

A man in a dark suit, white shirt, and red tie is seated at a desk, intently examining a document with a magnifying glass. The background features a dark blue globe with glowing connection points, a golden shield emblem with a classical building facade, and a pair of golden scales of justice. To the left, a stack of papers and a pen are visible on the desk.

Advanced **Anti-Corruption** Governance and Financial Crime Prevention — **Level 3**

ADVANCED ANTI-CORRUPTION GOVERNANCE

FINANCIAL CRIME PREVENTION

LEVEL 3

ADVANCED PROFESSIONAL TRAINING MANUAL

Copyright Notice**ADVANCED ANTI-CORRUPTION GOVERNANCE AND
FINANCIAL CRIME PREVENTION — LEVEL 3**

© 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.



WELCOME, LEVEL 2 RECAP AND LEVEL 3 OBJECTIVES

Welcome to **Advanced Anti-Corruption Governance and Financial Crime Prevention — Level 3.**

You have already covered the foundations. Level 1 explained corruption, financial integrity, ethical conduct and responsible reporting. Level 2 moved further by showing you how to identify corruption risks, assess their likelihood and impact, design controls and monitor whether those controls actually work.

Level 3 now takes you into advanced professional territory. The focus is no longer limited to individual misconduct or isolated control failures. You will examine how leadership, governance structures, financial systems and organised criminal activities can expose an entire institution.

In Level 2, you learned how to:

- Identify corruption risks within people, processes and systems
- Assess inherent and residual risk
- Use likelihood, impact and risk matrices
- Create corruption risk registers and treatment plans
- Apply preventive, detective and corrective controls
- Conduct third-party and supplier due diligence
- Monitor transactions and recognise control failure
- Report incidents and preserve evidence

In Level 3, you will learn how to:

- Understand advanced anti-corruption governance
- Examine the responsibilities of boards and senior leadership
- Develop an effective anti-corruption governance framework
- Strengthen compliance, internal audit and oversight functions
- Manage political exposure and high-risk relationships
- Conduct enhanced due diligence and identify beneficial owners
- Understand fraud, money laundering and other financial crimes
- Recognise the stages and warning signs of money laundering
- Manage risks involving politically exposed persons
- Apply customer and transaction-monitoring controls
- Recognise cyber-enabled fraud and digital financial crime
- Understand suspicious transaction reporting
- Strengthen investigation, asset-tracing and recovery processes

The standard at this level is higher. You are expected to move beyond recognising misconduct and begin examining whether the organisation's leadership, governance and financial-crime controls are strong enough to prevent, detect and respond to sophisticated abuse.

The central question throughout Level 3 is simple: **when corruption becomes organised, concealed and supported by weak governance, can the institution still detect it and act?**



UNDERSTANDING ADVANCED ANTI-CORRUPTION GOVERNANCE

Let us be clear: corruption does not survive only because individuals are dishonest. It survives when leadership looks away, oversight is weak, responsibilities are unclear and powerful people can override controls without consequences.

Advanced anti-corruption governance is the system through which an organisation directs, supervises and holds people accountable for preventing, detecting and responding to corruption.

It goes beyond having an anti-corruption policy. It examines whether:

- The board and senior leadership provide genuine oversight
- Ethical expectations apply equally to everyone
- Compliance and internal audit functions are independent
- High-risk decisions receive proper scrutiny
- Employees can report concerns without retaliation
- Conflicts of interest are declared and managed
- Control failures are reported to the right authority
- Investigations are fair and protected from interference
- Corrective actions are completed and monitored
- Leaders are held accountable for ignoring known risks

A strong governance system should clearly define the roles of:

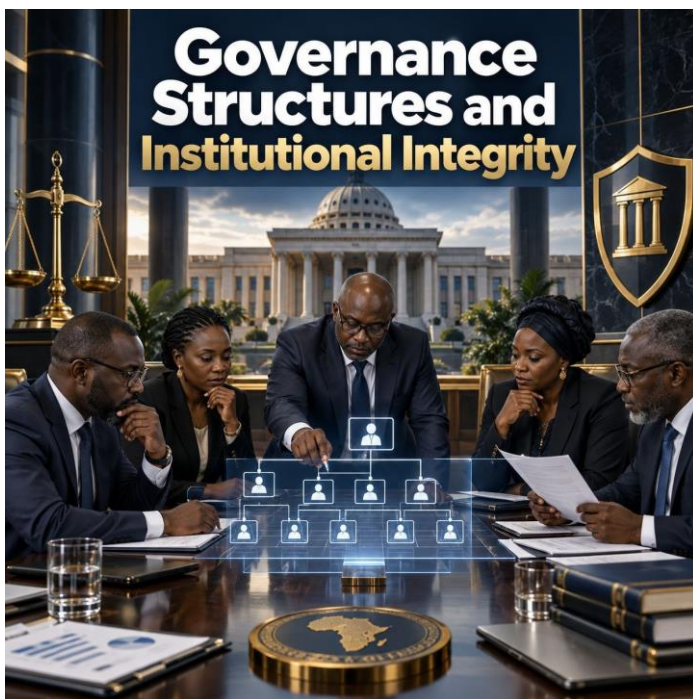
- **The board:** Provides oversight and challenges senior management
- **Senior management:** Implements the anti-corruption programme and provides resources
- **Compliance and risk functions:** Identify risks, advise management and monitor controls
- **Internal audit:** Independently evaluates whether governance and controls are working
- **Managers:** Apply controls and supervise high-risk activities
- **Employees:** Follow procedures and report concerns responsibly

Governance becomes weak when the same people create the rules, approve exceptions, investigate allegations and decide whether sanctions should apply.

For example, if a chief executive can approve a high-value contract involving a relative without independent review, the organisation has a governance failure—not merely a conflict-of-interest problem.

Advanced governance therefore requires independence, transparency, documented authority and meaningful consequences. No person should be so powerful that controls cannot question their decisions.

The key principle is simple: **anti-corruption governance is effective only when authority is controlled, oversight is independent and accountability reaches the highest level of the organisation.**



GOVERNANCE STRUCTURES AND INSTITUTIONAL INTEGRITY

An organisation cannot depend on the personal honesty of one leader. Leaders change, employees move and pressure increases. Integrity must therefore be built into the organisation's structure, responsibilities and decision-making processes.

A **governance structure** explains who has authority, who provides oversight, who manages risks and who can challenge improper decisions.

An effective structure should include:

- A board or governing body providing independent oversight
- Senior management responsible for implementing policies and controls
- A compliance function monitoring legal and ethical obligations
- A risk-management function assessing corruption exposure

- Internal audit independently testing governance and controls
- Human resources managing conduct and disciplinary procedures
- Legal advisers supporting investigations and regulatory reporting
- Clear reporting channels for employees and external stakeholders

Institutional integrity means the organisation consistently operates according to ethical principles, professional standards and established rules—regardless of who is involved.

Signs of institutional integrity include:

- Decisions are based on documented criteria
- Responsibilities and approval limits are clearly defined
- Conflicts of interest are declared and managed
- Records are accurate, complete and accessible for review
- Whistleblowers are protected against retaliation
- Investigations are free from improper interference
- Rules apply equally to junior employees and senior leaders
- Misconduct leads to consistent and proportionate consequences

Weak governance structures usually show the opposite:

- Unclear responsibilities
- Concentrated authority
- Informal decision-making
- Selective enforcement
- Management override without explanation
- Compliance officers reporting to suspected individuals
- Audit findings repeatedly ignored

A structure may look impressive on paper and still fail if people lack independence, authority or access to information. The real test is whether the system can challenge a powerful decision-maker without fear.

The key principle is clear: **institutional integrity exists when ethical conduct is protected by the organisation's structure—not left to individual goodwill.**



THE ROLE OF BOARDS AND SENIOR LEADERSHIP

Let us be direct: if the board and senior leadership are not serious about anti-corruption, the rest of the organisation will notice. Policies may exist, training may be conducted and reports may be submitted, but employees will follow the behaviour that leadership rewards or tolerates.

The **board or governing body** provides independent oversight of the organisation's anti-corruption programme.

Its responsibilities include:

- Approving the anti-corruption governance framework
- Understanding the organisation's major corruption risks
- Challenging management on high-risk decisions

- Ensuring compliance, risk and audit functions remain independent
- Reviewing serious allegations and investigation outcomes
- Monitoring overdue corrective actions
- Ensuring senior executives are held accountable
- Confirming that adequate resources are available

Senior leadership is responsible for turning board expectations into daily organisational practice.

Its responsibilities include:

- Communicating clear ethical standards
- Implementing policies and controls
- Assigning competent risk and control owners
- Providing staff, funding and technology for compliance activities
- Responding promptly to warning signs and control failures
- Protecting whistleblowers against retaliation
- Applying consequences consistently
- Reporting serious risks accurately to the board

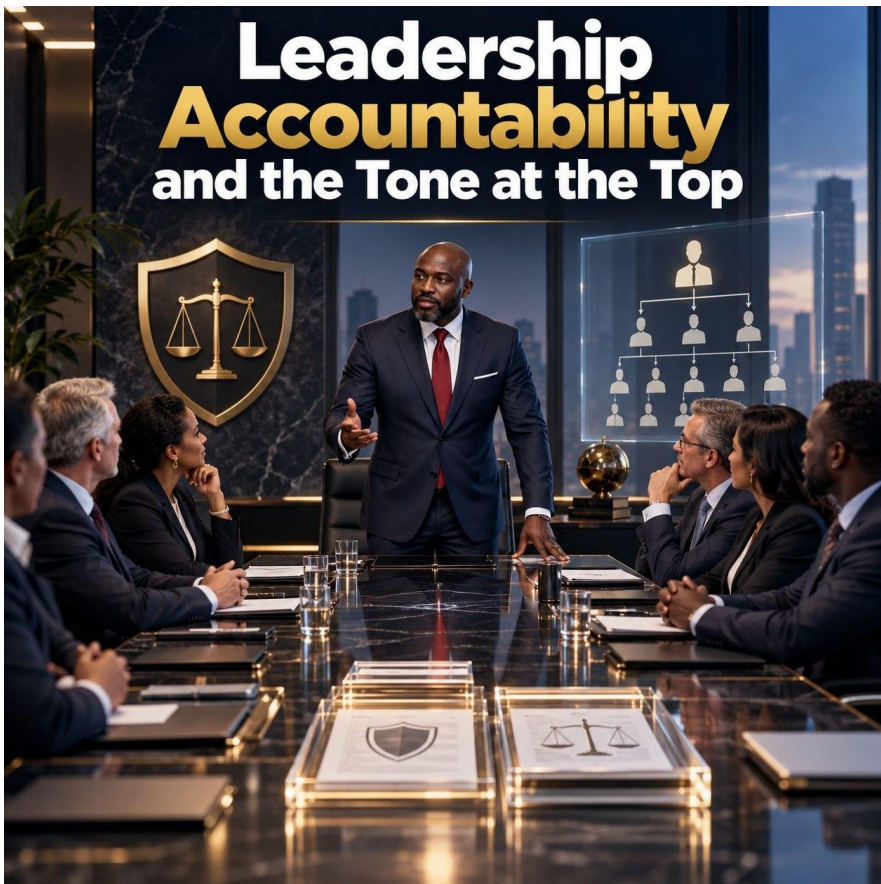
Boards and executives should regularly receive information on:

- High and critical corruption risks
- Serious control failures and management overrides
- Whistleblower complaints and retaliation concerns
- Investigation findings and disciplinary outcomes
- Third-party and politically exposed relationships
- Delayed risk-treatment actions
- Trends in fraud, bribery and financial-crime indicators

Leadership failure occurs when decision-makers ignore red flags, suppress reports, interfere with investigations or protect influential offenders.

