Budget-Holder Fraud Risk Guidance

Essential Guide for Financial Decision-Makers

Document Purpose

This guide provides practical, actionable fraud risk management guidance for budget-holders across all departments. Budget-holders control spending decisions and are on the front line of fraud prevention.

Who Is a Budget-Holder?

You are a budget-holder if you:

- Approve purchases or expenditure

- Manage a departmental/project budget

- Authorize supplier payments

- Approve timesheets or expenses

- Make procurement decisions

- Manage contracts with third parties

Your role is critical: 85% of occupational fraud involves budget-holder functions (procurement, payroll, expenses).

Your Legal & Ethical Obligations

Legal Duties

Under the **Economic Crime and Corporate Transparency Act 2023** (effective September 2025):

Organisational Liability:

If fraud is committed for the organisation's benefit and you failed to prevent it through reasonable procedures, the organisation can face:

- Unlimited fines

- Director disqualification

- Criminal conviction

Personal Liability:

If you knowingly participate in or facilitate fraud:

- Criminal prosecution (Fraud Act 2006)

- Dismissal for gross misconduct

- Civil recovery of losses

- Professional disqualification

Ethical Duties

Stewardship:

You manage stakeholder resources (taxpayer money, donor funds, shareholder capital). This is a position of trust.

Role Modeling:

Your team watches your behavior. Shortcuts you take signal "acceptable" conduct.

Fiduciary Duty:

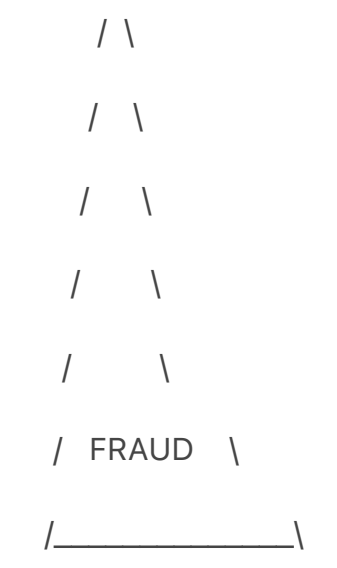
Act in the organisation's best interests, not personal convenience.

Understanding Fraud: The Budget-Holder Perspective

The Fraud Triangle

Fraud occurs when three elements align:

```
        PRESSURE
    (Financial stress,
     unrealistic targets)
          /\
```



(Weak controls, lack of oversight)

("Everyone does it," "I deserve this")

```

**Your Control Point:** OPPORTUNITY

You cannot control employee financial pressures or their ability to rationalize. But you CAN remove opportunities through robust controls.

---

## Common Fraud Scenarios in Budget-Holder Functions

### 1. Procurement Fraud

#### Scenario A: Fake Supplier Invoice
```

How it works:

- Fraudster creates fake supplier identity

- Submits invoice for goods/services never provided

- Invoice appears legitimate (professional branding, VAT number)

- Payment processed to fraudulent bank account

Red Flags:

- New supplier with no prior relationship

- Sole trader/individual rather than established company

- Generic email (Gmail, Hotmail vs. corporate domain)

- No physical address or vague location

- Payment urgency ("Pay immediately to avoid penalties")

- Round numbers (£5,000.00 vs. £4,847.23)

Controls:

- Verify ALL new suppliers before first payment

- Check Companies House registration (UK)

- Call supplier using independently verified phone number

- Require purchase order before invoice submission

- Three quotes for purchases above threshold

Example:

Finance team received £8,500 invoice from "IT Solutions Ltd" for software

licenses. Checked Companies House—company dissolved 2 years ago. Avoided £8,500 loss.

