

FRAUD RISK ASSESSMENT (FRA)

Aligned with UK GovS-013 and Fraud Prevention Standard

DOCUMENT CONTROL

Item	Details
Document Title	Fraud Risk Assessment (FRA)
Organization	[INSERT ORGANIZATION NAME]
Assessment Type	<input type="checkbox"/> Enterprise <input type="checkbox"/> Thematic <input type="checkbox"/> IFIA <input type="checkbox"/> Full FRA
Assessment Period	[INSERT DATE RANGE]
Assessor Name	[INSERT NAME]
Assessor Credentials	[INSERT CREDENTIALS]
Review Date	[INSERT DATE]
Approval By	[INSERT BOARD/EXEC NAME]
Document Version	1.0
Last Updated	[INSERT DATE]
Next Review Date	[INSERT DATE]
Classification	<input type="checkbox"/> Public <input type="checkbox"/> Internal <input type="checkbox"/> Confidential

EXECUTIVE SUMMARY

Purpose

This Fraud Risk Assessment identifies, evaluates, and prioritizes fraud risks faced by [INSERT ORGANIZATION NAME] and establishes a framework for implementing effective fraud prevention procedures. This assessment is conducted in accordance with:

- UK Government Functional Standard GovS-013: Counter Fraud
- Professional Standards and Guidance for Fraud Risk Assessment in Government
- Fraud Prevention Standard Requirements
- Economic Crime and Corporate Transparency Act 2023 (ECCTA) - "Failure to Prevent Fraud" Offense

Overall Risk Rating

Enterprise Fraud Risk Level: ☐ HIGH ☐ MEDIUM ☐ LOW

Key Findings Summary

Number of Risks Identified: [__]

- High Priority: [__]
- Medium Priority: [__]
- Low Priority: [__]

Critical Recommendations

1. [INSERT TOP PRIORITY #1] – Implement by [DATE]
2. [INSERT TOP PRIORITY #2] – Implement by [DATE]

3. [INSERT TOP PRIORITY #3] – Implement by [DATE]

SECTION 1: ORGANIZATION INFORMATION

1.1 Organizational Context

Item	Detail
Organization Name	[_____]
Organization Type	<input type="checkbox"/> Public Sector <input type="checkbox"/> Charity <input type="checkbox"/> Private Sector <input type="checkbox"/> Not-for-Profit
Primary Sector	[_____]
Annual Revenue/Budget	£[_____]
Number of Employees	[_____]
Geographic Presence	[_____]
Key Business Activities	[_____]
Legal Structure	[_____]
Regulatory Environment	[_____]

1.2 Governance Structure

Board/Executive Oversight:

- Chief Executive: [_____]
- Chief Financial Officer: [_____]
- Head of Counter Fraud: [_____]
- Board Risk Committee Chair: [_____]

Counter Fraud Functional Lead:

- Name: [_____]
- Title: [_____]
- Contact: [_____]
- Experience: [_____]

1.3 Assessment Scope & Boundaries

Scope Includes:

- [List all departments/functions assessed]

Scope Excludes:

- [List any areas outside scope]

Assessment Methodology:

- ☐ Interviews with stakeholders
- ☐ Document review
- ☐ Data analysis
- ☐ Testing and sampling
- ☐ Historical fraud data review
- ☐ Process walkthroughs

SECTION 2: ORGANIZATIONAL RISK APPETITE

2.1 Fraud Risk Tolerance

Organizational Risk Appetite Statement:

Our organization's risk appetite for fraud is LOW. We are committed to implementing and maintaining proportionate, practical fraud prevention procedures that demonstrate a strong organizational culture against fraud.

