Fraud Risk Awareness Briefing - Slide Deck

## Complete Presentation Content for Leadership & Trustees

### Presentation Metadata

- **Total Slides:** 12 core + 3 optional

- **Duration:** 30 minutes (45-60 with optional modules)

- **Format:** PowerPoint/Google Slides/Keynote

- **Design Notes:** Professional, minimal text, high-impact visuals

---

## SLIDE 1: Title Slide

### Visual Design

**Background:** Professional gradient (navy to teal) or organisational brand colors

**Layout:** Centered content

### Content

```

FRAUD RISK MANAGEMENT

A New Era of Accountability
```

Awareness Briefing for Leadership & Trustees

[Date]

[Organisation Name]

Presented by: [Facilitator Name, Title]

```

### Speaker Notes

- Welcome attendees

- Introduce yourself and role

- State workshop objectives: understand regulatory landscape, leadership responsibilities, and immediate next steps

- Emphasize interactive nature - encourage questions throughout

---

## SLIDE 2: Opening & Context

### Title

**"The Failure to Prevent Fraud Offence: What You Need to Know"**

### Visual Design
```

**Left Column (50%):** Large icon or graphic representing law/compliance

**Right Column (50%):** Key facts

### Content

**The New Landscape:**

📅 **Effective:** September 2025

⚖️ **Source:** Economic Crime and Corporate Transparency Act 2023

🎯 **Target:** Organisations, not just individuals

💰 **Penalty:** Unlimited fines + director disqualification + reputational damage

---

**What Changed?**

Before: Only individuals prosecuted for fraud

Now: Organisations criminally liable if fraud committed "for their benefit"

---

**The Critical Point:**

Your organisation can be convicted even if:

- Senior leadership had no knowledge

- Robust policies existed on paper

- It was one rogue employee

**Unless:** You can prove reasonable prevention procedures were in place

### Speaker Notes

- Emphasize paradigm shift: organisational accountability

- Ask: "How many have reviewed fraud risk in past 12 months?"

- Note: This isn't just compliance theatre; it's existential risk management

- September 2025 is closer than it appears—action needed now

---

## SLIDE 3: Who This Applies To

### Title

**"Is Your Organisation in Scope?"**

### Visual Design

**Center:** Qualification criteria in visual checklist format

**Bottom:** Warning banner

### Content

**Large Organisation Criteria**

(Must meet 2 of 3):

✓ Annual turnover > £36 million

✓ Balance sheet total > £18 million

✓ 250+ employees

---

**BUT WAIT...**

⚠️ Even if you're below these thresholds:

- Fraud committed "for your benefit" = you're liable

- Insurers expect fraud risk management

- Regulators scrutinize governance

- Stakeholders demand transparency

- **Best practice applies to ALL organisations**

---

**Key Question:**

"Can we afford NOT to manage fraud risk systematically?"