Scenario B: Inflated Pricing / Kickbacks

How it works:

- Employee colludes with supplier

- Supplier inflates prices above market rate

- Employee approves payment

- Supplier pays kickback to employee (cash, gifts, benefits)

Red Flags:

- Single supplier used repeatedly without competitive quotes

- Pricing significantly above market rate

- Employee resistant to changing suppliers

- Unusually close relationship between employee and supplier

- Employee lifestyle inconsistent with salary (luxury items, holidays)

- Split purchases just below approval threshold

Controls:

- Rotate supplier relationships periodically

- Require competitive quotes for purchases >£X

- Benchmark pricing against market rates

- Segregate duties (requisitioner ≠ approver)

- Declare conflicts of interest (family/friend suppliers)

- Random invoice sampling and price verification

Example:

Department spent £45,000 annually with one stationery supplier. Market comparison showed 40% overpricing. Investigation revealed employee received "loyalty rewards" (disguised kickbacks).

Scenario C: Split Purchases to Avoid Approval

How it works:

- Employee artificially divides one large purchase into multiple smaller transactions

- Each transaction falls below approval threshold

- Avoids scrutiny of higher-level authorization

- May be legitimate need or fraud concealment

Red Flags:

- Multiple invoices from same supplier on same day

- Sequential invoice numbers for similar items

- Purchases just below delegation threshold (e.g., £4,900 when limit is £5,000)

- Vague descriptions ("Miscellaneous supplies")

Controls:

- Monitor transaction patterns (automated alerts)

- Review supplier spending monthly

- Enforce "no splitting" policy

- Require justification for multiple small purchases

- Approval based on total project cost, not per-invoice

---

2. Invoice & Payment Fraud

Scenario D: Email Impersonation (Business Email Compromise)

How it works:

- Fraudster impersonates supplier via spoofed email

- Email states: "We've changed bank details—please update for future payments"

- Looks identical to legitimate supplier communication

- Payment diverted to fraudulent account

- Often timed when key person on leave/unavailable

Red Flags:

- Unexpected bank detail change request

- Urgency language ("Update immediately")

- Slight misspelling in sender email (supp1ier vs. supplier)

- Generic greeting ("Dear Customer" vs. your name)

- External email warning missing

- Request sent outside normal business hours

Controls:

- **NEVER update bank details via email alone**

- Call supplier using phone number from contract/invoice (not email)

- Verbal confirmation with two authorized signatories

- Test payment (£1) before full amount

- Flag all bank changes for senior approval

- Email security (SPF, DKIM, DMARC checks)

Example:

NHS trust received email from "construction supplier" requesting bank change. Verified by phone—supplier had not sent email. Avoided £127,000 fraud.

Critical Rule: All bank detail changes require phone verification using independently sourced contact information.

Scenario E: Duplicate Payments

How it works:

- Same invoice submitted twice (intentionally or accidentally)

- Different invoice numbers or formatting to avoid detection

- Second payment processed

- Fraudster pockets duplicate (if intentional) or supplier retains overpayment

Red Flags:

- Same amount, same supplier, similar dates

- Supplier unusually slow to notify overpayment

- Vague invoice descriptions making comparison difficult

- Missing purchase order reference

Controls:

- Three-way match (PO + receipt + invoice)

- Automated duplicate detection (finance system)

- Unique invoice numbering system

- Supplier statement reconciliation monthly

- Payment approval by someone other than requestor

---

3. Payroll & HR Fraud

Scenario F: Ghost Employees

How it works:

- Fictitious employee added to payroll system

- Salary payments made to fraudulent bank account

- Employee "works" in department with poor headcount oversight

- May be former employee not removed from system

Red Flags:

- Employees with no personnel file

- Same bank account for multiple employees

- Employees never taking leave

- No emergency contact information

- Employee unreachable or never seen in office

- Duplicate National Insurance numbers

Controls:

- Monthly headcount reconciliation (payroll vs. actual staff)

- Starter/leaver verification by HR and department

- Bank account uniqueness checks

- Mandatory annual leave (fraud detection opportunity)

- Random personnel file audits

Example:

Council payroll audit found 3 "employees" paid for 18 months. Total loss: £87,000. Fraudster was payroll clerk with weak oversight.

