From: deric deric7223r@gmail.com
Date: 26 Nov 2025 at 00:52:35
To: fred33bb3@icloud.com

Fraud Risk Assessment (FRA) – Pilot Package Overview

Purpose: Helping organisations demonstrate fraud prevention, reduce risk, and align with UK standards.

Scope of Service

The FRA Pilot Package includes the following components:

1. Initial Consultation & Intake Questionnaire

30-minute scoping call (no cost) to understand your organisation's specific context

Comprehensive intake questionnaire to gather essential information about your current fraud prevention measures

Discussion of key risk areas and organisational structure

2. Templated Fraud Risk Assessment (FRA)

Aligned with UK GovS-013 (UK Government Security Classification Policy)

Aligned with the Fraud Prevention Standard requirements

Standardised 10-12 page report format

Suitable for audits and compliance records

Demonstrates compliance with the new UK "failure to prevent fraud" offence (ECCTA 2023)

3. Identification of Priority Risk Areas

Assessment focuses on three key dimensions:

Process: Workflow vulnerabilities and procedural gaps

People: Internal and external personnel risks

Controls: Existing safeguards and control weaknesses

4. Actionable Recommendations

Proportional, practical steps tailored to your organisation's size and complexity

Risk mitigation priorities ranked by urgency and impact

Clear roadmap for implementation (3-6 months typical)

5. Evidence Pack

Includes:

Summary report of key findings and recommendations

Training awareness outline (slide deck template)

30-minute workshop outline for staff briefing

Documentation suitable for auditors, regulators, and trustees

6. Optional Subscription Add-on: Quarterly Prevention Dashboard

Ongoing quarterly dashboard tracking fraud prevention metrics

12-month subscription

Continuous monitoring and updated recommendations

Regular check-ins on implementation progress

Fixed-price options designed to be accessible for small organisations and charities:

Service	Price Range
FRA Health Check	£1,200 – £1,800
FRA Awareness Briefing	£2,000 – £2,500
FRA Awareness Quarterly Dashboard (12 months)	£3,000 – £3,500
Custom Multi-site / Complex Organisations	Custom pricing available

Why This Matters

Legal & Compliance Context:

Organisations are now accountable for having reasonable fraud prevention procedures under the Economic Crime and Corporate Transparency Act 2023 (ECCTA)

This FRA pilot provides:

Affordable, independent assurance of your fraud prevention measures

Tangible evidence for auditors, regulators, and trustees

Compliance demonstration with UK government standards

Risk mitigation to reduce potential criminal liability

Key Benefits:

Shows you take fraud prevention seriously

Demonstrates due diligence to external stakeholders

Identifies vulnerabilities before they become problems

Creates audit trail and documentary evidence

Supports insurance claims and regulatory submissions

Process Overview

Step 1: Book a 30-minute scoping call (no cost)

Discuss organisational context and requirements

Clarify scope and objectives

Step 2: Complete Intake Questionnaire

Gather detailed information about current systems

Identify known vulnerabilities or concerns

Step 3: Fraud Risk Assessment Delivery

Typically completed within 3-4 weeks

Comprehensive analysis and recommendations provided

Step 4: Optional Follow-up

Subscribe to quarterly dashboard (12-month commitment)

Ongoing training and awareness support

Regular implementation check-ins

Service

Small to medium organisations needing affordable fraud risk assessment

Charities and not-for-profits preparing for regulatory scrutiny

Organisations seeking compliance with ECCTA 2023 requirements

Companies wanting independent evidence of fraud prevention procedures

Businesses lacking dedicated fraud prevention expertise

Key Differentiators

✓ UK Standard Aligned – GovS-013 and Fraud Prevention Standard compliant
✓ Proportional Approach – Recommendations scaled to your organisation size
✓ Practical & Actionable – Not just theoretical; includes implementation roadmap
✓ Evidence Ready – Audit-suitable documentation included

✓ Cost-Effective – Pilot package pricing accessible for small organisations
✓ Optional Ongoing Support – Quarterly dashboard for continuous monitoring

Provider: Safeguard Advisory Ltd

Contact: To book your complimentary 30-minute scoping call

This package demonstrates your commitment to fraud prevention and provides the documentary evidence needed to show compliance with the new UK "failure to prevent fraud" offence under the ECCTA 2023.

Six-Step FRA Process

Step 1: Context & Scope Definition

Define assessment boundaries and objectives

Identify stakeholders with in-depth knowledge

Establish key decision makers and risk owners

Step 2: Research Known Risks

Conduct data analysis

Review previous audits

Gather sector-specific information

Study enforcement actions and best practice

Step 3: Identify & Categorize Risks

Identify key known and hypothetical fraud risks

Categorize by fraud type (asset misappropriation, fraudulent financial reporting, corruption, cybersecurity)

Define each risk clearly

Step 4: Risk Owner & Inherent Risk Evaluation

Assign a risk owner with sufficient seniority

Evaluate inherent risk using qualitative or quantitative scales

Assess probability and impact

Consider cost vs. materiality of risk exposure

Step 5: Control/Mitigation & Residual Risk Evaluation

Identify existing controls and mitigations

Evaluate residual risk (risk remaining after controls)

Assess control effectiveness

Step 6: Risk Prioritization

Prioritize residual risks against organizational risk appetite

Focus on highest-risk areas first

Create action plans for mitigation

Fraud Risk Assessment Framework - The Fraud Triangle

When assessing fraud risks, consider three key factors:

Opportunity – Can fraud occur?

Weak controls

Lack of segregation of duties

Poor authorization processes

Inadequate monitoring

Motive – Why might someone commit fraud?

Financial pressures and targets

Performance incentives

Recognition and reward systems

Emergency scenarios

Rationalization – How might someone justify fraud?