Board members must also remain independent. They should declare conflicts of interest, withdraw from affected decisions and avoid using their position for personal benefit.

The central principle is simple: **the board provides oversight, senior leadership drives implementation and both remain accountable for the integrity of the organisation.**



LEADERSHIP ACCOUNTABILITY AND THE TONE AT THE TOP

Employees watch what leaders do more closely than they read policy documents. If leaders bypass controls, protect favourites or punish people who raise concerns, that behaviour becomes the organisation's real standard.

Tone at the top refers to the ethical example, expectations and priorities established by the board and senior leadership.

A strong tone at the top exists when leaders:

→ Follow the same rules required of employees

- Declare and manage their own conflicts of interest
- Reject improper gifts, payments and influence
- Support independent compliance and audit functions
- Encourage responsible reporting
- Protect whistleblowers from retaliation
- Respond promptly to control failures
- Apply consequences regardless of position or influence
- Communicate honestly about identified weaknesses

Leadership accountability means decision-makers must explain and accept responsibility for their actions, omissions and control failures.

Leaders should be held accountable when they:

- Approve transactions without proper review
- Override controls without documented justification
- Ignore repeated audit findings
- Suppress reports or interfere with investigations
- Protect employees or third parties involved in misconduct
- Fail to act after receiving credible warning signs
- Create unrealistic targets that encourage unethical behaviour

A leader may not personally receive a bribe, but can still contribute to corruption by ignoring known weaknesses or allowing misconduct to continue.

The organisation must also avoid **selective accountability**.

Disciplining junior employees while protecting senior executives destroys trust and encourages further misconduct.

Leadership performance should therefore include measurable integrity responsibilities, such as completing corrective actions, responding to reports and maintaining effective controls.

The principle is straightforward: **leaders set the real standard through the behaviour they demonstrate, the misconduct they tolerate and the accountability they accept.**



INDEPENDENCE OF COMPLIANCE AND INTERNAL AUDIT FUNCTIONS

Compliance and internal audit cannot protect an organisation if they are afraid to question senior management. If the people being reviewed can control the reviewer's work, budget, access to information or career, genuine oversight becomes difficult.

Compliance helps the organisation understand and meet its legal, regulatory and ethical responsibilities.

Its responsibilities may include:

→ Advising management on anti-corruption requirements

- Monitoring compliance with policies and controls
- Assessing bribery, fraud and third-party risks
- Managing declarations and reporting channels
- Supporting staff training and awareness
- Escalating suspected violations

Internal audit provides independent assurance on whether governance, risk management and internal controls are properly designed and operating effectively.

Its responsibilities may include:

- Testing high-risk transactions and controls
- Reviewing management overrides and exceptions
- Examining the reliability of records and reports
- Identifying control weaknesses
- Following up on corrective actions
- Reporting significant findings to the board or audit committee

Although their roles are connected, they are not identical:

- Compliance helps management operate within required standards.
- Internal audit independently evaluates whether the entire system is working.

Independence requires:

- Direct access to the board or audit committee
- Authority to obtain relevant records and explanations
- Protection from retaliation or improper dismissal
- Freedom to determine the scope of reviews
- Adequate staffing, funding and professional competence
- Permission to report serious concerns without management filtering
- No responsibility for auditing controls they personally designed or operated

Warning signs of compromised independence include:

- Management removing serious findings from reports
- Auditors requiring permission from the department being reviewed
- Compliance officers being punished for escalating concerns
- Senior executives blocking access to records

→ Audit recommendations repeatedly ignored without explanation

Independence does not mean isolation. Compliance, internal audit, legal, risk management and leadership should cooperate, but their responsibilities and reporting lines must remain clear.

The key principle is simple: **compliance must be able to advise and challenge management, while internal audit must be able to examine the organisation independently and report the truth without fear.**



DEVELOPING AN ANTI-CORRUPTION GOVERNANCE FRAMEWORK

An anti-corruption policy on its own is not a complete governance framework. A policy states the organisation's position, but a framework explains how that position will be implemented, supervised, tested and improved.

An **anti-corruption governance framework** is the coordinated system of leadership responsibilities, policies, controls, reporting arrangements and oversight mechanisms used to prevent and respond to corruption.

A strong framework should include:

- **Leadership commitment:** The board and senior management must communicate and demonstrate zero tolerance for corruption.
- **Governance responsibilities:** The roles of the board, management, compliance, risk, internal audit, legal and employees must be clearly defined.
- **Risk assessment:** Corruption risks must be identified, rated, recorded and reviewed regularly.

- **Policies and procedures:** Clear rules must cover bribery, gifts, conflicts of interest, procurement, donations, third parties and financial transactions.
- **Internal controls:** Preventive and detective measures must address specific high-risk activities.
- **Third-party management:** Suppliers, agents, consultants and partners must undergo proportionate due diligence and monitoring.
- **Training and communication:** Employees and relevant third parties must understand their responsibilities.
- **Reporting mechanisms:** Confidential and accessible channels must allow concerns to be reported safely.
- **Investigation procedures:** Allegations must be assessed and investigated fairly, independently and promptly.
- **Enforcement:** Misconduct must result in consistent and proportionate consequences.
- **Monitoring and review:** The organisation must test controls, track indicators and improve identified weaknesses.

When developing the framework, the organisation should consider:

- Its size, structure and available resources
- The countries and industries in which it operates
- The value and complexity of its transactions
- Its use of agents, contractors and public officials
- Previous incidents, complaints and audit findings
- Relevant legal and regulatory requirements

The framework should also define how serious matters reach senior leadership or the board. A reporting system that stops at the manager involved cannot provide meaningful protection.

Responsibilities, deadlines and evidence requirements must be documented. Saying “management will monitor compliance” is not enough.

The central principle is clear: **an effective anti-corruption framework connects leadership commitment with risk assessment, practical controls, independent oversight and consistent accountability.**



ANTI-BRIBERY AND CORRUPTION POLICIES

Saying “our organisation does not tolerate corruption” is not enough. Employees and third parties need clear rules explaining what is prohibited, what must be declared and what happens when the rules are broken.

An **Anti-Bribery and Corruption Policy** sets the organisation’s standards for preventing, reporting and responding to bribery and other corrupt conduct.

A strong policy should clearly prohibit:

→ Offering, promising, giving or authorising a bribe

- Requesting, accepting or receiving an improper benefit
- Using an agent or third party to make an improper payment
- Secret commissions and kickbacks
- Facilitation payments, except where immediate personal safety is threatened
- Falsifying records to conceal payments
- Retaliating against someone who reports a genuine concern

The policy should apply to:

- Board members and senior executives
- Permanent and temporary employees
- Contractors and consultants
- Agents and intermediaries
- Suppliers and business partners

Important areas the policy should address include:

- Gifts, hospitality, travel and entertainment
- Conflicts of interest
- Political and charitable contributions
- Sponsorships and community projects
- Procurement and supplier relationships
- Dealings with public officials
- Third-party due diligence
- Record keeping and financial controls
- Reporting and investigation procedures

The policy must also explain:

- Who employees should contact for guidance
- Which transactions require prior approval
- What information must be declared and recorded
- How suspected misconduct should be reported
- How reporters will be protected
- Which disciplinary and legal consequences may apply

The language should be practical and easy to understand. A policy that is too technical, inaccessible or never discussed will not guide behaviour.

Training should use realistic situations employees may face. Third parties should also receive or formally accept the requirements relevant to their work.

Leaders must follow the policy themselves. Frequent exceptions for influential people will destroy its credibility.

The key principle is straightforward: **a strong anti-bribery and corruption policy defines the rules, assigns responsibilities and applies the same standard to everyone.**



DELEGATED AUTHORITY AND DECISION-MAKING CONTROLS

Organisations cannot require the chief executive or board to approve every transaction. Authority must be delegated. The risk begins when people receive power without clear limits, independent review or accountability.

Delegated authority is the formal assignment of decision-making power from a higher authority to another person or position.

A delegation framework should clearly state:

→ Who is authorised to make each type of decision

- The maximum financial or operational limit
- Which supporting documents are required
- Whether additional approval is necessary
- Which decisions cannot be delegated
- How temporary authority will be assigned
- How exceptions and emergency decisions will be handled

Examples of delegated authority include:

- Departmental spending limits
- Contract approval thresholds
- Recruitment and promotion authority
- Supplier-selection responsibilities
- Discount, refund and write-off limits
- Access to confidential records and financial systems

Effective decision-making controls should require:

- Clear and objective decision criteria
- Separation between recommendation and approval
- Disclosure of conflicts of interest
- Documented reasons for significant decisions
- Higher approval for unusual or high-risk transactions
- Independent review of exceptions
- Electronic or written evidence identifying the approver

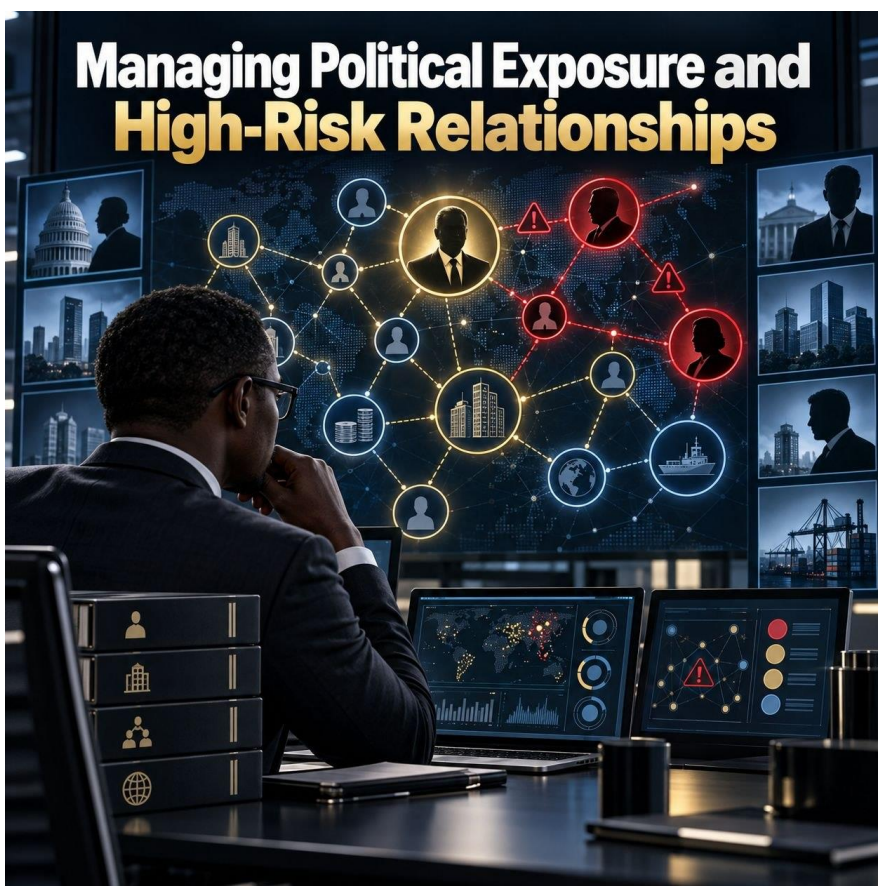
Common warning signs include:

- Transactions divided to remain below approval limits
- Employees approving their own requests or expenses
- Undocumented verbal approvals
- Temporary authority continuing without review
- Approval limits being exceeded or ignored
- Senior officers pressuring employees to bypass procedures
- Repeated emergency decisions without proper justification

Delegating authority does not remove accountability from the person who granted it. Senior leaders must monitor how delegated power is being used and withdraw or revise it when it is abused.