2.2 Risk Tolerance Parameters

Risk Dimension	Tolerance Level	Rationale
Financial Loss	£[____] threshold	[Explain]
Reputational Damage	[Low/Medium/High]	[Explain]
Regulatory Non-Compliance	[Specify]	[Explain]
Employee Misconduct	Zero tolerance	[Explain]

2.3 Risk Escalation Thresholds

- **Enterprise Risk Register:** Risks scoring >15/25
- **Board Report:** Risks with >£[____] potential impact
- **Immediate Escalation:** Any suspected fraud incidents
- **External Report:** Any reportable incidents to regulators

SECTION 3: FRAUD RISK IDENTIFICATION

3.1 Research Phase - Known Risks

Sources of Information Reviewed:

1. Historical Fraud Data

- Previous incidents: [____]
- Loss amounts: [____]
- Detection methods: [____]
- Root causes: [____]

2. Sector Intelligence

- [List industry reports, enforcement actions, sector warnings]

3. Regulatory & Compliance Data

- [List recent regulatory findings, enforcement notices]

4. Audit Reports

- [List control weaknesses identified]

5. External Best Practice

- [List industry standards, benchmarking data]

3.2 Fraud Risk Categories

Category 1: Asset Misappropriation

- Employee theft
- Inventory theft
- Cash theft
- Expense fraud
- Petty cash fraud

Category 2: Fraudulent Financial Reporting

- Revenue recognition fraud
- Inventory overstatement

- False journal entries
- Accrual manipulation
- Related party transactions

Category 3: Corruption & Bribery

- Procurement manipulation
- Vendor fraud
- Conflict of interest
- Gifts and hospitality violations
- Nepotism

Category 4: Cyber Fraud

- System access fraud
- Data theft
- Ransomware attacks
- Business email compromise
- Invoice manipulation

Category 5: Internal Threats

- Employee fraud
- Contractor fraud
- Supplier fraud
- Third-party collusion

SECTION 4: DETAILED RISK ASSESSMENT

4.1 Risk Assessment Matrix

Inherent Risk Scale:

Rating	Definition	Score
Critical	Would severely impact organization	5
High	Would significantly impact organization	4
Medium	Would moderately impact organization	3
Low	Minor impact on organization	2
Minimal	Negligible impact	1

Probability Scale:

Rating	Definition	Score
Almost Certain	Likely to occur	5
Likely	Probable	4
Possible	Could occur	3
Unlikely	Low probability	2

Rare	Very unlikely	1
------	---------------	---

4.2 Detailed Risk Assessments

RISK #1: [RISK DESCRIPTION]

Element	Detail
Risk ID	FRA-001
Risk Category	[Select from Section 3.2]
Process Area	[_____]
Risk Owner	[Name/Title]
Related Fraud Triangle	<input type="checkbox"/> Opportunity <input type="checkbox"/> Motive <input type="checkbox"/> Rationalization

Risk Description:

[Provide detailed description of the fraud risk, what could happen, and why it matters]

Potential Fraud Scenarios:

1. [Scenario 1]
2. [Scenario 2]
3. [Scenario 3]

Inherent Risk Assessment (before controls):

Factor	Rating	Notes
Impact	[1-5]	[Explain]
Probability	[1-5]	[Explain]
Inherent Risk Score	[____]/25	[Impact × Probability]

Existing Controls:

Control	Type	Effectiveness	Evidence
[Control 1]	Preventive/ Detective	[High/Medium/ Low]	[Documentation]
[Control 2]	Preventive/ Detective	[High/Medium/ Low]	[Documentation]
[Control 3]	Preventive/ Detective	[High/Medium/ Low]	[Documentation]

Control Effectiveness Assessment:

- Design: [Strong/Adequate/Weak]
- Operating Effectiveness: [Strong/Adequate/Weak]
- Testing Evidence: [Describe]

Residual Risk Assessment (after controls):

Factor	Rating	Notes
--------	--------	-------

Impact	[1-5]	[Explain]
Probability	[1-5]	[Explain]
Residual Risk Score	[]/25	[Impact × Probability]

Risk Rating: ☐ **HIGH** (15-25) ☐ **MEDIUM** (8-14) ☐ **LOW** (1-7)

Mitigating Factors:

- [Factor 1]
- [Factor 2]

Aggravating Factors:

- [Factor 1]
- [Factor 2]

RISK #2: [RISK DESCRIPTION]

[Follow same format as Risk #1]

RISK #3: [RISK DESCRIPTION]

[Follow same format as Risk #1]

[CONTINUE FOR ALL IDENTIFIED RISKS]