### Speaker Notes

- Many attendees may assume they're too small to be affected

- Emphasize: Fraud doesn't discriminate by organization size

- Even small charities, SMEs face significant fraud risks

- Regulatory expectations evolving across all sectors

---

## SLIDE 4: Understanding Fraud - The Triangle Model

### Title

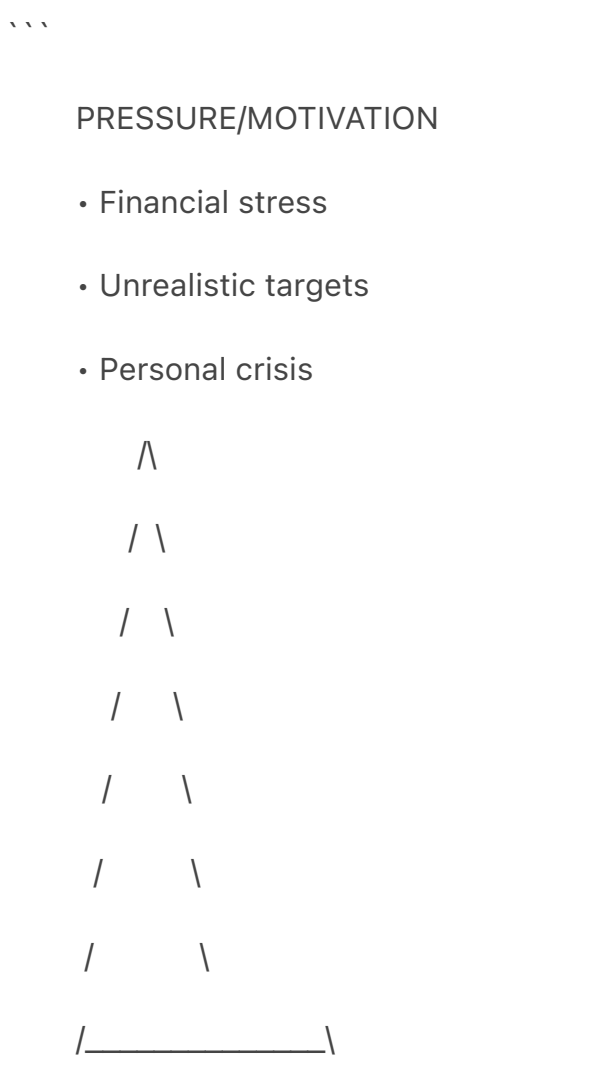
**"What Constitutes Fraud? The Three Elements"**

### Visual Design

**Center:** Triangle graphic with three labeled corners

**Surrounding:** Examples for each element

### Content


PRESSURE/MOTIVATION
• Financial stress
• Unrealistic targets
• Personal crisis
OPPORTUNITY
• Weak controls
• Lack of oversight
• Access to assets
RATIONALIZATION
• "Everyone does it"
• "I deserve this"
• "Just borrowing"

---

**Common Fraud Types in Your Organisation:**

🛒 **Procurement:** Fake suppliers, kickbacks, bid rigging

👥 **Payroll:** Ghost employees, timesheet manipulation

💵 **Revenue:** Sales inflation, premature recognition

📄 **Expenses:** False claims, personal use of funds

🔒 **Cyber:** Email impersonation, invoice fraud

### Speaker Notes

- Fraud is NOT committed by obvious criminals

- Often long-serving, trusted employees under pressure

- All three elements must be present—eliminate one, prevent fraud

- Most effective: Remove OPPORTUNITY through controls

---

## SLIDE 5: The Defence - Reasonable Procedures

### Title

**"Your Legal Shield: Reasonable Prevention Procedures"**

### Visual Design

**Left:** Shield icon with "Reasonable Procedures" text

**Right:** Six principles as numbered list

### Content

**The ONLY Defence:**

Prove you had **reasonable procedures** to prevent fraud

---

**Six Principles (GovS-013 Framework):**

1️⃣ **Top-level commitment**

Tone from the top—board demonstrates zero tolerance

2️⃣ **Risk assessment**

Systematic identification of fraud risks

3️⃣ **Proportionate procedures**

Controls matched to your risk profile

4️⃣ **Due diligence**

Third-party vetting (suppliers, partners)

5️⃣ **Communication & training**

Awareness at all levels of organisation

6️⃣ **Monitoring & review**

Continuous improvement, not one-off exercise

---

**"Reasonable" ≠ Perfect**

It means: Proportionate, documented, regularly reviewed

### Speaker Notes

- These principles are your roadmap

- GovS-013 is government standard but applies beyond public sector

- Courts will assess "reasonableness" based on your size, sector, risk profile

- Documentation is critical—can you prove what you did?