Approvers must also understand that signing a document is not a routine formality. They are confirming that the transaction is necessary, properly supported, lawful and within their authority.

The key principle is simple: **authority may be delegated, but it must remain limited, documented, monitored and accountable.**



MANAGING POLITICAL EXPOSURE AND HIGH-RISK RELATIONSHIPS

A connection to political power does not automatically mean corruption. However, relationships involving public officials, influential political figures or their close associates may create greater opportunities for bribery, favouritism, hidden ownership and misuse of public resources.

A **Politically Exposed Person (PEP)** is someone who holds or has held a prominent public position. This may include senior government officials, high-ranking politicians, senior judicial or military officers and executives of state-owned organisations.

The risk may also extend to:

- Close family members
- Known business partners
- Personal advisers and representatives
- Companies owned or controlled by connected persons
- Individuals acting on behalf of the politically exposed person

High-risk relationships may involve:

- Government contracts and licences
- Public procurement and concessions
- Donations and sponsorships
- Agents who claim access to decision-makers
- Joint ventures with unclear ownership
- Payments involving state-owned organisations
- Recruitment requests from influential officials

Warning signs include:

- Pressure to bypass normal procedures
- Undisclosed ownership or personal relationships
- Unusually high commissions or consultancy fees
- Requests for payment through unrelated accounts
- A third party claiming it can guarantee government approval
- Contracts awarded without competition or documented justification
- Sudden involvement of an intermediary with no clear role

Appropriate controls should include:

- Identifying the person and verifying beneficial ownership
- Understanding the source of funds and source of wealth where necessary
- Establishing the purpose of the relationship
- Conducting enhanced due diligence
- Obtaining senior or independent approval
- Recording conflicts of interest
- Monitoring transactions and changes in ownership
- Reviewing the relationship regularly

A PEP or politically connected person should not be automatically rejected or accused of wrongdoing. The correct response is to understand the increased exposure and apply proportionate controls.

Employees should never accept statements such as “this person is highly connected” as a reason to ignore procedure. Political influence increases the need for transparency; it does not reduce it.

The key principle is simple: **political exposure is not proof of corruption, but it demands stronger due diligence, independent approval and closer monitoring.**

Enhanced Due Diligence for High-Risk Engagements



ENHANCED DUE DILIGENCE FOR HIGH-RISK ENGAGEMENTS

Basic checks may be enough for a routine, low-value supplier. They are not enough when a relationship involves political exposure, hidden ownership, large payments, high-risk locations or an intermediary claiming unusual influence.

Enhanced Due Diligence (EDD) is a deeper level of investigation applied when an engagement presents greater corruption or financial-crime risk.

EDD may be necessary when:

- A politically exposed person is involved
- Ownership is complex or difficult to verify
- The engagement involves public contracts or licences
- Large commissions or advance payments are requested
- An agent will interact with government officials

- The transaction involves a high-risk country or industry
- Payments will pass through unrelated accounts or jurisdictions
- Negative information raises concerns about integrity
- The commercial purpose of the relationship is unclear

Enhanced checks should establish:

- The identities of the ultimate beneficial owners
- The source of funds used in the transaction
- The source of the individual's or company's wealth where relevant
- The genuine business purpose of the engagement
- The third party's qualifications and operational capacity
- Relationships with public officials, employees or decision-makers
- Previous allegations, sanctions, investigations or convictions
- The reason for unusual fees, structures or payment instructions

The organisation should also:

- Obtain approval from appropriately senior and independent officers
- Strengthen anti-corruption clauses in the contract
- Define the third party's services and payment basis clearly
- Require detailed invoices and supporting evidence
- Monitor transactions and performance more frequently
- Set a date for periodic reassessment

EDD is not a box-ticking exercise and should not become an automatic accusation. Its purpose is to understand the risk well enough to make an informed decision.

Possible decisions include:

- Approve the engagement with additional controls
- Request further information before approval
- Restrict the scope or payment method
- Escalate the matter for independent review
- Decline or terminate the relationship

The key principle is straightforward: **the higher the risk, the deeper the checks, the stronger the approval and the closer the monitoring.**

Governance of Donations, Sponsorships and Community Projects



GOVERNANCE OF DONATIONS, SPONSORSHIPS AND COMMUNITY PROJECTS

Donations and community projects may appear charitable, but they can be misused to hide bribes, reward influential people, divert funds or create unfair business advantages. A good purpose does not remove the need for proper controls.

A **donation** is support given without expecting a commercial return. A **sponsorship** provides support in exchange for legitimate publicity or another defined benefit. A **community project** is intended to benefit a particular population or location.

Corruption risks may arise when:

- A public official requests support for a preferred organisation
- A charity is secretly controlled by an employee or decision-maker

- Sponsorship is offered during contract negotiations
- Project costs are inflated and part of the money is diverted
- Beneficiaries cannot be independently verified
- Funds are paid into personal or unrelated accounts
- Donations are used to influence approvals or inspections
- Political contributions are disguised as community support

Before approving support, the organisation should:

- Verify the recipient's identity, registration and beneficial owners
- Confirm the genuine purpose and intended beneficiaries
- Check connections to employees, public officials and third parties
- Review the proposed budget and payment arrangements
- Assess whether the timing could influence a business decision
- Obtain independent approval according to defined limits
- Document the reason for providing the support

Effective controls should include:

- Written applications and selection criteria
- Conflict-of-interest declarations
- Direct payment to verified organisational accounts
- Milestone-based funding for major projects
- Receipts, progress reports and evidence of delivery
- Site visits or independent verification where appropriate
- Prohibition of cash payments without exceptional justification
- Public disclosure of significant donations where required

After approval, the organisation must confirm that the money or resources were used for the stated purpose. Photographs and receipts alone may not be enough if they cannot be independently verified.

Employees must never promise donations or sponsorships to secure a contract, licence, favourable inspection or government decision.

The key principle is clear: **charitable language must never be allowed to hide improper influence, private benefit or diversion of organisational funds.**

Managing Lobbying and Political Contributions



MANAGING LOBBYING AND POLITICAL CONTRIBUTIONS

Organisations may legitimately communicate with government officials or participate in public-policy discussions. The risk begins when lobbying becomes secret influence or political support is used to obtain contracts, licences, protection or favourable treatment.

Lobbying involves attempting to influence public policy, legislation or government decisions through lawful communication and advocacy.

A **political contribution** is money, property, services or other support provided to a political party, candidate or political cause.

Corruption risks may arise when:

- Lobbyists offer benefits to public officials
- Political contributions are linked to business opportunities

- Consultants are hired because of undisclosed government connections
- Donations are routed through employees or third parties
- Payments are disguised as advisory or professional fees
- Company resources are used for political purposes without approval
- Meetings and communications with officials are not documented
- Former public officials are hired mainly for their influence

Effective lobbying controls should require:

- A legitimate and documented purpose
- Prior approval from authorised management
- Due diligence on lobbyists and political consultants
- Clear contracts describing the services to be provided
- Reasonable and transparent fees
- Records of meetings, communications and expenditure
- Compliance with applicable lobbying and disclosure laws

Political-contribution controls should include:

- Clear rules on whether contributions are permitted
- Written approval at the appropriate level
- Verification of recipients and payment accounts
- Prohibition of anonymous, cash or reimbursed personal contributions
- Public disclosure where legally required or organisationally appropriate
- Monitoring to ensure that no favour is expected in return

Warning signs include:

- A consultant guaranteeing access or government approval
- Large success fees linked to public contracts
- Requests to pay an unrelated organisation
- Contributions requested during bidding or licensing decisions
- Pressure to conceal the organisation's involvement
- Employees asked to donate and claim reimbursement later

Even where lobbying or political contributions are lawful, they must remain transparent, properly authorised and separated from commercial decision-making.

The key principle is simple: **political engagement must never become a hidden payment for influence, access or favourable treatment.**

Whistleblowing Systems and Protection Against Retaliation



WHISTLEBLOWING SYSTEMS AND PROTECTION AGAINST RETALIATION

Many serious corruption cases are first detected because someone inside or connected to the organisation speaks up. But employees will remain silent if reporting misconduct could cost them their job, promotion, safety or reputation.

A **whistleblowing system** allows employees and other stakeholders to report suspected misconduct safely, confidentially and without fear of punishment.

Effective reporting channels may include:

- A dedicated telephone hotline
- A secure email address or online portal
- Direct access to compliance or internal audit
- An independent external reporting service
- A confidential channel to the board or audit committee

The system should allow reports from:

- Employees and former employees
- Contractors and consultants
- Suppliers and business partners
- Customers, beneficiaries and members of the public

A strong whistleblowing system should provide:

- Confidential or anonymous reporting where permitted
- Clear instructions on what and how to report
- Access outside the normal management structure
- Prompt acknowledgement and risk assessment
- Independent and competent investigation
- Secure handling of identities and evidence
- Regular updates where appropriate
- Documented outcomes and corrective actions

Retaliation is any harmful action taken because someone reported a genuine concern or participated in an investigation.

It may include:

- Dismissal, suspension or demotion
- Threats, harassment or intimidation
- Unfair transfer or denial of promotion
- Reduced duties, benefits or working hours
- Isolation, humiliation or damage to reputation
- Negative performance ratings without proper justification

Protection against retaliation should include:

- A clear non-retaliation policy
- Restricted access to the reporter's identity
- Monitoring of employment decisions affecting the reporter
- Alternative escalation channels

- Immediate investigation of retaliation complaints
- Disciplinary action against anyone responsible

Whistleblower protection does not mean every allegation is automatically true. Reports must be assessed fairly, and people accused of wrongdoing must receive appropriate procedural protection.

