reassigning sensitive responsibilities
- Separating suspected individuals from relevant records
- Protecting employees against threats or retaliation

These actions should be lawful, proportionate and documented. They are protective measures—not automatic declarations of guilt.

Employees must not:

- Confront or warn the suspected person without authorisation
- Alter, remove or secretly circulate evidence
- Discuss the allegation with unrelated colleagues
- Post accusations publicly or on social media
- Make promises about the investigation's outcome
- Attempt to investigate matters beyond their authority

The investigation should establish what happened, who was involved, which controls failed, what damage occurred and what corrective action is required.

Afterwards, the organisation may need to:

- Recover funds or assets
- Apply disciplinary measures
- Report offences to relevant authorities
- Correct financial and operational records
- Strengthen failed controls
- Reassess the corruption risk

The key principle is straightforward: **respond promptly, preserve evidence, protect confidentiality and follow a fair, authorised process.**

Investigation Readiness and Evidence Preservation



INVESTIGATION READINESS AND EVIDENCE PRESERVATION

An organisation should not wait until corruption is suspected before deciding how an investigation will be handled. By then, records may already be missing, responsibilities may be unclear and suspected individuals may have been alerted.

Investigation readiness means having the policies, people, procedures and systems required to respond properly when misconduct is reported or detected.

A prepared organisation should have:

- A clear incident-reporting and escalation procedure
- Trained and authorised investigators
- Independent oversight of sensitive investigations

- Defined roles for management, compliance, audit, legal and human resources
- Procedures for protecting whistleblowers and witnesses
- Secure systems for storing reports and evidence
- Rules for managing confidentiality and conflicts of interest
- Criteria for involving regulators or law-enforcement agencies

Evidence preservation means protecting relevant information from being altered, destroyed, lost or accessed without authorisation.

Possible evidence may include:

- Contracts, invoices, receipts and bank records
- Emails, messages and call records
- System logs and access histories
- Personnel and supplier records
- Meeting minutes and approval documents
- CCTV recordings and access-control data
- Physical documents, devices or assets

When an incident is identified, authorised personnel should:

- Record when, where and how the evidence was obtained
- Preserve original documents and work from secure copies
- Restrict access to authorised individuals
- Prevent routine deletion of relevant electronic records
- Document every transfer or examination of evidence
- Store physical and digital materials securely

The documented history showing who collected, handled, transferred and stored evidence is known as the **chain of custody**. Weak chain-of-custody records can create doubts about whether evidence was altered or mishandled.

Employees should not search personal devices, seize property, access private accounts or secretly record people without proper authority and legal guidance.

The principle is clear: **a strong investigation depends on evidence that is relevant, secure, traceable and lawfully obtained.**



LEADERSHIP, GOVERNANCE AND CONTINUOUS IMPROVEMENT

Anti-corruption controls will not remain effective if leaders ignore them, bypass them or apply them only to junior employees. Staff members pay more attention to what leaders do than to what organisational policies say.

Leadership sets the ethical direction of the organisation. Leaders must:

- Demonstrate integrity in their own decisions
- Follow the same controls required of other employees
- Refuse improper pressure, gifts and favours
- Provide resources for risk management and compliance
- Protect employees who report concerns honestly

→ Take consistent action when misconduct occurs

Governance provides the structure through which corruption risks are supervised and controlled.

Good governance requires:

→ Clear roles for the board, management, audit and compliance functions

→ Independent oversight of high-risk decisions

→ Transparent approval and reporting procedures

→ Regular review of corruption risks and control failures

→ Accurate information reaching the appropriate decision-makers

→ Accountability for overdue or incomplete corrective actions

→ Consistent consequences regardless of rank or influence

Leaders should not receive only comfortable reports. They need accurate information about:

→ High and critical corruption risks

→ Control failures and repeated exceptions

→ Whistleblower allegations and investigation outcomes

→ Delayed risk-treatment actions

→ Emerging risks involving employees or third parties

→ Lessons from audits, incidents and complaints

Continuous improvement means learning from experience and strengthening the anti-corruption system over time.

This may involve:

