

UK FAILURE TO PREVENT FRAUD

# The supplier readiness toolkit.

A practical workbook for UK businesses supplying – or wanting to supply – large organisations.

## CONTENTS

# Inside the toolkit.

Seven sections. Best done with a pen, not a spreadsheet. The scorecard, risk assessment, and delegation matrix are designed to be completed in one room, in under two hours.

- 
- |           |  |       |
|-----------|--|-------|
| <b>01</b> | <b>The readiness scorecard</b>                     | p. 03 |
|           | 19 statements, 19 points. Score yourself honestly. |       |
- 
- |           |   |       |
|-----------|---|-------|
| <b>02</b> | <b>The fraud risk assessment template</b>                     | p. 05 |
|           | A one-page workbook you can complete in a leadership meeting. |       |
- 
- |           |  |       |
|-----------|--|-------|
| <b>03</b> | <b>The delegation of authority matrix</b>                                      | p. 06 |
|           | Who can approve what, up to what value – the document procurement asks to see. |       |
- 
- |           |  |       |
|-----------|--|-------|
| <b>04</b> | <b>The implementation plan</b>                 | p. 07 |
|           | Five steps. Owners and evidence at each stage. |       |
- 
- |           |  |       |
|-----------|--|-------|
| <b>05</b> | <b>Model answers to the supplier questionnaire</b> | p. 08 |
|           | The eight questions a customer will actually ask.  |       |
- 
- |           |   |       |
|-----------|---|-------|
| <b>06</b> | <b>The internal conversation</b>                      | p. 10 |
|           | Three objections you'll hear, and how to handle them. |       |
- 
- |           |                                       |       |
|-----------|---------------------------------------|-------|
| <b>07</b> | <b>What to do this week</b>           | p. 11 |
|           | Four actions for the next seven days. |       |
-

## SECTION 01

# The readiness scorecard.

Tick every statement that is true of your business today. Be strict – a customer's procurement team will be. Each tick scores one point out of 19, and the next page tells you what your total means.

## 01 Ownership and governance 3 PTS

- A named individual at director or board level is formally responsible for fraud prevention, and it's written into their remit.
- Fraud prevention appears on the agenda of leadership meetings at least quarterly.
- Senior leaders have signed off a written fraud prevention policy in the last 12 months.

## 02 Risk assessment 3 PTS

- You have a documented fraud risk assessment that lists where fraud could occur, who could commit it, and what currently prevents it.
- The risk assessment has been reviewed in the last 12 months and is dated.
- The assessment covers risks of fraud committed to benefit the company (e.g. revenue overstated), not only fraud against the company.

## 03 Approval controls 4 PTS

- Invoice approvals run through a documented workflow with thresholds and required approvers – not on email or by a single person.
- Segregation of duties: the person who raises a payment is not the person who approves it.
- Approval limits are written down and tied to individual roles (a delegation of authority matrix exists).
- Every approved invoice has a timestamped audit trail showing who approved it and when.

## 04 Due diligence and onboarding 3 PTS

- New employees in finance, procurement, and sales roles are vetted before they start.
- New suppliers are checked against Companies House (or equivalent) and sanctions lists before onboarding.
- A documented process exists for verifying changes to supplier bank details.

## 05 Communication and culture 3 PTS

- A whistleblowing route exists and staff know how to use it.
- Anti-fraud training has been delivered to relevant staff in the last 12 months.
- Staff have acknowledged receipt of the fraud prevention policy in writing.

## 06 Monitoring 3 PTS

- Someone reviews exception reports – failed approvals, manual overrides, duplicate payments – at least monthly.
- A scheduled review of the controls happens at least quarterly.
- Incidents and near-misses are logged.

## SECTION 01 · CONTINUED

# What your score means.

Where the number lands tells you what to do next – and how urgently. Find your band, read the action, then turn to Section 02.

**0–4****CRITICAL GAP**

You don't have a defensible position. This needs to be a **board-level conversation this quarter**. The cheapest controls – naming an owner, writing a one-page risk assessment, documenting an approval matrix – add four to six points within a fortnight.

**5–9****EXPOSED**

You'll struggle with a refreshed supplier questionnaire and **risk losing renewals**. Start with Section 04 (the implementation plan) and work through it in order. Aim to be at 12+ within 90 days.

**10–14****PARTIAL**

You have the building blocks but **gaps a procurement team will notice**. Prioritise the lowest-scoring category above – most often it's approval controls or the documented risk assessment.

**15–19****READY**

You can answer a customer questionnaire today with **evidence to back it up**. The work now is keeping the framework alive – reviews, refresher training, updating the risk assessment.

## SECTION 02

# The fraud risk assessment.

Customers will ask whether you've done one. Most haven't. A one-page document, dated and signed, puts you ahead of most of your peers. For each area where value moves in or out, name the risk, who could commit it, what stops them, and what's left.