Knowingly false or malicious reports should be addressed carefully, but an honest report should not be punished simply because the allegation could not be proven.

The key principle is clear: **a reporting system is trustworthy only when people can speak up safely, concerns are examined independently and retaliation produces real consequences.**

Anti-Corruption Audits and Compliance Reviews



ANTI-CORRUPTION AUDITS AND COMPLIANCE REVIEWS

Policies, training records and signed declarations may create the appearance of compliance. The real question is whether employees follow the controls and whether those controls can prevent or expose corruption in actual transactions.

An **anti-corruption audit** is an independent examination of governance, transactions, records and controls to determine whether corruption risks are being properly managed.

A **compliance review** checks whether specific activities follow applicable laws, policies, procedures and contractual requirements.

The difference is important:

- **Compliance reviews** usually monitor whether required rules and procedures are being followed.
- **Internal audits** independently assess whether governance, risk management and controls are properly designed and effective.

Areas that may be examined include:

- Procurement and contract awards
- Gifts, hospitality and conflict declarations
- Donations, sponsorships and political contributions
- Third-party due diligence
- Payments, expenses and reimbursements
- Management overrides and emergency approvals
- Whistleblowing and investigation procedures
- Training, disciplinary actions and corrective measures

Audit and review activities may involve:

- Examining a sample of transactions
- Verifying invoices, contracts and approvals
- Reviewing system access and audit logs
- Interviewing employees and control owners
- Comparing supplier prices with market information
- Checking beneficial ownership and related parties
- Testing whether corrective actions were completed

Warning signs may include:

- Missing or altered documents
- Repeated awards to connected suppliers
- Payments without evidence of delivery
- Transactions divided to avoid approval limits
- Management exceptions without proper justification
- Repeated findings that remain unresolved

An audit finding should clearly state:

- What weakness was identified
- Which requirement or control was affected
- What risk or consequence may result

- Who is responsible for corrective action
- When the action must be completed

Audit independence must be protected. Management should not remove serious findings, restrict access to evidence or select only low-risk transactions for review.

The process does not end when the report is issued. Corrective actions must be tracked, verified and escalated when deadlines are missed.

The key principle is straightforward: **an audit identifies and evaluates weaknesses, while effective follow-up ensures those weaknesses are actually corrected.**

Measuring Organisational Integrity and Compliance Performance



MEASURING ORGANISATIONAL INTEGRITY AND COMPLIANCE PERFORMANCE

An organisation cannot prove integrity simply by saying it has zero tolerance for corruption. Leadership needs reliable evidence showing whether employees follow the rules, controls work and reported problems are corrected.

Integrity and compliance performance can be measured using **Key Performance Indicators (KPIs)** and **Key Risk Indicators (KRIs)**.

- **KPIs** show whether compliance activities and responsibilities are being completed effectively.
- **KRIs** warn that corruption exposure or control failure may be increasing.

Useful performance indicators may include:

- Percentage of employees completing required training
- Percentage of conflicts and gifts declared on time
- Completion rate for third-party due diligence
- Number of overdue audit and investigation actions
- Average time taken to assess reported concerns
- Percentage of high-risk controls tested
- Number of substantiated retaliation cases
- Percentage of high-risk suppliers receiving periodic review

Useful risk indicators may include:

- Rising use of non-competitive procurement
- Repeated management overrides
- Transactions divided below approval limits
- Increasing payments without adequate documentation
- Multiple suppliers sharing addresses or bank details
- Recurring audit findings
- Sudden decline in whistleblower reports despite known concerns

Numbers must be interpreted carefully. For example:

- More reports may show greater misconduct, or increased confidence in the reporting system.
- Fewer reports may show improvement, or fear and lack of trust.
- High training completion does not prove that employees understand or apply the lessons.

Measurement should therefore combine:

- Quantitative data such as percentages, totals and completion rates
- Qualitative evidence from interviews, surveys, audits and case reviews
- Outcome measures showing whether behaviour and risk exposure changed

Results should be reported regularly to management and the board. Serious trends, repeated failures and missed deadlines must lead to corrective action.

Avoid **vanity metrics**—figures that look impressive but reveal little. Counting policies, training sessions or signed forms is not enough if misconduct continues and controls remain ineffective.

The key principle is clear: **do not measure only what the organisation has done; measure whether its actions have improved behaviour, strengthened controls and reduced corruption risk.**

Day 1 Review and Key Takeaways



DAY 1 REVIEW AND KEY TAKEAWAYS

Today, we examined a hard truth: corruption is not sustained only by dishonest individuals. It is sustained when leadership fails, authority is uncontrolled, oversight lacks independence and powerful people can bypass procedures without consequences.

The major lessons from Day 1 are:

- Advanced anti-corruption governance controls how authority is exercised, supervised and held accountable.
- Institutional integrity must be built into structures and procedures rather than depending on individual goodwill.
- The board provides independent oversight, while senior leadership implements the anti-corruption programme.

- Tone at the top is established through what leaders practise, reward, ignore and punish.
- Leaders remain accountable for control overrides, ignored warnings and failures to correct known weaknesses.
- Compliance advises, monitors and supports adherence to legal and ethical requirements.
- Internal audit independently evaluates whether governance, risks and controls are being properly managed.
- Compliance and internal audit require authority, resources, unrestricted access and protection from interference.
- An anti-corruption governance framework connects leadership, risk assessment, policies, controls, reporting, investigations and enforcement.
- Anti-bribery policies must clearly define prohibited conduct, responsibilities, reporting procedures and consequences.
- Delegated authority must have documented limits, approval requirements and independent monitoring.
- Management override is a major warning sign, particularly when it bypasses due diligence, competition or board approval.
- Political exposure does not prove corruption, but it requires stronger due diligence, approval and monitoring.
- Third-party governance must establish who owns, controls and ultimately benefits from an organisation.
- Enhanced Due Diligence is required when ownership, political connections, payments or operating conditions create higher risk.
- Donations, sponsorships and community projects must not become hidden channels for influence or private benefit.
- Lobbying and political contributions must remain lawful, transparent, documented and separated from commercial decisions.
- Whistleblowing systems must provide confidentiality, independent investigation and protection against retaliation.
- Anti-corruption audits and compliance reviews test whether rules and controls actually work in practice.
- Integrity performance must be measured through meaningful indicators, not policy counts or training attendance alone.

The practical exercise showed how governance can collapse even when policies, compliance departments and audit functions exist. When leaders suppress reports, interfere with oversight and punish

whistleblowers, the organisation's formal controls become meaningless.

The central lesson from Day 1 is clear: **good governance controls authority, protects independent oversight and ensures that accountability reaches the highest level of the organisation.**

LEVEL 3 DAY 2 — FINANCIAL CRIME PREVENTION AND RESPONSE



DAY 2 — FINANCIAL CRIME PREVENTION AND RESPONSE

Day 1 Recap and Day 2 Overview



DAY 1 RECAP AND DAY 2 OVERVIEW

Welcome back. Yesterday, we examined how leadership, governance and independent oversight determine whether an anti-corruption programme works in practice or exists only on paper.

In Day 1, we established that:

- Institutional integrity must be supported by clear structures and accountability
- Boards provide oversight while senior leadership drives implementation
- Tone at the top is demonstrated through leadership behaviour
- Compliance and internal audit must operate without improper interference

- Delegated authority must have clear limits and monitoring
- High-risk third parties require enhanced due diligence
- Beneficial ownership checks expose the real individuals behind companies
- Political relationships, donations, sponsorships and lobbying require stronger controls
- Whistleblowers must be protected against retaliation
- Audits, reviews and performance indicators must produce corrective action

Day 2 moves from governance into **financial crime prevention and response**.

Financial crime is rarely committed through one obvious transaction. It may involve false documents, hidden ownership, multiple accounts, digital platforms, cooperating insiders and apparently legitimate businesses.

Today, you will learn how to:

- Understand the major forms of financial crime
- Recognise fraud schemes and financial manipulation
- Understand money laundering and its three stages
- Examine terrorist-financing and proliferation-financing risks
- Understand how corruption becomes a predicate offence
- Apply Know Your Customer and Customer Due Diligence controls
- Identify and manage politically exposed persons
- Monitor transactions and recognise suspicious patterns
- Understand suspicious transaction reporting and confidentiality
- Apply sanctions and watchlist-screening controls
- Recognise cyber-enabled fraud and digital financial crime
- Support internal investigations and preserve evidence
- Understand asset tracing, recovery and interagency cooperation

The focus today is not only on identifying missing money. You must understand how illegal funds are generated, moved, disguised and introduced into apparently legitimate systems.

The central question is straightforward: **can your organisation recognise financial crime before it becomes hidden inside normal business activity?**

Understanding Financial Crime



UNDERSTANDING FINANCIAL CRIME

Let us keep this practical: financial crime is not limited to someone stealing cash from an office. It can involve false documents, hidden ownership, manipulated accounts, illegal transfers, digital platforms and legitimate businesses used to conceal criminal activity.

Financial crime refers to illegal conduct committed for financial gain or involving the unlawful use, movement, concealment or control of money and other assets.

Common forms include:

- Fraud
- Bribery and corruption

- Embezzlement
- Money laundering
- Terrorist financing
- Tax evasion
- Insider dealing and market manipulation
- Identity theft
- Cyber-enabled financial crime
- Sanctions evasion

Financial crime may involve:

- Employees abusing their positions
- Senior managers overriding controls
- Customers providing false information
- Suppliers submitting fraudulent invoices
- Criminal groups moving illegal funds
- Professionals helping to conceal transactions
- Companies created to hide ownership or assets

Financial crime usually follows one or more of these patterns:

- Money or assets are obtained illegally
- Legitimate transactions are manipulated for private benefit
- Illegal funds are moved through financial systems
- Ownership or the source of funds is concealed
- Criminal proceeds are made to appear legitimate

The consequences can include:

- Direct financial loss
- Regulatory sanctions and licence restrictions
- Criminal prosecution
- Loss of customers and business partners
- Reputational damage
- Funding of organised crime or terrorism
- Reduced public confidence in institutions

Not every unusual transaction is criminal. However, unexplained activity, false information or attempts to avoid controls must be examined properly.

Employees must understand their responsibility to identify warning signs, follow due-diligence procedures, document concerns and escalate suspicious activity through authorised channels.

The key principle is clear: **financial crime succeeds when illegal activity is allowed to hide inside normal-looking transactions.**

Major Forms of Financial Crime



MAJOR FORMS OF FINANCIAL CRIME

Financial crime does not appear in one form. Different schemes may involve employees, customers, public officials, companies or organised criminal groups. Several offences can also occur within the same transaction.