→ Reviewing risk assessments when operations change

→ Updating policies and approval limits

→ Improving staff training

→ Replacing controls that are no longer effective

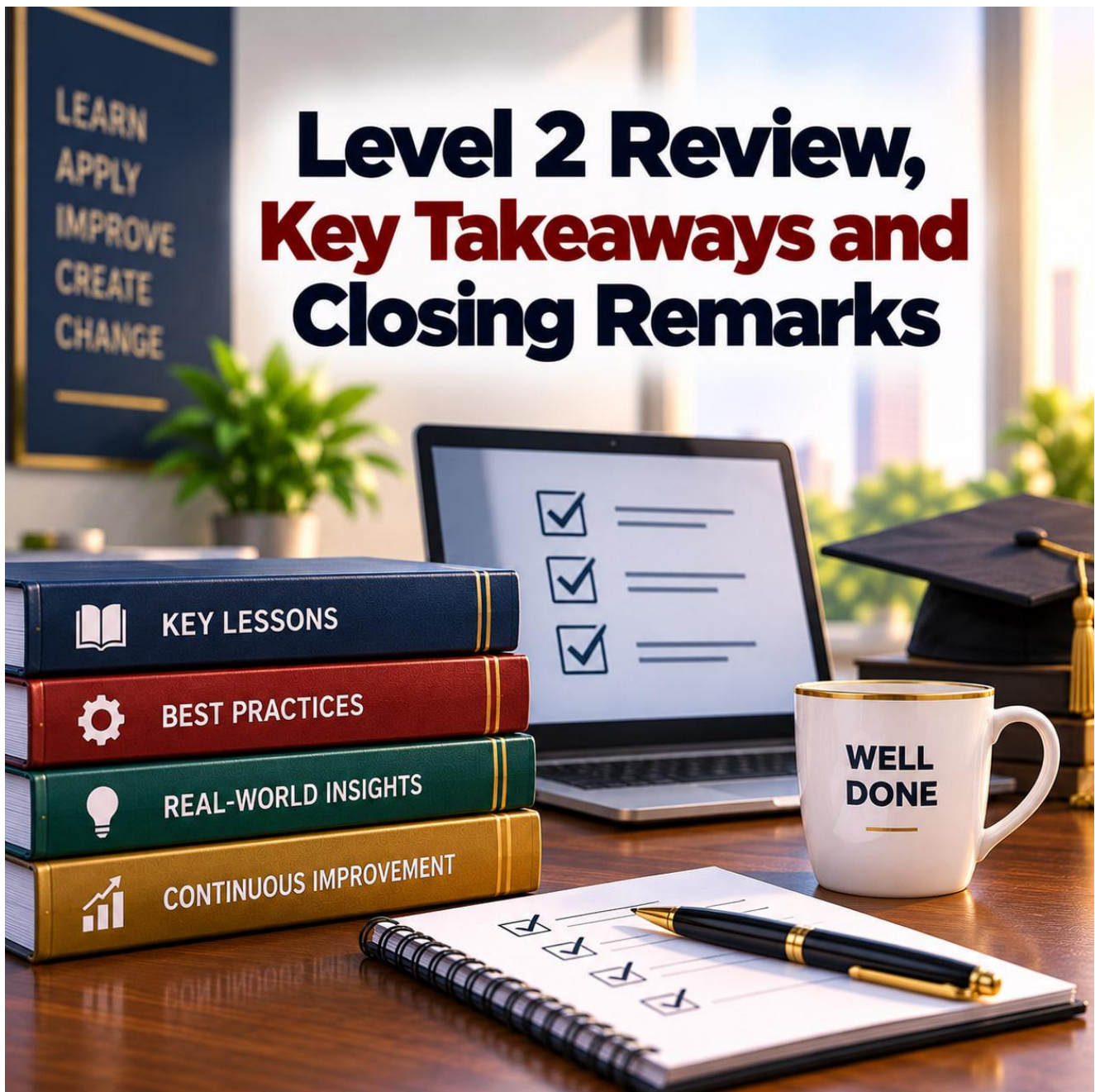
→ Using investigation findings to close control gaps

→ Monitoring whether corrective actions produce results

An organisation should not treat every incident as an isolated case. If misconduct occurs, management must ask what weakness allowed it, whether similar risks exist elsewhere and what must change.

The central principle is simple: **leaders set the standard, governance maintains accountability and continuous improvement prevents yesterday's weakness from becoming tomorrow's corruption scandal.**

Level 2 Review, Key Takeaways and Closing Remarks



LEVEL 2 REVIEW, KEY TAKEAWAYS AND CLOSING REMARKS

We have reached the end of **Anti-Corruption and Risk Management — Level 2**. The central message of this course is straightforward: corruption should not be managed only after money is lost, evidence disappears or public trust is damaged. It must be anticipated and controlled.

The major lessons from Level 2 are:

- Anti-corruption awareness explains misconduct, while risk management identifies where and how it could occur.
- Corruption risks may originate from people, processes, systems, leadership decisions and external relationships.
- A properly written risk event explains the specific misconduct that could happen.
- Risk causes explain why the event could occur, while consequences describe the damage it could produce.

- Process mapping exposes vulnerable decision points, control gaps and excessive concentrations of authority.
- Likelihood measures the probability of occurrence, while impact measures the seriousness of the possible harm.
- A risk matrix helps rate and prioritise corruption risks consistently.
- A corruption risk register records risks, controls, owners, deadlines and review status.
- Preventive controls reduce opportunities for corruption.
- Detective controls reveal suspicious activity and control failures.
- Corrective controls address confirmed incidents, losses and weaknesses.
- Segregation of duties prevents one person from controlling an entire transaction.
- Financial monitoring helps identify unusual payments, split transactions, false invoices and unsupported expenses.
- Procurement controls must cover the full process, from identifying a need to approving payment.
- Third-party due diligence must establish who owns, controls and benefits from an external organisation.
- Gifts, hospitality and conflicts of interest must be declared and independently managed.
- Every significant risk requires a named owner, treatment plan and implementation deadline.
- Controls must be tested because their existence does not prove that they work.
- Key Risk Indicators provide early warning that exposure is increasing.
- Suspected incidents must be reported, escalated and documented through authorised channels.
- Evidence must be preserved securely and handled through a documented chain of custody.
- Leadership must follow the controls, demand accurate reporting and act consistently when failures occur.

Completing a risk assessment is not the end of the process. The real result is achieved when identified risks lead to stronger controls, clear accountability, continuous monitoring and measurable improvement.

You are now expected to move beyond saying, **“Corruption is wrong.”** You should be able to ask where it could happen, why the opportunity exists, how serious the exposure is, who owns the risk and whether the controls genuinely work.

That is the professional standard of corruption risk management.