---

## SLIDE 6: Financial & Reputational Consequences

### Title

**"The True Cost of Fraud"**

### Visual Design

**Two columns:** Direct Costs | Indirect Costs

**Bottom:** Case study highlight box

### Content

**Direct Costs**

💰 **Average fraud loss:**

5% of annual revenue (ACFE 2024)

📊 **Investigation costs:**

Legal fees, forensic accounting

⚖️ **Regulatory fines:**

Unlimited under new offence

---

**Indirect Costs**

📉 **Reputational damage**

Customer/donor trust erosion

📈 **Insurance premiums**

Increased costs, reduced coverage

❌ **Lost contracts**

Partners exit relationships

😔 **Employee morale**

Culture of distrust

👔 **Director disqualification**

Personal consequences for leadership

---

**Case Study:**

NHS Trust procurement fraud

- £1.2M loss over 3 years

- £400K investigation costs

- CEO resignation

- 18 months to restore stakeholder confidence

### Speaker Notes

- 5% revenue loss = £1.8M for £36M turnover organisation

- Reputational damage often exceeds direct financial loss

- Ask: "What would fraud scandal mean for OUR organisation?"

- Emphasize: Prevention cheaper than cure

---

## SLIDE 7: Board & Leadership Responsibilities

### Title

**"What Leadership Must Own"**

### Visual Design

**Top:** Five non-delegable duties as icons

**Bottom:** Red flag checklist

### Content

**Non-Delegable Duties**

1️⃣ **Approve fraud risk strategy**

Board-level ownership and oversight

2️⃣ **Allocate adequate resources**

Budget for prevention, detection, response

3️⃣ **Set the tone**

Model ethical behavior consistently

4️⃣ **Receive regular reports**

Fraud risk on board agenda (minimum quarterly)

5️⃣ **Challenge & scrutinize**

Ask difficult questions, don't accept platitudes

---

**🚩 Red Flags of Governance Failure:**

❌ No fraud risk on board agenda in past 12 months

❌ No designated fraud risk owner

❌ Fraud response plan doesn't exist or untested

❌ No training for budget-holders or procurement staff

❌ Whistleblowing policy not publicized to staff

---

**Critical Question:**

"When did our board last receive a comprehensive fraud risk report?"

### Speaker Notes

- These are leadership responsibilities—cannot delegate to operational teams

- Board owns the strategy; management executes

- If you can't answer "when we last reviewed fraud risk," that's a red flag

- Interactive: Ask attendees to self-assess against red flags

---

## SLIDE 8: Budget-Holder Accountability

### Title

**"Budget-Holders: You Are the Front Line"**

### Visual Design

**Center:** Four-quadrant graphic showing fraud scenarios

**Border:** "Your Obligations" footer

### Content

**Why Budget-Holders Are Critical:**

You control spending, approve transactions, manage supplier/staff relationships

---

**Common Fraud Scenarios:**

📦 **Procurement Fraud**

- Split purchases to avoid approval thresholds

- Sole-sourcing without justification

- Conflicts of interest (family/friend suppliers)

📄 **Invoice Fraud**

- Fake supplier invoices

- Inflated pricing, duplicate payments

- Bank account change requests (impersonation)

👥 **Payroll Manipulation**

- Ghost employees on payroll

- Unauthorized overtime claims

- Inappropriate use of temp staff budgets

💳 **Expense Abuse**

- Personal expenses claimed as business

- Inflated mileage/subsistence claims

---

**Your Obligations:**

✓ Know your delegated authority limits

✓ Question unusual requests

✓ Follow procurement procedures (no shortcuts)

✓ Report suspicions immediately (not tomorrow, NOW)

---

**Scenario Exercise:**

"A trusted 10-year supplier emails: 'Urgent—update bank details for payment.' What do you do?"

### Speaker Notes

- Budget-holders often feel pressure to "make things happen quickly"

- Shortcuts create opportunities for fraud

- **Scenario answer:** STOP. Call supplier using known phone number. Verify request. Email impersonation is #1 fraud vector.