Major forms of financial crime include:

- **Fraud:** Using deception or false information to obtain money, property or another benefit.
- **Bribery:** Offering, giving, requesting or receiving something valuable to improperly influence a decision.
- **Embezzlement:** Dishonestly taking money or assets entrusted to someone because of their position.

- **Money laundering:** Concealing the criminal origin, ownership or movement of illegally obtained funds.
- **Terrorist financing:** Collecting or providing funds to support terrorist individuals, groups or activities.
- **Tax evasion:** Illegally concealing income, transactions or assets to avoid paying tax.
- **Forgery:** Creating, altering or using false documents to deceive another person or organisation.
- **Identity theft:** Using another person's personal or financial information without authority.
- **Cyber-enabled financial crime:** Using digital systems, communication platforms or malicious software to steal or redirect funds.
- **Insider dealing:** Using confidential information to obtain an unfair financial advantage in securities or investment transactions.
- **Market manipulation:** Creating a false or misleading appearance of market activity, price or demand.
- **Sanctions evasion:** Concealing parties, payments, ownership or shipping routes to avoid legal restrictions.
- **Procurement fraud:** Manipulating bidding, contracting, delivery or payment processes for improper benefit.
- **Accounting manipulation:** Falsifying financial records to hide losses, inflate performance or conceal improper transactions.

These crimes may be connected. For example, an official may receive a bribe, hide the payment through a false consulting contract and later move the money through several companies. This may involve corruption, fraud, false accounting and money laundering.

Warning signs may include:

- Transactions with no clear business purpose
- False or incomplete documents
- Unexplained wealth or lifestyle changes
- Payments through unrelated accounts
- Hidden ownership structures
- Attempts to avoid approval or reporting requirements

The key principle is straightforward: **different financial crimes may use different methods, but they usually depend on**

deception, concealment, abuse of trust or manipulation of legitimate systems.

Fraud Schemes and Financial Manipulation



FRAUD SCHEMES AND FINANCIAL MANIPULATION

Fraud does not always look like outright theft. In many cases, the transaction appears properly approved and documented. The deception is hidden inside false suppliers, altered figures, fabricated services or manipulated records.

A **fraud scheme** is a planned method of deception used to obtain money, assets or another improper benefit.

Common workplace fraud schemes include:

- **False invoicing:** Submitting invoices for goods or services that were never supplied
- **Invoice inflation:** Charging more than the agreed price or actual value
- **Duplicate payments:** Processing the same invoice more than once
- **Ghost employees:** Creating nonexistent workers and diverting their salaries
- **Payroll manipulation:** Altering salaries, allowances or overtime records dishonestly
- **Expense fraud:** Claiming false, personal or exaggerated business expenses
- **Procurement fraud:** Manipulating bids, suppliers, prices or delivery records
- **Asset misappropriation:** Stealing or improperly using cash, stock, equipment or property
- **Revenue diversion:** Redirecting customer payments before they reach organisational accounts
- **Refund fraud:** Creating false refunds and sending the money to connected accounts
- **Financial-statement fraud:** Altering records to hide losses, inflate profits or mislead stakeholders

Financial manipulation may involve:

- Backdating or altering documents
- Recording expenses as assets
- Hiding liabilities or losses
- Creating fictitious sales or customers
- Moving transactions between reporting periods
- Splitting payments to avoid approval limits
- Using complex entries to conceal unauthorised transfers

Warning signs include:

- Missing original documents
- Unexplained changes to supplier bank details
- Payments made before delivery
- Repeated round-number invoices
- Employees refusing to share duties or take leave

- Manual adjustments made near reporting deadlines
- Revenue or profit growth unsupported by cash flow
- Suppliers sharing employee contact details

Preventing fraud requires:

- Segregation of duties
- Independent approval and verification
- Restricted system access
- Regular account reconciliation
- Transaction and exception monitoring
- Supplier and employee data analysis
- Protected reporting channels
- Prompt investigation of irregularities

One red flag does not automatically prove fraud. It means the transaction requires closer examination.

The key principle is simple: **fraud succeeds when deception appears normal, records are trusted without verification and warning signs are ignored.**

Understanding Money Laundering



UNDERSTANDING MONEY LAUNDERING

Criminals cannot safely enjoy illegal money while its true source remains obvious. They therefore try to separate the funds from the crime and create an explanation that makes the money appear legitimate.

Money laundering is the process of concealing or disguising the criminal origin, ownership, location or movement of money and other assets.

The illegal funds may come from:

- Bribery and corruption
- Fraud and embezzlement

- Drug trafficking
- Human trafficking
- Kidnapping and extortion
- Cybercrime and identity theft
- Smuggling and illegal trade
- Tax crimes
- Environmental and organised crime

Money laundering may involve:

- Depositing illegal cash into financial accounts
- Dividing large amounts into smaller transactions
- Moving funds through several accounts or countries
- Using false invoices, loans or consulting contracts
- Purchasing property, vehicles, jewellery or businesses
- Using relatives, agents or shell companies to hide ownership
- Mixing criminal proceeds with legitimate business income
- Converting funds into digital assets or other financial products

Money laundering does not always involve physical cash. It may involve property, company shares, cryptocurrency, valuable goods or any asset representing criminal proceeds.

An employee or organisation can become involved by:

- Knowingly helping to conceal illegal funds
- Ignoring obvious warning signs
- Accepting false customer information
- Failing to conduct required due diligence
- Allowing transactions designed to avoid controls

Possible warning signs include:

- Transactions inconsistent with a customer's known activities
- Complex movements with no clear business purpose
- Unexplained payments involving unrelated third parties
- Secretive or unnecessarily complicated ownership structures
- Large cash activity without a reasonable explanation
- Customers resisting identification or source-of-funds checks

Not every unusual transaction is money laundering. It becomes suspicious when the activity lacks a reasonable explanation, conflicts with known information or appears designed to avoid scrutiny.

The key principle is clear: **money laundering attempts to make criminal proceeds look legitimate by hiding where they came from, who controls them or why they are being moved.**

The Three Stages of Money Laundering



THE THREE STAGES OF MONEY LAUNDERING

Money laundering is commonly explained through three stages: **placement, layering and integration**. In real cases, these stages may overlap, happen in a different order or not all appear clearly. However, the model helps you understand how criminal funds are introduced, concealed and eventually used.

1. PLACEMENT

Placement is the introduction of criminal proceeds into the financial or commercial system.

Examples include:

- Depositing illegal cash into bank accounts
- Dividing large cash amounts into smaller deposits
- Purchasing money orders, digital assets or valuable goods
- Mixing criminal cash with the income of a legitimate business
- Using another person to make deposits

This stage can be risky for criminals because the money may still be closely connected to the original crime.

2. LAYERING

Layering involves moving or restructuring the funds to make their origin and ownership difficult to trace.

Examples include:

- Transferring money through several accounts
- Moving funds between companies or countries
- Using shell companies and hidden beneficial owners
- Creating false loans, invoices or consultancy agreements
- Buying and selling assets repeatedly
- Converting funds between currencies or digital assets

The purpose is to create complexity, break the audit trail and distance the assets from the original offence.

3. INTEGRATION

Integration occurs when the funds return to the economy with an apparently legitimate explanation.

Examples include:

- Purchasing property or businesses
- Receiving money as false investment returns
- Claiming repayment of a fabricated loan
- Declaring illegal funds as business income
- Buying luxury assets through apparently legitimate companies

At this stage, the criminal may use the assets openly because they appear to come from a lawful source.

Consider this example:

- A corrupt official deposits bribe money through several small cash transactions — **placement**
- The funds are moved through connected companies using false invoices — **layering**
- The money is used to purchase property through a legitimate-looking business — **integration**

Organisations must monitor the full transaction pattern. Examining one payment in isolation may hide the wider movement of funds.

The key principle is simple: **placement introduces the criminal proceeds, layering conceals their origin and integration makes them appear legitimate.**

Terrorist Financing and Proliferation-Financing Risks



TERRORIST FINANCING AND PROLIFERATION-FINANCING RISKS

These two crimes may use the same financial channels as money laundering, but their purposes are different. You must understand the distinction because suspicious funds are not always proceeds of an earlier crime.

Terrorist financing involves collecting, providing, moving or using money or other assets to support terrorists, terrorist organisations or terrorist activities.

The funds may come from:

→ Criminal activities such as fraud, kidnapping, smuggling or extortion

- Apparently legitimate businesses or employment income
- Donations, charities or fundraising campaigns
- Cash couriers and informal transfer systems
- Digital assets and online payment platforms
- Support provided through goods, travel or accommodation

Unlike traditional money laundering, terrorist financing may involve legally obtained money used for an illegal purpose. The transaction amount may also be small and appear routine.

Proliferation financing involves providing funds or financial services connected to the development, acquisition, movement or supply of nuclear, chemical or biological weapons and related materials or technology.

It commonly involves attempts to:

- Evade targeted financial sanctions
- Hide the real buyer, seller or beneficiary
- Use intermediaries, front companies or shell companies
- Misrepresent controlled goods or their final destination
- Route payments through several countries or unrelated businesses
- Exploit shipping, trade-finance or digital-payment systems

Warning signs may include:

- Transactions involving sanctioned persons or entities
- Customers connected to high-risk goods or jurisdictions
- Complex ownership with no reasonable commercial explanation
- Goods inconsistent with the customer's normal business
- Unusual shipping routes or destination changes
- Payments made by unrelated third parties
- Vague descriptions on trade and shipping documents
- Attempts to remove identifying information from transactions

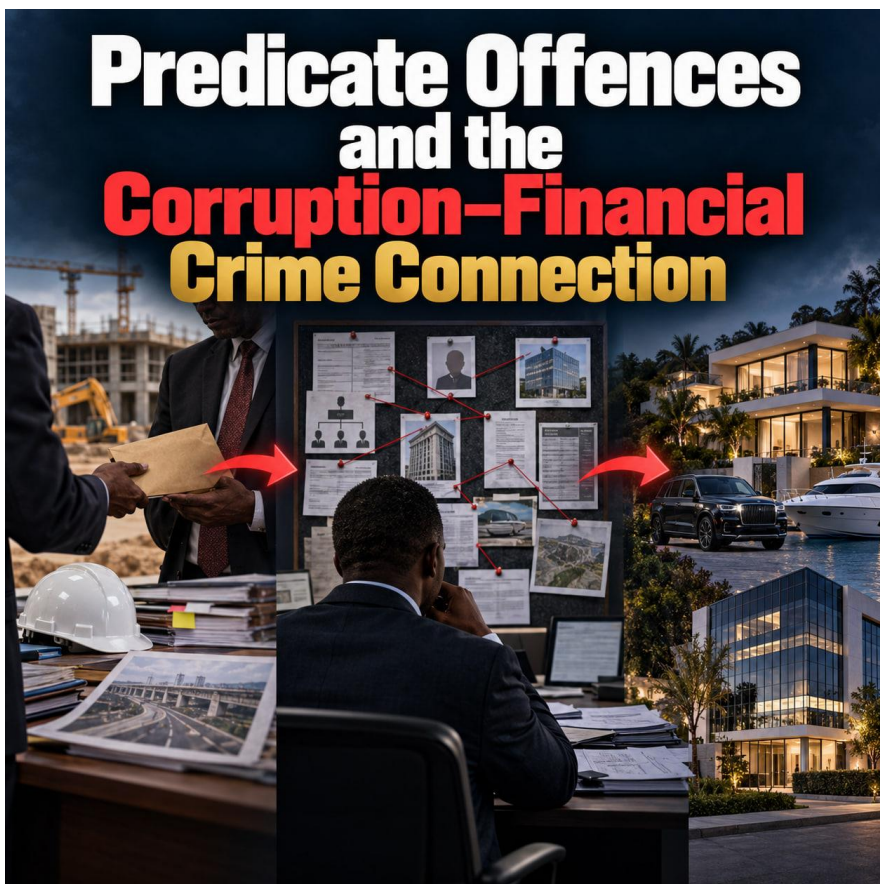
Appropriate controls include:

- Customer and beneficial-ownership verification
- Sanctions and watchlist screening
- Enhanced Due Diligence for high-risk relationships
- Transaction and trade-document monitoring

- Immediate escalation of suspicious activity
- Freezing or rejecting transactions where legally required

Employees should not confront the customer or reveal that a report or investigation may be underway.