Scenario G: Timesheet Fraud

How it works:

- Employee inflates hours worked

- Unauthorized overtime claimed

- Time claimed for personal activities

- Collusion between employee and timesheet approver

Red Flags:

- Overtime patterns inconsistent with workload

- Timesheets always submitted at maximum allowed

- Lack of work output despite claimed hours

- Approver doesn't verify actual work performed

- Retrospective timesheet changes

Controls:

- Require evidence of work completed (deliverables)

- Spot checks on claimed hours vs. building access logs

- Approval by direct supervisor who knows workload

- Pre-authorization required for overtime

- System alerts for unusual patterns

---

4. Expense Fraud

Scenario H: False Expense Claims

How it works:

- Personal expenses claimed as business (meals, travel, accommodation)

- Receipts fabricated or altered (Photoshop, online generators)

- Same receipt submitted multiple times to different approvers

- Expenses for events that didn't occur

Red Flags:

- Receipts from unusual sources (handwritten, poor quality)

- Mileage claims inconsistent with diary/meetings

- High-value claims with vague descriptions

- Weekend/holiday expenses for "business" activities

- Receipts in employee's name (hotels should show organisation name)

- Sequential receipt numbers across different vendors

Controls:

- Require original itemized receipts (not credit card slips)

- Cross-check mileage vs. calendar appointments

- Sample verification (call hotel/restaurant to confirm)

- Expense policy with clear examples (what's allowed/prohibited)

- Random audit of expense claims

- Digital receipt submission (harder to alter)

Example:

Employee claimed £8,000 in "client entertainment" over 6 months. Audit revealed receipts from family birthday parties, personal dining. Dismissed for gross misconduct.

Scenario I: Mileage Fraud

How it works:

- Inflated distance claimed

- Personal journeys claimed as business

- Commuting distance included (not reimbursable)

- Phantom journeys (claim travel that didn't occur)

Red Flags:

- Mileage claims exceed vehicle capacity (e.g., 50,000 miles/year)

- Routes inefficient (Google Maps shows shorter distance)

- Claims for dates when employee was on leave

- Same journey different distances each claim

Controls:

- Require destination details (address, postcode)

- Automated mileage calculation (system-generated)

- Comparison to calendar/meeting invites

- Spot checks using mapping tools

- Annual declaration of business vs. personal mileage

- Consider company vehicles to eliminate mileage claims

---

5. Contract & Revenue Fraud

Scenario J: Contract Splitting

How it works:

- Large contract artificially divided into smaller contracts

- Each below competitive tender threshold

- Avoids procurement scrutiny

- May involve kickbacks from supplier

Red Flags:

- Multiple small contracts with same supplier for similar services

- Contracts start/end on consecutive dates

- Total value would exceed tender threshold

- Services could reasonably be consolidated

Controls:

- Aggregate spending review per supplier annually

- Contracts board review all awards (even below threshold)

- Require business justification for multiple contracts

- Procurement oversight of contract patterns

Scenario K: Revenue Manipulation

How it works:

- Cash receipts pocketed before recording

- Sales recorded at inflated values

- Revenue recognized prematurely

- Refunds processed to fraudster's account

Red Flags:

- Unexplained revenue variances

- Cash handling by single individual

- Missing receipt numbers (sequential gaps)

- Refunds processed without supporting evidence

- Customer complaints about missing receipts

Controls:

- Dual control over cash handling

- Pre-numbered receipt books (gap analysis)

- Daily cash reconciliation

- Refund approval by manager

- Surprise cash counts

- Segregation of duties (cash handler ≠ reconciler)

Your Fraud Prevention Checklist

Use this checklist daily/weekly to ensure robust controls:

Daily Responsibilities

Before Approving ANY Payment:

- [ ] Verify goods/services actually received (three-way match)

- [ ] Confirm supplier is legitimate (if new/unusual)

- [ ] Check invoice amount matches agreement/quote

- [ ] Ensure proper authorization obtained

- [ ] Verify bank details if payment to new account

- [ ] Question anything unusual or urgent

Before Approving Timesheets/Expenses:

- [ ] Verify hours/expenses are reasonable and consistent with work

- [ ] Check receipts are original, itemized, and dated

- [ ] Confirm business purpose is legitimate

- [ ] Cross-check dates (employee was at work/traveling)

- [ ] Apply policy consistently (no favoritism)

Weekly Responsibilities

- [ ] Review budget variances (investigate significant deviations)

- [ ] Check for unusual transaction patterns (duplicates, round numbers)

- [ ] Reconcile supplier statements to payments

- [ ] Review aged payables (are we paying on time? delays may indicate issues)

- [ ] Spot-check a sample of transactions approved by subordinates

---

Monthly Responsibilities

- [ ] Review total spending by supplier (concentration risk)

- [ ] Benchmark key costs against market/budget

- [ ] Reconcile headcount to payroll

- [ ] Review exception reports (split purchases, high-value transactions)

- [ ] Assess control effectiveness (are processes working?)