- Emphasize: You won't be penalized for questioning suspicious requests

---

## SLIDE 9: Conducting a Fraud Risk Assessment

### Title

**"Starting Your Fraud Risk Assessment Journey"**

### Visual Design

**Left column:** 5-step process flowchart

**Right column:** Timeline and tools

### Content

**Step-by-Step Process:**

**1. Identify fraud risk areas**

Where could fraud occur in our operations?

**2. Assess inherent risk**

Impact × Likelihood (without controls)

**3. Review existing controls**

What prevents/detects fraud now?

**4. Calculate residual risk**

Risk remaining after controls applied

**5. Prioritize gaps**

Focus resources on high-residual risks

---

**Time Required:**

🏢 Small organisation: 2-4 weeks

🏛️ Medium/large organisation: 6-8 weeks

---

**Tools Available:**

✅ **Stop FRA platform**

Automated, GovS-013 aligned, generates reports

✅ **Internal audit-led assessment**

Leverage existing assurance function

✅ **External consultant support**

Specialist fraud risk advisors

---

**Key Message:**

"You don't need perfection on day one. Start with basic assessment and iterate."

### Speaker Notes

- Assessment is foundation of reasonable procedures

- Can't manage what you haven't measured

- Stop FRA automates much of this—13 comprehensive modules

- Question: "Who here has budget responsibility for risk assessment?"

---

## SLIDE 10: Implementation Roadmap

### Title

**"From Assessment to Action: Your 90-Day Plan"**

### Visual Design

**Four-phase timeline** with checkboxes

### Content

**Phase 1: Weeks 1-4 (Foundation)**

- [ ] Board resolution: Commit to fraud risk management
- [ ] Appoint fraud risk owner (CFO, COO, Head of Governance)
- [ ] Budget allocation for assessment & controls
- [ ] Communicate commitment to all staff

---

**Phase 2: Weeks 5-8 (Assessment)**

- [ ] Conduct fraud risk assessment (Stop FRA or similar)
- [ ] Identify top 5-10 priority risks
- [ ] Review existing policies (whistleblowing, gifts, procurement)
- [ ] Gap analysis of current controls

---

**Phase 3: Weeks 9-12 (Action)**

- [ ] Draft/update fraud response plan

- [ ] Implement priority control improvements

- [ ] Schedule mandatory training (budget-holders first)

- [ ] Establish quarterly board reporting schedule

---

**Phase 4: Ongoing (Embed)**

- [ ] Annual fraud risk assessment refresh

- [ ] Bi-annual training updates

- [ ] Incident monitoring & reporting

- [ ] Independent assurance (audit review)

---

**Critical Path:**

Foundation → Assessment → Action → Embed

### Speaker Notes

- 90 days to operational baseline—ambitious but achievable

- Phase 1 is leadership commitment—without this, rest fails

- Phase 4 is continuous—fraud risk management never "finished"

- Stop FRA packages align with these phases

---

## SLIDE 11: Resources & Support

### Title

**"Support Available to You"**

### Visual Design

**Two-column layout:** Internal Resources | External Resources

**Bottom:** Stop FRA package comparison

### Content

**Internal Resources**

🛡️ **Stop FRA platform**

Package 1: Basic Health Check

Package 2: + Awareness Training

Package 3: + Real-time Dashboard

🔍 **Internal audit function**

Independent assurance and testing

⚖️ **Legal/compliance team**

Policy review and governance

👥 **HR department**

Employment fraud risks, culture assessment

---

**External Resources**

📘 **Government guidance**

"Failure to Prevent Fraud" (v1.5)

📊 **GovS-013 Standard**

Counter-Fraud Functional Standard

🏛️ **Sector-specific guides**

NHS CFA, Charity Commission, FCA guidance

💼 **Professional advisors**

Legal counsel, forensic accountants

---

**Stop FRA Packages:**

| Feature | Package 1 | Package 2 | Package 3 |
|---|---|---|---|
| Fraud risk assessment | ✅ | ✅ | ✅ |
| Automated reporting | ✅ | ✅ | ✅ |
| Employee training | — | ✅ | ✅ |
| Real-time dashboard | — | — | ✅ |
| Key-pass distribution | — | ✅ | ✅ |