The key distinction is clear: **money laundering conceals criminal proceeds, terrorist financing supports terrorist purposes and proliferation financing supports prohibited weapons activity or evades related sanctions.**



PREDICATE OFFENCES AND THE CORRUPTION-FINANCIAL CRIME CONNECTION

Money laundering does not begin with the laundering transaction. It begins with an earlier crime that produces money, property or another financial benefit. That earlier crime is called a **predicate offence**.

A **predicate offence** is the underlying criminal activity from which proceeds are generated and later concealed, transferred or made to appear legitimate.

Common predicate offences include:

- Bribery and corruption
- Fraud and embezzlement
- Drug trafficking
- Human trafficking
- Kidnapping and extortion
- Smuggling
- Tax crimes
- Cybercrime
- Environmental crime
- Organised theft

Corruption and financial crime are closely connected because corrupt conduct often generates proceeds that offenders must hide or spend without revealing their origin.

For example:

- A public official receives a bribe — **corruption**
- The payment is described as a consultancy fee — **false accounting**
- The money is transferred through connected companies — **layering**
- Property is purchased in another person's name — **money laundering and concealed beneficial ownership**

Corruption may also help other financial crimes succeed. An offender may bribe:

- A bank employee to ignore suspicious transactions
- A customs officer to allow illegal goods through a border
- An inspector to conceal regulatory violations
- A procurement officer to approve false invoices
- An investigator to suppress evidence

This means corruption can operate in two ways:

- As the original offence that generates illegal proceeds
- As a method used to protect, conceal or continue another crime

Investigators and compliance officers should therefore avoid examining offences in isolation. A bribery allegation may lead to false contracts, hidden assets, tax violations and money laundering.

When suspicious wealth or transactions are identified, important questions include:

- What activity generated the funds?
- Who ultimately owns or controls the assets?
- Which documents were used to disguise the source?
- Who helped move, conceal or legitimise the proceeds?

The key principle is clear: **to understand money laundering, follow the funds backwards to the crime that generated them and forwards to the people, assets and systems used to conceal them.**

Customer Identification and Know Your Customer Requirements



CUSTOMER IDENTIFICATION AND KNOW YOUR CUSTOMER REQUIREMENTS

An organisation should not provide financial or high-risk services to someone it cannot properly identify. A name, telephone number or photocopied document is not enough if the information has not been independently verified.

Know Your Customer (KYC) refers to the procedures used to establish who a customer is, understand their activities and assess the risk they may present.

Customer identification begins by collecting information such as:

→ Full legal name

- Date of birth or incorporation
- Residential or registered address
- Nationality or country of registration
- Occupation, business activities or source of income
- Official identification or company-registration details
- Contact information
- Tax or other legally required identification numbers

Identification means obtaining the customer's information.

Verification means confirming that information using reliable and independent documents, data or sources.

For companies and other legal arrangements, the organisation should identify:

- The legal entity and its registration status
- Directors, trustees or authorised representatives
- Ownership and control structure
- Ultimate beneficial owners
- Persons authorised to operate the account or relationship
- The purpose of the business relationship

KYC should also establish:

- Why the customer requires the service
- The expected nature and volume of transactions
- The anticipated source of funds
- Countries, products and payment channels involved
- Whether political exposure or sanctions risk exists

KYC is not completed only when the relationship begins. Customer information must be updated, and transactions should be monitored to confirm that they remain consistent with the known profile.

Additional checks may be required when:

- Information is inconsistent or difficult to verify
- Ownership is unnecessarily complex
- A politically exposed person is involved
- Transactions involve high-risk locations or activities
- Money comes from unexplained third parties

→ Previous customer information becomes doubtful

If the organisation cannot complete the required verification, it should not simply ignore the missing information. The relationship or transaction may need to be declined, restricted, terminated or escalated according to applicable law and organisational procedure.

The key principle is straightforward: **know who the customer is, who ultimately controls the relationship, why they require the service and whether their transactions make sense.**

Customer Due Diligence and Enhanced Due Diligence



CUSTOMER DUE DILIGENCE AND ENHANCED DUE DILIGENCE

Knowing a customer's name is only the starting point. An organisation must also understand who controls the relationship, where the money comes from and whether the customer's transactions are consistent with their known activities.

Customer Due Diligence (CDD) is the process of identifying, verifying, assessing and continuously monitoring a customer.

Standard CDD should include:

→ Identifying and verifying the customer

- Identifying and verifying the beneficial owner
- Understanding the ownership and control structure
- Establishing the purpose of the relationship
- Understanding expected transaction activity
- Assessing the source of funds where appropriate
- Screening for sanctions and political exposure
- Assigning a customer-risk rating
- Monitoring transactions throughout the relationship
- Keeping customer information accurate and current

Enhanced Due Diligence (EDD) involves deeper checks and stronger monitoring where the customer, transaction or relationship presents higher risk.

EDD may be required when:

- A politically exposed person is involved
- Ownership is complex or difficult to verify
- Transactions involve high-risk countries or industries
- The customer handles large amounts of cash
- Funds come from unexplained third parties
- Activity is inconsistent with the customer's profile
- Sanctions, criminal allegations or serious negative information exist
- The source of wealth or funds is unclear

Enhanced measures may include:

- Obtaining additional identification and ownership information
- Verifying source of funds and source of wealth
- Understanding the reason for complex transactions
- Obtaining senior-management approval
- Conducting more frequent customer reviews
- Applying closer transaction monitoring
- Requesting supporting contracts, invoices or tax records
- Independently verifying business activities

The difference is straightforward:

- **CDD** establishes and monitors the normal customer relationship.

→ **EDD** applies deeper investigation and stronger controls when risk is higher.

Due diligence must continue after onboarding. A low-risk customer can become high-risk if ownership, behaviour, transaction patterns or political exposure changes.

The organisation should not reduce controls merely to avoid losing a profitable customer. Commercial pressure does not cancel financial-crime risk.

The key principle is clear: **every customer requires appropriate due diligence, but higher-risk relationships require deeper checks, stronger approval and closer monitoring.**

Politically Exposed Persons and High-Risk Customers



POLITICALLY EXPOSED PERSONS AND HIGH-RISK CUSTOMERS

A customer should not be labelled corrupt simply because they hold a prominent public position. However, access to public funds, contracts and decision-making authority can create greater exposure to bribery, embezzlement and money laundering.

A **Politically Exposed Person (PEP)** is someone who holds or has held a prominent public function.

This may include:

→ Senior government and political officials

- High-ranking judicial or military officers
- Senior executives of state-owned organisations
- Senior officials of major political parties
- Individuals entrusted with prominent international functions

The risk may also extend to:

- Close family members
- Known close associates
- Business partners
- Companies or arrangements controlled by connected persons

Other customers may be classified as high-risk because of:

- Complex or hidden ownership structures
- Large or unexplained cash transactions
- Operations in high-risk industries or locations
- Unclear sources of funds or wealth
- Unusual use of intermediaries or third parties
- Serious negative information or criminal allegations
- Transactions inconsistent with their known business
- Connections to sanctioned persons or entities

Appropriate controls for PEPs and other high-risk customers may include:

- Establishing the person's role and level of influence
- Identifying and verifying beneficial owners
- Determining the source of funds and source of wealth
- Obtaining appropriately senior approval
- Conducting Enhanced Due Diligence
- Applying closer transaction monitoring
- Reviewing the relationship more frequently
- Examining unexplained third-party payments
- Documenting the reasons for accepting or continuing the relationship

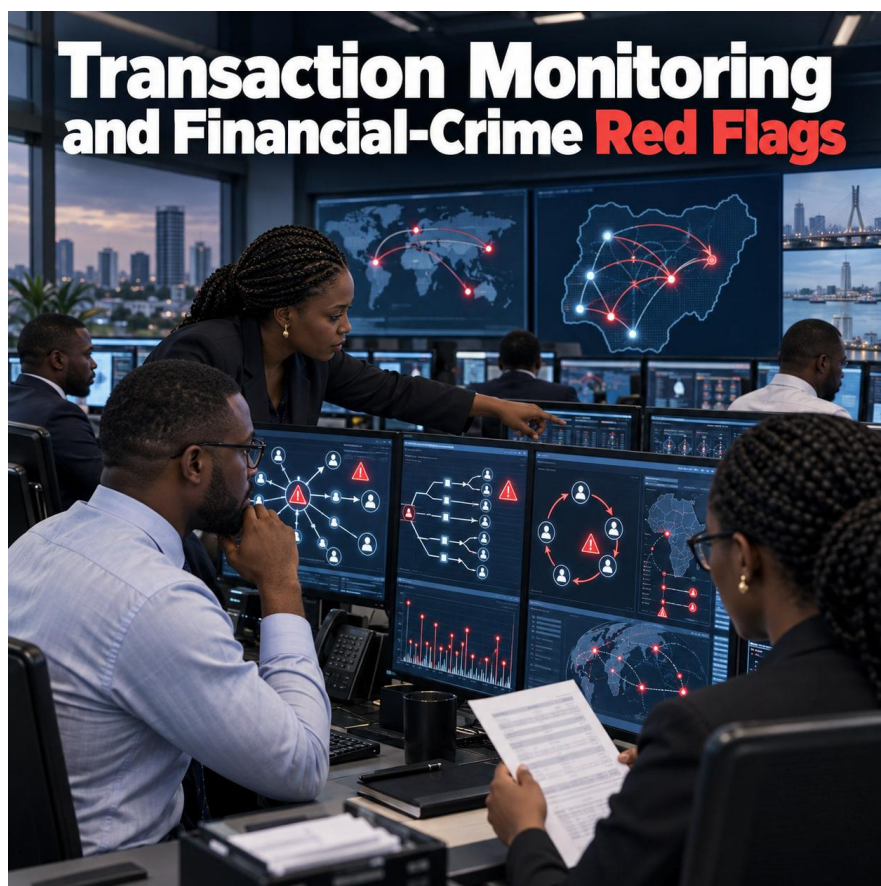
A customer's high-risk status is not proof of wrongdoing, and it should not automatically result in rejection. The purpose is to understand the increased exposure and apply proportionate controls.