- [ ] Update fraud risk register for your area

Quarterly Responsibilities

- [ ] Conduct surprise audits/spot checks

- [ ] Review and update delegated authorities

- [ ] Refresh fraud awareness with team

- [ ] Report fraud risk metrics to senior management

- [ ] Test controls (e.g., attempt to process fake invoice—does it get caught?)

Annual Responsibilities

- [ ] Complete fraud risk assessment for your budget area

- [ ] Review and update financial policies/procedures

- [ ] Mandatory fraud awareness training

- [ ] Declare conflicts of interest

- [ ] Rotate duties/responsibilities (prevent over-familiarity)

Delegation of Authority: Know Your Limits

Why Authority Limits Matter

Delegation limits exist to:

- Prevent single-person fraud

- Ensure appropriate oversight

- Protect you from unwitting involvement in fraud

- Spread accountability

Common Authority Structures

Example Authority Matrix:

| Transaction Type | Up to £1,000 | £1,000-£5,000 | £5,000-£25,000 | £25,000+ |

|---|---|---|---|---|

| **Procurement** | Team Leader | Budget Holder | Senior Manager | Director + CFO |

| **Expenses** | Line Manager | Budget Holder | Director | CEO |

| **Payroll Changes** | HR Officer | HR Manager | HR Director | CEO |

| **Contract Awards** | N/A | Budget Holder | Director + Procurement | Board |

| **New Suppliers** | N/A | Budget Holder (verified) | Senior Manager | CFO |

Golden Rules:

1. Never exceed your authority (even "just this once")

2. Never approve your own transactions

3. Never approve for family/friends without disclosure

4. If in doubt, escalate upward

Spotting Red Flags: Your Fraud Radar

Behavioral Red Flags (People)

Watch for changes in behavior:

Financial Stress Indicators:

- Employee discussing money problems

- Debt collector calls to workplace

- Gambling references

- Sudden lifestyle changes (new car, luxury items inconsistent with salary)

Work Behavior Indicators:

- Reluctance to take leave (fear of discovery)

- Working unusual hours alone

- Defensive when questioned

- Overly close relationships with suppliers/contractors

- Control issues (won't delegate, won't share passwords)

- Unusually helpful in "covering" for colleagues

Attitudinal Indicators:

- Disgruntlement with employer

- Entitlement mentality ("I'm underpaid, so I deserve this")

- Pressure to meet unrealistic targets

- "Everyone else does it" justifications

Important: These are indicators, not proof. Do not accuse—report concerns through proper channels.

Transactional Red Flags (Documents)

Invoice Red Flags:

- Photocopied invoices (original should be available)
- Handwritten invoices from "established" companies
- Invoice numbers out of sequence
- Dates inconsistent (invoice dated before PO)
- Vague descriptions ("Miscellaneous services")
- Unprofessional formatting/typos
- Missing VAT registration (if VAT charged)
- Post office box address only

Payment Red Flags:

- Payee name doesn't match supplier
- Payment to individual for corporate service
- Offshore bank accounts (when not expected)
- Round numbers (£10,000.00 vs. £9,847.50)
- Urgency demands ("Pay today or face penalties")

Supplier Red Flags:

- No online presence (website, Companies House, reviews)
- Contact details generic (mobile phone, Gmail)
- Address is residential or non-existent
- Company name very similar to established firm
- Recently incorporated (check formation date)

What to Do If You Suspect Fraud

Step 1: Do Not Confront the Individual

Why?