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

### Speaker Notes

- Stop FRA designed for GovS-013 compliance from day one
- Package 1 sufficient for initial assessment
- Package 3 provides ongoing monitoring (large organisations)
- External resources are free—use them

---

## SLIDE 12: Q&A + Commitments

### Title

**"Questions & Commitments"**

### Visual Design

**Top half:** Open space for discussion

**Bottom half:** Commitment capture template

### Content

**Open Floor for Questions**

[Space for live discussion]

---

**Before We Leave: Collective Commitments**

**1. Board Commitment:**

- [ ] Fraud risk standing agenda item (quarterly minimum)

- [ ] Quarterly fraud risk report to board

**2. Leadership Action:**

- [ ] Fraud risk owner appointed by: _____

- [ ] Budget allocated for assessment: £_____

**3. Immediate Next Step:**

- Who will lead our fraud risk assessment? _____

- Target completion date: _____

---

**Closing Message:**

> "Fraud risk management isn't about assuming the worst of people.

> It's about building robust systems that protect everyone—

> our organisation, our employees, and those we serve."

### Speaker Notes

- Capture commitments in writing before attendees leave

- Emphasize: This session is start, not end

- Assign action owners for each commitment

- Schedule follow-up meeting (30 days) to review progress

- Distribute take-home materials

---

## OPTIONAL SLIDE 13: Live Fraud Scenario Exercise

### Title

**"Test Your Fraud Radar: Live Scenario"**

### Visual Design

**Top:** Scenario description box

**Bottom:** Group discussion prompts

### Content

**Scenario:**

Your Finance Manager of 8 years approaches you:

"We have an urgent payment due to a new IT supplier—£15,000 for cybersecurity software. The supplier needs payment today to maintain our license. I've checked them out; they're legitimate. Can you approve this as an exception to our normal procurement process? The vendor form is here."

**What do you do?**

---

**Breakout Discussion (5 minutes):**

1. What are the red flags?

2. What controls should exist to prevent this?

3. What's your immediate action?

---

**Debrief:**

**Red Flags:**

- Urgency ("needs payment today")

- New supplier (no due diligence)

- Exception to process

- Unusual request from trusted employee

**Controls:**

- Segregation of duties (approval ≠ requestor)

- Supplier verification process

- No exceptions to procurement policy

- Two-person approval for new suppliers

**Immediate Action:**

- STOP the payment

- Verify supplier independently (not via provided info)

- Check if software actually requested/needed

- Follow standard process—no shortcuts

---

**Real-World Outcome:**

This was an attempted invoice fraud. The "supplier" was fake. The Finance Manager's email had been compromised (spoofing attack). Organisation lost £0 because they followed procedures.

### Speaker Notes

- Only use if time permits (15-minute extension)

- Encourage active participation from all attendees

- Emphasize: Pressure to bypass controls is key fraud indicator

- Ask: "Would your team have caught this?"

---

## OPTIONAL SLIDE 14: Whistleblowing Deep Dive

### Title

**"Speak Up Culture: Your First Line of Defense"**

### Visual Design

**Center:** Statistics graphic

**Bottom:** Checklist for effective whistleblowing

### Content

**The Evidence:**

📊 **40% of fraud detected via whistleblowing** (ACFE 2024)

📊 **2x more likely to detect fraud** with formal hotline

📊 **Median loss 50% lower** when whistleblowing effective

---

**What Makes Whistleblowing Effective?**

✅ **Multiple channels**

Hotline, email, in-person, web portal

✅ **Anonymous option**

Remove fear of retaliation

✅ **Visible promotion**

Staff know it exists and how to use it

✅ **Protected disclosures**

Clear policy: no retaliation tolerated

✅ **Timely action**

Reports investigated promptly, outcomes communicated

✅ **Board oversight**

Quarterly report on whistleblowing activity

---

**Self-Assessment:**

When did you last:

- Review your whistleblowing policy?