Former public officials may still present elevated risk after leaving office, particularly where they retain influence, relationships or

unexplained wealth. Their status should therefore be reviewed according to continuing risk rather than removed automatically.

Employees should not ignore warning signs because the customer is wealthy, influential or commercially valuable. High status does not reduce the need for scrutiny.

The key principle is straightforward: **political exposure and high-risk status require deeper understanding, stronger approval and continuous monitoring—not automatic accusation or special exemption.**



TRANSACTION MONITORING AND FINANCIAL-CRIME RED FLAGS

A customer may provide convincing documents during onboarding and still use the relationship improperly later. That is why due diligence must continue after the account, contract or business relationship has been approved.

Transaction monitoring is the ongoing review of financial activity to determine whether transactions are consistent with the customer's identity, business, risk profile and expected behaviour.

Monitoring may be:

- **Manual:** Employees review transactions, documents and customer explanations.
- **Automated:** Systems generate alerts when activity meets predefined risk rules.
- **Event-driven:** A review begins because ownership, behaviour or risk circumstances have changed.

Common financial-crime red flags include:

- Transactions inconsistent with the customer's known business
- Sudden activity in a previously inactive account
- Repeated transfers just below reporting or approval thresholds
- Large payments involving unrelated third parties
- Rapid movement of funds through several accounts
- Payments to or from high-risk locations without clear justification
- Multiple customers using the same address, contact details or device
- Frequent changes to beneficiary or supplier bank accounts
- Complex transactions with no reasonable commercial purpose
- Funds received and immediately transferred elsewhere
- Large cash deposits inconsistent with expected activity
- False, altered or inconsistent supporting documents
- Customers resisting questions about ownership or source of funds
- Transaction descriptions that do not match the underlying activity

A red flag does not automatically prove a crime. It indicates that the transaction requires closer examination.

When an alert is generated, the reviewer should:

- Examine the customer's profile and transaction history
- Compare the activity with expected behaviour
- Review contracts, invoices and supporting documents
- Identify counterparties and beneficial owners
- Record the reason for concern
- Seek an appropriate explanation where permitted
- Escalate unresolved suspicion through authorised channels

Monitoring rules must be reviewed regularly. Poorly designed systems may generate excessive alerts, while weak thresholds may fail to detect serious activity.

Employees must not close alerts simply because the customer is profitable, influential or familiar.

The key principle is clear: **do not examine transactions only as individual payments—look for patterns, relationships and activity that do not make reasonable business sense.**



SUSPICIOUS TRANSACTION REPORTING AND CONFIDENTIALITY

When a transaction raises serious and unresolved concerns, employees should not ignore it, confront the customer or attempt to prove the crime themselves. Their responsibility is to document the facts and escalate the matter through the approved reporting process.

A **Suspicious Transaction Report (STR)** is a formal report submitted to the appropriate authority when there are reasonable grounds to suspect that funds or transactions may be connected to money laundering, terrorist financing, fraud or another financial crime.

Suspicion may arise when:

- Activity is inconsistent with the customer's known profile
- Ownership or source of funds cannot be explained
- False or altered documents are presented
- Transactions appear designed to avoid reporting thresholds
- Funds move rapidly through unrelated accounts
- A customer refuses to provide required information
- Payments involve sanctioned or high-risk parties
- Several red flags appear without a reasonable explanation

Employees should initially report concerns to the designated internal authority, such as:

- The Money Laundering Reporting Officer
- The compliance function
- Another officer authorised under the organisation's procedure

The report should contain:

- Customer and account details
- Relevant dates, amounts and transactions
- Parties and accounts involved
- Warning signs that created the suspicion
- Supporting records and documents
- The employee's factual reasons for concern

An STR should describe facts clearly. It should not contain exaggeration, insults or unsupported accusations. Proof of the underlying crime is generally not required before a genuine suspicion is escalated.

Confidentiality is essential.

Employees must not:

- Tell the customer that a report has been or may be submitted
- Discuss the matter with unauthorised colleagues
- Warn any person involved in the transaction
- Alter, remove or circulate supporting records
- Post details publicly or on social media

Improperly revealing the report may alert suspects, lead to evidence destruction and compromise an investigation. This is commonly known as **tipping off**.

The authorised officer should evaluate the internal report, determine whether an external report is legally required and ensure relevant records are preserved.

Requirements concerning reporting deadlines, transaction restrictions and external authorities vary by jurisdiction. Employees must follow applicable law and organisational procedure.

The key principle is straightforward: **document the facts, report genuine suspicion promptly and protect the confidentiality of the process.**



SANCTIONS SCREENING AND WATCHLIST CONTROLS

A transaction may appear commercially legitimate and still involve a person, company, vessel, country or organisation subject to legal restrictions. That is why screening must take place before funds, goods or services are provided.

Sanctions are legal restrictions imposed by authorised national or international bodies to address threats such as terrorism, weapons proliferation, serious crime or international-security violations.

Watchlists contain names or information relating to persons and entities requiring restriction, prohibition or additional scrutiny.

Screening may cover:

- Customers and beneficial owners
- Directors and authorised representatives
- Suppliers, agents and business partners
- Payment senders and beneficiaries
- Banks and financial institutions
- Vessels, aircraft and shipping companies
- Countries, locations and transaction routes

Effective screening should occur:

- Before beginning a customer or third-party relationship
- Before processing relevant transactions
- When ownership or authorised persons change
- When official sanctions lists are updated
- During periodic customer and supplier reviews

Screening systems should consider:

- Alternative spellings and aliases
- Previous names
- Dates of birth or incorporation
- Nationality and addresses
- Identification and registration numbers
- Beneficial ownership and control relationships

A possible match is not automatically a confirmed match. The organisation should compare additional identifying information before deciding.

Possible results include:

- **False positive:** The name appears similar, but the person or entity is not the listed party.
- **Potential match:** Additional information is required.
- **Confirmed match:** The identifying information supports the conclusion that the party is sanctioned or restricted.

Employees must not ignore an alert because the customer is influential, the transaction is urgent or the name is common.

When a potential match appears, the organisation should:

- Pause processing where required
- Escalate the alert to authorised personnel
- Verify the party using reliable information
- Document the review and decision
- Freeze, reject or report the transaction where legally required
- Maintain strict confidentiality

Sanctions lists and legal obligations change. Screening data, procedures and system rules must therefore be updated regularly.

The key principle is clear: **screen the parties, ownership, transaction and destination before allowing organisational resources to reach a prohibited or high-risk recipient.**



CYBER-ENABLED FRAUD AND DIGITAL FINANCIAL CRIME

Technology has made financial transactions faster, but it has also made fraud easier to scale, disguise and carry out across borders. A criminal no longer needs physical access to an office or bank account to steal money.

Cyber-enabled fraud is traditional fraud committed or expanded through digital technology.

Cyber-dependent crime exists because of technology and directly targets computers, networks or data.

Common examples include:

- Phishing emails and fake websites
- Business Email Compromise
- Identity theft and account impersonation
- Mobile banking and payment fraud
- SIM-swap attacks
- Ransomware and malicious software
- Unauthorised system access
- Online investment and cryptocurrency scams
- Invoice and supplier-payment diversion
- Theft of customer or employee information

A common workplace example is **Business Email Compromise**. A criminal gains access to or imitates a senior officer's email account and instructs finance staff to make an urgent payment to a different bank account.

Warning signs include:

- Unexpected changes to payment instructions
- Urgent requests demanding secrecy
- Slight differences in email addresses or domain names
- Requests to bypass normal approval procedures
- Login attempts from unusual devices or locations
- Multiple password-reset requests
- New beneficiaries receiving large payments immediately
- Customers or suppliers denying transactions recorded in their names

Controls should include:

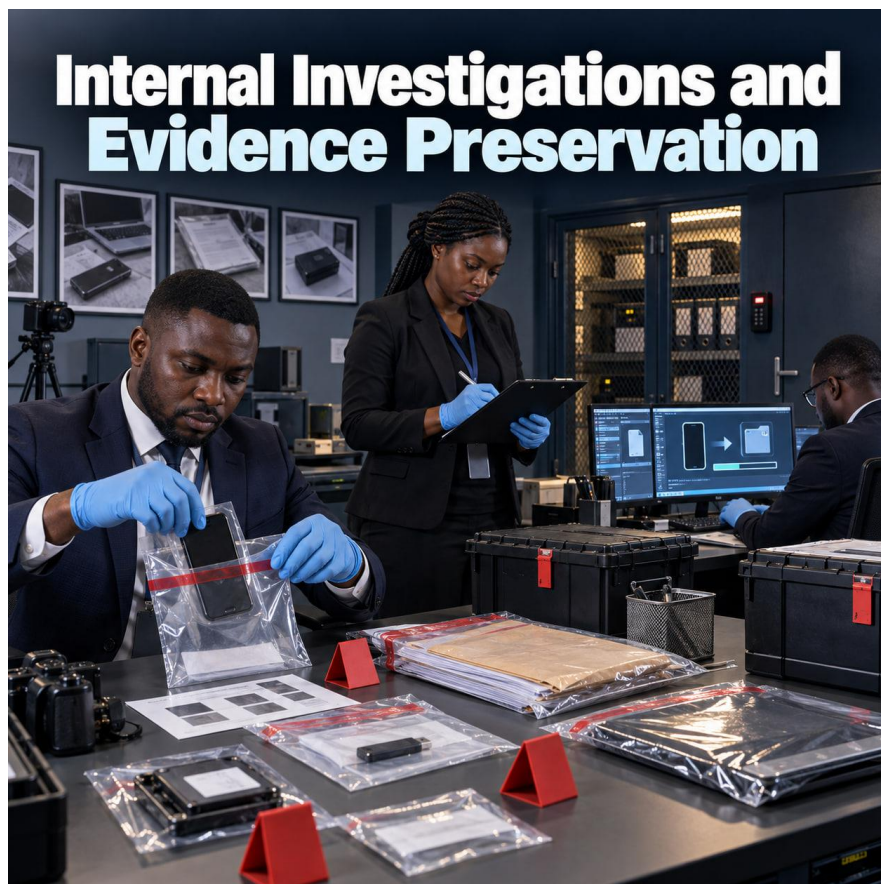
- Multi-factor authentication
- Strong, unique passwords
- Role-based access restrictions
- Independent confirmation of payment-detail changes
- Dual authorisation for sensitive transactions
- Regular software updates and security testing
- Monitoring of login and transaction activity
- Staff training on phishing and impersonation
- Secure backups and incident-response procedures

If suspicious digital activity is detected:

- Stop or restrict the transaction where authorised
- Contact the bank or payment provider immediately
- Preserve emails, logs, messages and device records
- Report the incident through approved channels
- Change compromised credentials
- Avoid deleting, forwarding or altering possible evidence

Artificial intelligence can also be used to create convincing messages, cloned voices, false documents and manipulated videos. Familiar voices and professional-looking messages must still be independently verified.