- Fraudster may destroy evidence

- May pose personal safety risk

- May intimidate witnesses

- Could constitute defamation if wrong

Instead:

- Document your concerns objectively

- Secure evidence (take copies, don't remove originals)

- Report through proper channels

Step 2: Report Through Proper Channels

Internal Reporting Options:

1. **Line Manager/Senior Manager**

   Best for: Concerns about subordinates or peers

2. **Fraud Risk Owner** (typically CFO, Head of Finance, Head of Governance)

   Best for: Concerns about your manager or complex fraud

3. **Whistleblowing Hotline/Email**

   Best for: Sensitive concerns, desire for anonymity

   [Insert your organisation's whistleblowing contact details]

4. **Internal Audit**

   Best for: Systemic control weaknesses

5. **HR Department**

   Best for: Concerns about employment fraud (timesheets, expenses)

External Reporting Options (if internal channels ineffective):

- **Serious Fraud Office (SFO):** Major/complex fraud

- **Action Fraud (National Fraud & Cyber Crime Reporting Centre):** 0300 123 2040

- **HMRC:** Tax fraud

- **Charity Commission:** Charity sector fraud

- **NHS Counter Fraud Authority:** NHS fraud

Step 3: Preserve Evidence

Do:

- Make copies of suspicious documents

- Save emails (don't delete or forward to personal accounts)

- Note dates, times, people involved

- Write down your observations contemporaneously

- Secure physical evidence (lock in drawer/safe)

Don't:

- Remove original documents (could be construed as theft)

- Discuss with colleagues (rumors, tipping off fraudster)

- Conduct your own investigation (contaminate evidence)

- Use company IT systems to store evidence (may be accessed by fraudster)

Step 4: Cooperate with Investigation

If an investigation is launched:

- **Be available** for interviews

- **Answer honestly** - don't speculate or embellish

- **Maintain confidentiality** - don't discuss with anyone except investigators/ legal counsel

- **Don't retaliate** against whistleblower (even if you disagree with allegation)

- **Follow instructions** from investigators (e.g., don't alert the subject)

Protection for Whistleblowers

Legal Protections (UK)

Public Interest Disclosure Act 1998 protects you if:

- You report in good faith

- You reasonably believe the information is true

- You report to appropriate person/body

- The disclosure is in the public interest

You are protected from:

- Dismissal

- Disciplinary action

- Demotion or denial of promotion

- Harassment or victimization

Your responsibilities:

- Report through proper channels first (internal before external)

- Do not make malicious/false allegations

- Do not disclose for personal gain

If you face retaliation:

Contact [Insert HR/Legal contact] immediately. Retaliation is grounds for employment tribunal claim.

Common Myths About Fraud

Myth 1: "Fraud only happens in large organisations"

Reality: Small organisations suffer higher fraud losses (as % of revenue) due to:

- Fewer resources for controls

- Greater trust/familiarity (less skepticism)

- Lack of segregation of duties

Myth 2: "Trusted, long-serving employees won't commit fraud"

Reality:

- Average fraudster tenure: 8+ years (ACFE)

- Trust creates opportunity

- Pressure/rationalization can affect anyone

Myth 3: "We have an audit—fraud would be detected"

Reality:

- Audits sample transactions (don't check 100%)

- Auditors aren't forensic investigators

- Sophisticated fraud designed to pass audit scrutiny

- 15% of fraud detected by external audit vs. 40% by whistleblowing

Myth 4: "Fraud prevention is Finance's job"

Reality:

- Budget-holders approve 85% of fraud transactions

- YOU are the front line

- Finance provides oversight, but you approve day-to-day spending

Myth 5: "Small amounts don't matter"

Reality:

- Small frauds escalate (fraudster becomes emboldened)

- Signal weak controls (attracts more fraud)

- £100/week = £5,200/year per fraudster

- Cultural impact ("if they get away with it, why can't I?")