Organizational culture and tone from the top

Speak-up culture (or lack thereof)

Management integrity

Key Risk Areas to Assess

Process Risks:

Procurement and supplier management

Financial transactions and approvals

Payroll and HR processes

Cash handling and bank reconciliations

Conflict of interest management

People Risks:

Employee screening and vetting

Third-party and contractor risks

Management oversight

Whistleblowing culture

Gifts, hospitality, and bribery risks

Control Risks:

Segregation of duties

Authorization workflows

IT system access controls

Data security and cybersecurity

Monitoring and detection systems

Audit trails and record-keeping

Fraud Risk Assessment Standards - Key Components

Organization Guidance:

Governance structures for managing fraud risk

Board/executive oversight requirements

Three-level assurance framework

Process Guidance:

Recommended processes for effective FRA implementation

Integration with organizational risk registers

Stakeholder engagement approach

Product Guidance:

What good quality FRA outputs look like

Fraud Risk Register requirements

Documentation standards

Output: Fraud Risk Register

The final product must include a fully populated Fraud Risk Register containing:

Specific identified fraud risks

Risk owner for each risk

Inherent risk rating (before controls)

Residual risk rating (after controls)

Mitigating controls

Implementation timeline

Success metrics

Areas of uncertainty

The Register should integrate into organizational risk registers as appropriate.

GovS-013 Requirements

Organizations should establish:

1. Risk Assessments at Three Levels:

High-level enterprise assessment for the board

Intermediate assessment for departments/functions

Detailed assessments for highest-risk areas

2. Counter Fraud Policies & Procedures:

Regularly reviewed counter fraud policy

Fraud response plan

Conflict of interest policies

Gifts and hospitality controls

3. Proactive Testing & Reporting:

Annual work program to mitigate risks

Outcome-based metrics reporting

4. Organizational Assurance:

Three separate levels of assurance

Operational management oversight

Senior management review

Independent audit

"Failure to Prevent Fraud" Offense Compliance

For ECCTA 2023 compliance, organizations must demonstrate "reasonable fraud prevention procedures" including:

Risk Assessment Considerations:

Reward and recognition systems that may incentivize fraud

Financial or operating pressures (time pressures, targets, reporting dates)

Emergency scenarios where fraud risks increase

Inside-out view of employees and third parties

Fraud Prevention Measures:

Risk assessments across the corporate group

Updated training programs

Robust control frameworks

Regular monitoring and review

Best Practice Implementation Timeline

Immediate (Months 1-2):

Map core business areas and processes

Identify high-risk areas

Conduct enterprise-level FRA

Engage senior management

Short-term (Months 3-6):

Conduct detailed FRAs in high-risk areas

Document fraud risk register

Develop mitigation strategies

Implement priority controls

Ongoing (6+ months):

Quarterly risk reviews

Annual comprehensive reassessment

Monitor control effectiveness

Update based on enforcement actions and incidents

Key Success Factors

✓ Leadership Commitment – Clear tone from the top about fraud prevention importance

✓ Stakeholder Engagement – Involve people with deep knowledge of operations

✓ Proportionality – Tailor assessments to organization size and risk profile

✓ Data-Driven – Use actual data, audits, and incident history

✓ Integration – Link FRA with broader risk management and governance

✓ Documentation – Maintain audit trail for compliance evidence

✓ Regular Review – Update assessments annually or after significant changes

This comprehensive FRA framework ensures organizations can demonstrate "reasonable fraud prevention procedures" under UK law and protect themselves against fraud threats.

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	□ Enterprise □ Thematic □ IFIA □ 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	□ Public □ Internal □ 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	□ Public Sector □ Charity □ Private Sector □ 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	□ Opportunity □ Motive □ 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

continue

I'll continue with the comprehensive Fraud Risk Assessment document:

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:

. Risk of Weak Leadership on Anti-Fraud

- Inherent Risk: [H/M/L]

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

1. 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]

1. 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:

. Risk of Contractor Fraud

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

. 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]

1. 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:

. Risk of Incompatible Duties Assigned

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

. 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:

. 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:

. Risk of Inadequate System Audit Trails

- Inherent Risk: [H/M/L]
- Residual Risk: [H/M/L]
- Current Audit Trail Capability: [Describe]
- Gaps: [Identify]

. 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	□ In Place	[___]	[___]
Whistleblowing Policy	□ In Place	[___]	[___]
Gifts & Hospitality Policy	□ In Place	[___]	[___]
Conflict of Interest Policy	□ In Place	[___]	[___]
Supplier Code of Conduct	□ In Place	[___]	[___]
Code of Ethics	□ 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]

8.2 Medium Priority Recommendations (Implement within 6 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	□ ✓ □ ×	[____]	[____]
Three-level assurance framework	□ ✓ □ ×	[____]	[____]
Counter fraud policies in place	□ ✓ □ ×	[____]	[____]
Fraud response plan documented	□ ✓ □ ×	[____]	[____]
Training program established	□ ✓ □ ×	[____]	[____]
Proactive testing conducted	□ ✓ □ ×	[____]	[____]
Investigation capability in place	□ ✓ □ ×	[____]	[____]
Reporting metrics established	□ ✓ □ ×	[____]	[____]

9.2 Alignment with Fraud Prevention Standard

FPS Requirement	Current Status	Evidence	Gap
Leadership & Accountability	□ ✓ □ ×	[____]	[____]
Counter Fraud Policy	□ ✓ □ ×	[____]	[____]
Risk Assessment	□ ✓ □ ×	[____]	[____]
Proportionate Response	□ ✓ □ ×	[____]	[____]
Detection Capability	□ ✓ □ ×	[____]	[____]
Investigation Capability	□ ✓ □ ×	[____]	[____]
Sanctions & Prosecution	□ ✓ □ ×	[____]	[____]