SECTION 5: FRAUD RISK REGISTER

5.1 Summary Risk Register

Risk ID	Risk Description	Category	Impact	Probability	Inherent Score	Current Controls	Residual Score	Priority	Risk Owner
FRA-001	[]	[]	[1-5]	[1-5]	[]	[]	[]	[H/M/L]	[Name]
FRA-002	[]	[]	[1-5]	[1-5]	[]	[]	[]	[H/M/L]	[Name]
FRA-003	[]	[]	[1-5]	[1-5]	[]	[]	[]	[H/M/L]	[Name]

SECTION 6: RISK ASSESSMENT BY PROCESS, PEOPLE & CONTROLS

6.1 PROCESS RISKS

6.1.1 Procurement & Supplier Management

Risk Overview:

Fraud in procurement can include supplier fraud, kickbacks, conflicts of interest, and collusion.

Key Risks Identified:

1. Risk of Fraudulent Suppliers

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]

- Gaps: [Identify]

2. Risk of Procurement Process Bypass

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

3. Risk of Conflict of Interest

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]
- [Action 3]

6.1.2 Financial Transactions & Approvals

Risk Overview:

Fraud in financial processes including unauthorized transactions, false entries, and payment fraud.

Key Risks Identified:

1. Risk of Unauthorized Transactions

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

2. Risk of Expense Fraud

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

3. Risk of Payroll Fraud

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]
- [Action 3]

6.1.3 Cash Handling & Bank Reconciliations

Risk Overview:

Cash and banking fraud including theft, unauthorized transfers, and reconciliation manipulation.

Key Risks Identified:**1. Risk of Cash Theft**

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

2. Risk of Unauthorized Bank Transfers

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

3. Risk of Reconciliation Fraud

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]
- [Action 3]

6.1.4 Revenue & Income Recognition**Risk Overview:**

Fraudulent revenue recording, fictitious revenue, and income manipulation.

Key Risks Identified:**1. Risk of Revenue Manipulation**

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

2. Risk of Fictitious Transactions

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]

6.1.5 Inventory & Asset Management**Risk Overview:**

Inventory theft, asset misappropriation, and false recording.

Key Risks Identified:**1. Risk of Inventory Theft**

- Inherent Risk: [H/M/L]

- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

2. Risk of Asset Misappropriation

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]

6.2 PEOPLE RISKS

6.2.1 Employee Screening & Vetting

Risk Overview:

Risks from inadequate background checking and unsuitable recruitment.

Key Risks Identified:

1. Risk of Hiring Individuals with Fraud History

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

2. Risk of Inadequate Reference Checking

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]

6.2.2 Management Oversight & Tone from Top

6.2.2 Management Oversight & Tone from Top

Risk Overview:

Weak management oversight, poor organizational culture, and failure to set appropriate tone increases fraud risk.

Key Risks Identified:

1. Risk of Weak Leadership on Anti-Fraud

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

2. Risk of Inadequate Performance Incentives

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]

- Controls: [List]
- Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]

6.2.3 Whistleblowing & Speak-Up Culture

Risk Overview:

Inadequate mechanisms for reporting fraud reduce detection and increase risk.

Key Risks Identified:

1. Risk of Unreported Fraud
 - Inherent Risk: [H/M/L]
 - Residual Risk: [H/M/L]
 - Controls: [List]
 - Gaps: [Identify]
2. Risk of Inadequate Protection for Whistleblowers
 - Inherent Risk: [H/M/L]
 - Residual Risk: [H/M/L]
 - Controls: [List]
 - Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]

6.2.4 Third-Party & Contractor Risks

Risk Overview:

Fraud by suppliers, contractors, and external parties.

Key Risks Identified:

1. Risk of Contractor Fraud
 - Inherent Risk: [H/M/L]
 - Residual Risk: [H/M/L]
 - Controls: [List]
 - Gaps: [Identify]
2. Risk of Inadequate Third-Party Due Diligence
 - Inherent Risk: [H/M/L]
 - Residual Risk: [H/M/L]
 - Controls: [List]
 - Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]

6.2.5 Gifts, Hospitality & Conflict of Interest

Risk Overview:

Inadequate management of conflicts of interest and improper gifts/hospitality.