Training & Awareness

Mandatory Training Requirements

All budget-holders must complete:

1. **Initial fraud awareness training** (upon appointment)

   - This guidance document

   - Organisation-specific policies

   - Case studies

   - Assessment quiz

2. **Annual refresher training**

   - Update on new fraud trends

   - Policy changes

   - Control effectiveness review

3. **Specific training for role**

   - Procurement fraud (if managing contracts)

   - Payroll fraud (if approving timesheets)

   - Expense fraud (if approving claims)

Team Awareness

Your responsibility: Ensure your team understands:

- Fraud risks relevant to their roles

- How to report concerns

- Why controls exist (not "red tape")

- Consequences of fraud (organisational and personal)

Suggested methods:

- Team meetings (quarterly fraud risk discussion)

- Case study reviews (anonymized)

- Control walkthroughs (explain why we do things)

- "Fraud of the month" email (brief awareness)

Case Studies: Learn from Real Incidents

Case Study 1: The Trusted Administrator

Background:

Finance administrator, 12 years' service, highly trusted, never took leave.

Fraud:

Created fake supplier ("Office Solutions Pro")

Submitted 47 invoices over 3 years for office supplies never delivered

Invoices just below approval threshold (£4,950)

Payments diverted to personal bank account

Total Loss: £232,650

How Detected:

Administrator went on sick leave (unexpected)

Temporary cover queried invoice from unfamiliar supplier

Investigation revealed supplier was fake

Controls That Failed:

- No mandatory annual leave policy

- No supplier verification for amounts below £5,000

- Same person requested and processed payments

- No periodic supplier review

Lessons:

- Mandatory leave is a control (fraud can't be concealed when absent)

- Verify ALL suppliers, not just large ones

- Segregation of duties prevents single-person fraud

Case Study 2: The Email Impersonation

Background:

Finance team received email from "building contractor" working on premises.

Fraud Attempt:

Email stated: "Our bank has changed. Please update payment details for final invoice (£87,000) due this week."

Email looked identical to contractor's format

Sender address: contractor-ltd.com (real company: contractorltd.com - subtle difference)

Outcome:

Finance officer called contractor using phone number from original contract

Contractor confirmed they had NOT changed banks and had not sent email

Payment blocked

Police notified (international fraud gang)

Total Loss: £0 (prevented)

Controls That Worked:

- Policy: All bank changes verified by phone

- Used independently sourced contact info (not from email)

- Staff trained to spot impersonation

Lessons:

- Email is not a secure method for bank changes

- Visual inspection of sender email address critical

- Phone verification using known contact details is gold standard

---

Case Study 3: The Split Purchases

Background:

Department manager had £10,000 single-transaction authority.

Fraud:

Over 18 months, made 60+ purchases from same IT supplier

Each purchase £9,500-£9,900 (just below threshold)

Total spending: £580,000

Market comparison showed 35% overpricing

Investigation Findings:

Manager receiving "commission" from supplier (disguised as "consulting fees" to shell company)

Supplier inflated prices and paid kickback

Many items never delivered or inferior quality

Total Loss: £203,000 (overpayments + fictitious goods)

How Detected:

Finance team ran supplier spend analysis

Flagged concentration risk (single supplier, 60+ transactions)

Internal audit investigation launched

Controls That Failed:

- No competitive quotes required below £10,000

- No periodic supplier spend review

- Manager not required to declare conflict (consulting relationship)

Lessons:

- Analyse transaction patterns, not just individual transactions

- Require competitive quotes periodically (even for established suppliers)

- Mandatory conflict of interest declarations annually

Policy & Procedure Quick Reference

Key Policies You Must Follow

1. **Financial Regulations/Standing Orders**
   - Delegation of authority limits
   - Procurement thresholds
   - Payment approval process

2. **Procurement Policy**
   - Competitive quotes/tender requirements
   - Supplier verification process

- Contract award procedures

3. **Expenses Policy**
   - What can be claimed (mileage, meals, accommodation)
   - Receipt requirements
   - Approval limits
   - Timescales for submission

4. **Gifts & Hospitality Policy**
   - What can be accepted (typically <£50)
   - Declaration requirements
   - Register of interests

5. **Whistleblowing Policy**
   - How to report concerns
   - Protections available
   - Investigation process

6. **Fraud Response Plan**
   - What constitutes fraud
   - Immediate actions if fraud suspected
   - Investigation procedures
   - Disciplinary process

Action: Confirm you have read and understood these policies. Keep copies accessible.