The key principle is clear: **never allow urgency, familiarity or digital appearance to replace proper verification and approval.**



Internal Investigations and Evidence Preservation

INTERNAL INVESTIGATIONS AND EVIDENCE PRESERVATION

When financial crime is suspected, acting quickly matters—but acting carelessly can destroy the case. An organisation must establish the facts without alerting suspects, contaminating evidence or denying anyone a fair process.

An **internal investigation** is a formally authorised examination of suspected misconduct within or connected to an organisation.

Its objectives are to determine:

→ What happened

- When and how it happened
- Who was involved
- Which funds, accounts or assets were affected
- Which laws, policies or controls may have been breached
- Whether other people or transactions are connected
- Which control failures allowed the incident

The investigation should be:

- Independent and free from interference
- Conducted by competent and authorised personnel
- Based on facts rather than assumptions
- Confidential and limited to those who need to know
- Fair to the reporter, witnesses and accused persons
- Properly documented from beginning to end

Possible evidence may include:

- Bank statements and transaction records
- Invoices, contracts and payment approvals
- Emails, messages and call records
- Accounting entries and system logs
- Customer and supplier due-diligence files
- CCTV recordings and access records
- Computers, mobile devices and storage media
- Interview notes and witness statements

Evidence preservation requires the organisation to:

- Stop routine deletion of relevant electronic records
- Secure original documents and devices
- Create protected working copies where appropriate
- Record who collected, accessed or transferred each item
- Restrict access to authorised personnel
- Preserve metadata and system timestamps
- Store physical and digital evidence securely

The documented record showing how evidence was collected, handled and stored is called the **chain of custody**. If this record is weak, the reliability of the evidence may be challenged.

Investigators must not alter original records, coach witnesses or make conclusions before examining the evidence. Employees must also avoid confronting suspects or circulating allegations.

Where criminal conduct may have occurred, legal advisers and relevant authorities may need to be involved according to applicable law.

The key principle is clear: **investigate independently, preserve the original evidence and document every important action taken.**



ASSET TRACING, RECOVERY AND INTERAGENCY COOPERATION

Finding out that money was stolen is not the end of the matter. The organisation must determine where the proceeds went, who controls them and whether they can be lawfully recovered.

Asset tracing is the process of identifying and following money, property and other benefits connected to corruption or financial crime.

Assets may include:

- Money held in bank or digital-payment accounts
- Land, buildings and other property

- Vehicles, equipment and valuable goods
- Company shares and business interests
- Investments, securities and insurance products
- Digital assets and cryptocurrency
- Assets registered in another person's name

Investigators may examine:

- Bank statements and payment records
- Company and beneficial-ownership information
- Property and vehicle records
- Contracts, invoices and accounting entries
- Tax and customs information
- Digital wallets and transaction histories
- Connections between suspects, relatives and associates

Asset recovery is the lawful process of freezing, seizing, confiscating and returning proceeds of crime or property of equivalent value.

The recovery process may involve:

- Identifying and valuing suspected assets
- Preserving evidence linking assets to the offence
- Preventing transfer, sale or concealment
- Obtaining appropriate court or regulatory orders
- Confiscating assets through lawful proceedings
- Returning recovered assets to the rightful owner or public authority

Organisations should not seize property or freeze accounts without proper legal authority. Suspicion alone does not remove a person's legal rights.

Financial crime often crosses organisational and national boundaries.

Interagency cooperation may therefore involve:

- Law-enforcement agencies
- Anti-corruption bodies
- Financial-intelligence units
- Tax and customs authorities
- Financial regulators
- Prosecutors and courts

→ Foreign authorities and international partners

Effective cooperation requires:

→ Timely and lawful information sharing

→ Clear responsibilities and points of contact

→ Secure handling of confidential information

→ Coordinated investigative and recovery strategies

→ Proper preservation of evidence

→ Respect for due process and data-protection requirements

A delayed or uncoordinated response may allow assets to be transferred, converted, hidden behind companies or moved to another jurisdiction.

The key principle is clear: **follow the money, identify who truly controls the assets, preserve the evidence and use lawful cooperation to recover what was taken.**



LEVEL 3 REVIEW, KEY TAKEAWAYS AND CLOSING REMARKS

We have reached the end of **Advanced Anti-Corruption Governance and Financial Crime Prevention — Level 3**.

At this level, we moved beyond individual misconduct and basic controls. We examined how leadership, governance, financial systems, third parties and organised criminal activities can expose an entire institution.

The major lessons from Level 3 are:

- Corruption survives when leadership fails, oversight is weak and powerful individuals can override controls without consequences.

- Institutional integrity must be supported by clear governance structures rather than individual goodwill.
- Boards provide independent oversight, while senior leadership is responsible for implementation and accountability.
- Tone at the top is demonstrated through what leaders practise, reward, tolerate and punish.
- Compliance and internal audit must have sufficient authority, resources, independence and access to information.
- An effective anti-corruption framework connects leadership, risk assessment, policies, controls, reporting, investigations and enforcement.
- Anti-bribery policies must clearly define prohibited conduct, responsibilities, approval requirements and consequences.
- Delegated authority must remain limited, documented, monitored and accountable.
- Political exposure does not prove corruption, but it requires stronger due diligence and closer monitoring.
- Third-party governance must identify the real individuals who own, control or benefit from an organisation.
- High-risk engagements require Enhanced Due Diligence, senior approval and continuous review.
- Donations, sponsorships, lobbying and political contributions must not become hidden channels for improper influence.
- Whistleblowing systems must protect confidentiality and prevent retaliation.
- Audits and compliance reviews must test whether controls actually work—not merely confirm that policies exist.
- Financial crime includes fraud, bribery, embezzlement, money laundering, terrorist financing, cybercrime and sanctions evasion.
- Fraud often hides inside apparently legitimate invoices, contracts, payments and accounting records.
- Money laundering attempts to conceal the criminal source, ownership or movement of assets.
- Placement introduces criminal proceeds, layering hides their origin and integration makes them appear legitimate.
- Terrorist financing may involve lawful or unlawful funds used for an illegal purpose.

- Proliferation financing may involve funding prohibited weapons activities or evading related sanctions.
- A predicate offence is the underlying crime that generates proceeds later concealed through money laundering.
- KYC and Customer Due Diligence establish who the customer is, who controls the relationship and whether the activity makes sense.
- High-risk customers and politically exposed persons require proportionate Enhanced Due Diligence.
- Transaction monitoring identifies unusual patterns that cannot be explained by the customer's known activities.
- Suspicious activity must be documented, escalated and reported through authorised channels.
- Confidentiality must be protected to prevent tipping off and evidence destruction.
- Sanctions screening must cover customers, beneficial owners, third parties, transactions and destinations.
- Cyber-enabled fraud exploits technology, urgency, impersonation and weak verification procedures.
- Internal investigations must be independent, fair, confidential and properly authorised.
- Evidence must be preserved securely with a documented chain of custody.
- Asset tracing follows criminal proceeds, while asset recovery uses lawful procedures to return or confiscate them.
- Interagency cooperation is essential when financial crime crosses organisations, sectors or national borders.

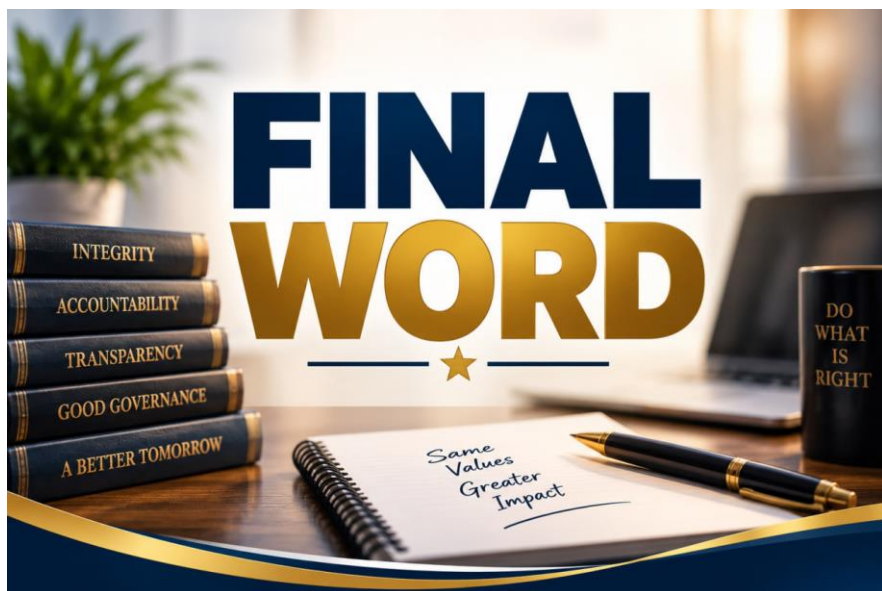
The central lesson from Level 3 is clear: **advanced corruption and financial crime rarely appear as one obvious illegal payment.** They are often hidden behind legitimate companies, professional documents, trusted individuals, digital systems and complex transactions.

Your responsibility is to look beyond appearances, question unexplained activity, identify who truly benefits, preserve evidence and ensure that authority remains accountable.

Completing Level 3 does not make you a law-enforcement officer, forensic investigator or legal practitioner. It gives you advanced awareness and practical knowledge to recognise governance failures,

identify financial-crime risks, support preventive controls and escalate concerns responsibly.

The professional standard is straightforward: **know the customer, understand the transaction, identify the real beneficiary, protect the evidence and never allow influence or urgency to replace proper controls.**



FINAL WORD

As we close this programme, remember that corruption and financial crime do not survive only because dishonest people exist. They survive because warning signs are ignored, controls are bypassed, records are poorly examined and influential people are allowed to operate without accountability.

You have now progressed through three important stages:

- **Level 1** taught you to recognise corruption and understand financial integrity.
- **Level 2** taught you to identify, assess, control and monitor corruption risks.
- **Level 3** taught you to examine governance failures, financial-crime methods, suspicious transactions, hidden ownership and institutional response.

This knowledge must be applied with discipline. Do not make accusations without evidence. Do not ignore suspicious activity because someone is powerful. Do not treat compliance as paperwork. Do not allow urgency, familiarity or profit to replace proper verification.

Wherever you work, your responsibility is to protect processes, resources, institutions and public trust.

Integrity is not demonstrated by what you say when everything is easy. It is demonstrated by what you do when dishonesty is profitable, pressure is present and silence would be more convenient.