Key Risks Identified:

1. Risk of Undisclosed Conflicts of Interest

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

2. Risk of Inappropriate Gifts/Hospitality

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]

6.3 CONTROL RISKS

6.3.1 Segregation of Duties

Risk Overview:

Inadequate separation of authorization, execution, and reconciliation functions.

Key Risks Identified:

1. Risk of Incompatible Duties Assigned

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Current Segregation: [Describe]
- Gaps: [Identify]

2. Risk of Manual Override of System Controls

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Controls: [List]
- Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]

6.3.2 Authorization & Approval Workflows

Risk Overview:

Ineffective authorization procedures allowing unauthorized transactions.

Key Risks Identified:

1. Risk of Inadequate Authorization Levels

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Current Controls: [Describe]
- Gaps: [Identify]

2. Risk of Authorization System Bypass

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]

- Controls: [List]
- Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]

6.3.3 IT System Access Controls

Risk Overview:

Inappropriate system access allowing unauthorized transactions and data manipulation.

Key Risks Identified:

1. Risk of Excessive System Access
 - Inherent Risk: [H/M/L]
 - Residual Risk: [H/M/L]
 - Access Controls: [Describe]
 - Gaps: [Identify]
2. Risk of Default Passwords and Weak Authentication
 - Inherent Risk: [H/M/L]
 - Residual Risk: [H/M/L]
 - Controls: [List]
 - Gaps: [Identify]
3. Risk of Inadequate User Termination Procedures
 - Inherent Risk: [H/M/L]
 - Residual Risk: [H/M/L]
 - Current Procedures: [Describe]
 - Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]
- [Action 3]

6.3.4 Monitoring & Detection Systems

Risk Overview:

Lack of effective monitoring mechanisms reduces fraud detection capability.

Key Risks Identified:

1. Risk of Inadequate Transaction Monitoring
 - Inherent Risk: [H/M/L]
 - Residual Risk: [H/M/L]
 - Monitoring Tools: [List]
 - Gaps: [Identify]
2. Risk of Delayed Fraud Detection
 - Inherent Risk: [H/M/L]
 - Residual Risk: [H/M/L]
 - Detection Mechanisms: [Describe]
 - Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]

6.3.5 Audit Trails & Record-Keeping

Risk Overview:

Inadequate audit trails prevent detection and investigation of fraudulent activity.

Key Risks Identified:

1. Risk of Inadequate System Audit Trails
 - Inherent Risk: [H/M/L]
 - Residual Risk: [H/M/L]
 - Current Audit Trail Capability: [Describe]
 - Gaps: [Identify]
2. Risk of Destroyed or Altered Records
 - Inherent Risk: [H/M/L]
 - Residual Risk: [H/M/L]
 - Record Retention Policy: [Reference]
 - Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]

6.3.6 Data Security & Cybersecurity

Risk Overview:

Inadequate cybersecurity increases risk of fraud through system compromise.

Key Risks Identified:

1. Risk of System Breach/Ransomware
 - Inherent Risk: [H/M/L]
 - Residual Risk: [H/M/L]
 - Controls: [List]
 - Gaps: [Identify]
2. Risk of Business Email Compromise
 - Inherent Risk: [H/M/L]
 - Residual Risk: [H/M/L]
 - Controls: [List]
 - Gaps: [Identify]

Recommendations:

- [Action 1]
- [Action 2]

SECTION 7: FRAUD PREVENTION FRAMEWORK

7.1 Organization's Fraud Prevention Approach

Counter-Fraud Culture:

Our organization is committed to creating a strong anti-fraud culture characterized by:

- Clear tone from leadership
- Zero tolerance for fraud
- Comprehensive training and awareness
- Open speak-up channels
- Proportionate and swift investigation

7.2 Existing Fraud Prevention Procedures

7.2.1 Counter Fraud Policies

Policy	Status	Last Review	Next Review
Counter Fraud Policy	<input type="checkbox"/> In Place	[]	[]
Whistleblowing Policy	<input type="checkbox"/> In Place	[]	[]
Gifts & Hospitality Policy	<input type="checkbox"/> In Place	[]	[]
Conflict of Interest Policy	<input type="checkbox"/> In Place	[]	[]
Supplier Code of Conduct	<input type="checkbox"/> In Place	[]	[]
Code of Ethics	<input type="checkbox"/> In Place	[]	[]