FAQs for Budget-Holders

Q1: I've approved a payment but now suspect it might be fraudulent. What do I do?

A: Report immediately to your manager or fraud risk owner. Do not delay. The sooner fraud is detected, the more likely recovery. Do not feel embarrassed—detecting fraud is a success, not a failure.

Q2: A supplier is pressuring me to bypass procurement procedures due to "urgency." Can I do this?

A: No. Urgency is a common fraud indicator. Legitimate suppliers understand proper procedures. Escalate to procurement or senior management if genuinely urgent. Document the request and your response.

Q3: I'm worried about reporting a colleague—we've worked together for years.

A: Your duty is to the organisation, not personal relationships. Report concerns; let investigators determine facts. Most suspicions are resolved innocently. Failing to report is a breach of your responsibilities.

Q4: How do I balance fraud prevention with trust in my team?

A: Controls are not about distrust—they protect everyone. Fraud controls prevent false accusations (evidence trail) and protect honest employees from suspicion. Frame controls as protecting the team, not policing them.

Q5: What if I make a mistake and accidentally approve something I shouldn't?

A: Honest mistakes happen. Report immediately. Fraud requires intent. If you approved in good faith but were deceived, that's fraud by the other party, not you. Cooperate with any investigation.

Q6: Can I approve my own expenses or purchases?

A: No. Self-approval is a fundamental control weakness. All transactions require independent approval by someone with appropriate authority.

Q7: Our budget is tight. Can we skip controls to save time/money?

A: No. Weak controls cost more in fraud losses than they save in efficiency. Budget constraints are fraud pressure—controls become MORE important, not less.

Q8: What's the difference between fraud, error, and poor judgment?

A:

- **Fraud:** Intentional deception for personal gain (criminal)

- **Error:** Unintentional mistake (training/process issue)

- **Poor judgment:** Bad decision made honestly (performance issue)

Intent is the key. If unsure, report and let investigators determine.

Your Fraud Prevention Pledge

As a budget-holder, I commit to:

- [ ] Understand and comply with all financial policies
- [ ] Exercise delegated authority responsibly and within limits
- [ ] Apply controls consistently (no shortcuts, no exceptions)
- [ ] Question unusual, urgent, or suspicious requests
- [ ] Verify suppliers, invoices, and bank details before approval
- [ ] Never approve my own transactions
- [ ] Declare all conflicts of interest
- [ ] Report fraud concerns immediately through proper channels
- [ ] Set the tone for my team (ethical behavior, speak-up culture)
- [ ] Complete mandatory fraud awareness training annually
- [ ] Support fraud investigations with full cooperation
- [ ] Protect whistleblowers from retaliation

Signature: _____

Date: _____

Budget Area/Department: _____

Additional Resources

Internal Resources

- **Fraud Risk Owner:** [Name, Email, Phone]

- **Whistleblowing Hotline:** [Number/Email]

- **Internal Audit:** [Contact]

- **Procurement Team:** [Contact]

- **HR Department:** [Contact]

External Resources

- **Action Fraud:** 0300 123 2040 | www.actionfraud.police.uk

- **Serious Fraud Office:** www.sfo.gov.uk

- **Government Counter-Fraud Standards:** [GovS-013](https://www.gov.uk/government/publications/government-functional-standard-govs-013-counter-fraud)

- **Chartered Institute of Public Finance & Accountancy (CIPFA):** Fraud guidance

- **Association of Certified Fraud Examiners (ACFE):** Global fraud statistics

Stop FRA Platform

- **Platform:** Automated fraud risk assessment

- **Contact:** [Insert Stop FRA contact details]

- **Resources:** Training modules, case studies, templates

Document Version: 1.0

Last Updated: January 1, 2026

Next Review: January 1, 2027

Owner: [Fraud Risk Owner Name/Title]

Distribution: All budget-holders, procurement staff, senior management

Status: Mandatory reading for all financial decision-makers