- Communicate it to all staff?

- Investigate a whistleblowing report?

- Report whistleblowing metrics to the board?

**If answers are "I don't know" or "Never"—you have a gap.**

### Speaker Notes

- Whistleblowing is early warning system

- Employees often see fraud indicators before management

- Fear of retaliation is biggest barrier—must be eliminated

- Ask: "How many staff could describe our whistleblowing process right now?"

---

## OPTIONAL SLIDE 15: Cyber Fraud Focus

### Title

**"Cyber Fraud: The Fastest-Growing Threat"**

### Visual Design

**Three-panel layout:** Email Impersonation | Ransomware | IT Controls

### Content

**Email Impersonation (Invoice Fraud)**

📧 **How it works:**

- Fraudster impersonates supplier/senior executive

- Requests urgent payment or bank detail change

- Often sent when key person on holiday/sick

🛡️ **Controls:**

- Verify ALL bank changes via known phone number

- Dual authorization for payment >£X

- Staff training on spotting spoofed emails

---

**Ransomware Readiness**

🔒 **Threat:**

- Systems locked, data encrypted

- Ransom demand (often cryptocurrency)

- Business disruption for weeks/months

🛡️ **Controls:**

- Regular backups (tested restoration)

- Patch management (keep systems updated)

- Access controls (principle of least privilege)

- Incident response plan (pre-agreed actions)

---

**IT Control Environment**

**High-Risk Areas:**

- Privileged access (who can do what)

- Change management (unauthorized system changes)

- Data loss prevention

- Third-party access (vendors with system access)

**Assessment Questions:**

- Do we have IT audit trail/logging?

- Are access rights reviewed regularly?

- How quickly could we detect unauthorized access?

### Speaker Notes

- Cyber fraud often overlaps with IT security—but distinct risks

- Email impersonation #1 fraud vector globally

- Question for CIO/CTO (if present): "When did we last test our ransomware response plan?"

- Many organisations have strong perimeter security but weak internal controls

---

## Design Guidelines for Slide Deck

### Visual Design Principles

**Color Palette:**

- Primary: Navy blue (#003366) or organisation brand

- Accent: Teal (#00A5A8) for highlights

- Alert: Red (#D32F2F) for warnings

- Success: Green (#388E3C) for checkmarks

**Typography:**

- Headings: Sans-serif, bold, 32-40pt

- Body text: Sans-serif, 18-24pt

- Maximum 6 lines per slide body

**Icons:**

- Use consistent icon set (Font Awesome, Material Icons, or custom)

- Minimum 48×48px size for visibility

**Imagery:**

- Avoid generic stock photos

- Use data visualizations where possible

- Infographics over text-heavy slides

### Accessibility Considerations

- Minimum 18pt font size

- High contrast text (WCAG AA standard)

- Alt text for all images

- Avoid red-green only color coding (colorblind accessible)

---

## Presenter Notes General Guidance

**Delivery Tips:**

1. **Pace:** Maximum 2-3 minutes per slide

2. **Interaction:** Ask questions every 3-4 slides

3. **Stories:** Use real case studies (anonymized if needed)

4. **Energy:** Vary tone—avoid monotone delivery

5. **Eye contact:** Engage all attendees, not just senior person

**Handling Questions:**

- If technical/complex: "Let's take that offline after session"

- If beyond your expertise: "I'll find the answer and follow up"

- If challenging your content: "Valid point—let's explore that"

**Time Management:**

- Start on time (demonstrates respect)

- Have "parking lot" for off-topic questions

- 5-minute buffer built into 30-minute design

---

**Document Version:** 1.0

**Last Updated:** January 1, 2026

**Companion Document:**