Policy Gaps:

- [Identify any missing policies]

7.2.2 Fraud Training & Awareness

Training Type	Frequency	Attendance	Evidence
Induction Training	[]	[]%	[]
Annual Mandatory Training	[]	[]%	[]
Role-Specific Training	[]	[]%	[]
Senior Management Training	[]	[]%	[]
Contractor/ Supplier Training	[]	[]%	[]

Training Gaps:

- [Identify any training needs]

7.2.3 Reporting Mechanisms

- ☐ Dedicated fraud hotline

- ☐ Anonymous reporting portal
- ☐ Email reporting address
- ☐ In-person reporting to manager
- ☐ External reporting to regulator
- ☐ Protected whistleblower channels

Reporting Procedures:

[Describe how reports are logged, tracked, and investigated]

7.2.4 Investigation & Response

Function	Responsibility	Contact
Fraud Investigation Lead	[Name/Title]	[Contact]
Investigation Procedures	[Reference document]	[__]
Timeline for Investigation	[Specify]	[__]
Disciplinary Procedures	[Reference document]	[__]
External Reporting Procedures	[Reference document]	[__]

7.3 Governance & Oversight

7.3.1 Board Oversight

- Board has responsibility for fraud risk oversight: ☐ Yes ☐ No
- Board receives regular fraud reporting: ☐ Yes ☐ No
- Frequency of reporting: [__]
- Board Committee: [__]

7.3.2 Risk Committee

- Risk Committee established: ☐ Yes ☐ No
- Fraud risk on committee agenda: ☐ Yes ☐ No
- Frequency of review: [__]
- Chair: [Name]

7.3.3 Counter Fraud Function

- Dedicated counter fraud resource: ☐ Yes ☐ No
- Head of Counter Fraud: [Name]
- Team size: [__]
- Reporting line: [__]

SECTION 8: PRIORITY RECOMMENDATIONS & ACTION PLAN

8.1 High Priority Recommendations (Implement within 3 months)

#	Recommendation	Rationale	Responsible Party	Target Date	Success Criteria
---	----------------	-----------	-------------------	-------------	------------------

1	[Action]	[Why this is priority]	[Name]	[Date]	[How success measured]
2	[Action]	[Why this is priority]	[Name]	[Date]	[How success measured]
3	[Action]	[Why this is priority]	[Name]	[Date]	[How success measured]

8.3 Low Priority Recommendations (Implement within 12 months)

#	Recommendation	Rationale	Responsible Party	Target Date	Success Criteria
1	[Action]	[Why this is priority]	[Name]	[Date]	[How success measured]
2	[Action]	[Why this is priority]	[Name]	[Date]	[How success measured]

8.4 90-Day Quick Wins

Actions with immediate high impact to implement within 90 days:

1. Action: [____]
 - Timeline: [____]
 - Resource Required: [____]
 - Expected Outcome: [____]
2. Action: [____]
 - Timeline: [____]
 - Resource Required: [____]
 - Expected Outcome: [____]
3. Action: [____]
 - Timeline: [____]
 - Resource Required: [____]
 - Expected Outcome: [____]

SECTION 9: COMPLIANCE MAPPING

9.1 Alignment with GovS-013

GovS-013 Requirement	Current Status	Evidence	Gap
----------------------	----------------	----------	-----

Risk Assessment conducted	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]
Three-level assurance framework	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]
Counter fraud policies in place	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]
Fraud response plan documented	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]
Training program established	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]
Proactive testing conducted	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]
Investigation capability in place	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]
Reporting metrics established	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]

9.2 Alignment with Fraud Prevention Standard

FPS Requirement	Current Status	Evidence	Gap
Leadership & Accountability	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]
Counter Fraud Policy	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]
Risk Assessment	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]
Proportionate Response	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]
Detection Capability	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]
Investigation Capability	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]
Sanctions & Prosecution	<input type="checkbox"/> ✓ <input type="checkbox"/> ✗	[]	[]

9.3 Alignment with ECCTA 2023 "Failure to Prevent Fraud