AREA	WHAT COULD GO WRONG	WHO COULD DO IT	CURRENT CONTROL	RESIDUAL RISK	ACTION NEEDED
Invoice payments	<i>Write here</i>	<i>Role / team</i>	<i>Control in place</i>	<i>Low / Med / High</i>	<i>Owner · Due date</i>
Supplier bank detail changes					
Expense claims					
Payroll changes					
Refunds and credit notes					
Sales contracts & revenue recognition					
Petty cash					
Procurement & purchase orders					

**How to use it.** Hold one 90-minute meeting with the FD, ops director, and head of finance. Fill the table in together. Date it. Both leaders sign it. Diarise the next review for three months from now.

COMPLETED

NEXT REVIEW

SIGNED (FD)

SIGNED (OPS)

## SECTION 03

# The delegation of authority matrix.

The single document procurement teams ask for most often. It says who can approve what, up to what value. Use this as a starting point and adapt the thresholds to the size of your business.

Spend category	Up to £1,000	£1,001 – £10,000	£10,001 – £50,000	£50,001 – £250,000	Over £250,000
Operating expenses	Team lead	Department head	FD	MD	Board
Capital expenditure	–	Department head	FD	MD	Board
Supplier bank detail changes	<i>Two-person verification required at any spend level</i>				
Payroll changes	<i>HR + FD approval required at any spend level</i>				
New supplier onboarding	Procurement lead	FD	FD + MD	Board	Board
Customer refunds & credit notes	Team lead	Finance manager	FD	MD	Board

A 60-person services firm and a 240-person manufacturer will have different bandings. What matters is that the matrix exists, that two people are required at every level above the lowest, and that the rules are *actually followed in practice*.

The matrix is only credible if your approval workflow **enforces** it. If approvers can be bypassed on email, or a single person can both raise and approve a payment, the document is window-dressing – and procurement teams will ask for a sample of approved invoices to prove the matrix operates in practice.

SECTION 04

# The implementation plan.

Six weeks if you treat it as a priority. Twelve at a more realistic pace. Owners, evidence, and what to put in the diary at each stage.

<p><b>01</b></p> <p>WEEK 1</p>	<p><b>Appoint an owner</b></p> <p>A single paragraph added to the job description naming responsibility for fraud prevention. That is the whole of step one.</p>	<p><b>WHO</b></p> <p>MD signs off · FD or Ops Director takes the role</p>	<p><b>EVIDENCE</b></p> <p>Updated job description, dated and signed.</p>
<p><b>02</b></p> <p>WEEKS 2-3</p>	<p><b>Run the risk assessment</b></p> <p>One 90-minute meeting using the template on page 05. Don't over-engineer it.</p>	<p><b>WHO</b></p> <p>FD leads; Ops Director, Head of Finance, Head of Sales attend</p>	<p><b>EVIDENCE</b></p> <p>Completed, dated, signed one-pager. Diary entry for next review.</p>
<p><b>03</b></p> <p>WEEKS 2-6 · IN PARALLEL</p>	<p><b>Tighten approval controls</b></p> <p>Document the matrix (p. 06). Then look honestly at how approvals actually happen – if they run on email, the matrix isn't being enforced. The fix is a workflow that hard-codes the matrix, timestamps every action, builds in segregation of duties, and requires two people for supplier-bank-detail changes every time.</p>	<p><b>WHO</b></p> <p>FD owns; Head of Finance executes</p>	<p><b>EVIDENCE</b></p> <p>Matrix document plus a sample of recent approvals showing the audit trail.</p>
<p>ApprovalMax is the workflow many of our customers use to satisfy this requirement – it enforces the matrix, builds in segregation of duties, and timestamps every approval into the audit trail procurement teams ask to see.</p>			
<p><b>04</b></p> <p>WEEKS 4-6</p>	<p><b>Write the three policies</b></p> <p>A fraud prevention policy, a whistleblowing policy, a supplier onboarding policy. One to two pages each. Circulate and ask for written acknowledgement.</p>	<p><b>WHO</b></p> <p>FD drafts · MD signs off</p>	<p><b>EVIDENCE</b></p> <p>Signed policies and the acknowledgement records.</p>
<p><b>05</b></p> <p>WEEK 6 ONWARDS</p>	<p><b>Schedule the reviews</b></p> <p>Recurring quarterly calendar entries for the FD and Ops Director to revisit the risk assessment, sample-check that controls are being followed, and log any incidents or near-misses.</p>	<p><b>WHO</b></p> <p>FD</p>	<p><b>EVIDENCE</b></p> <p>Diary entries plus a one-page log of each review's findings.</p>

## SECTION 05 · MODEL ANSWERS

# Eight questions a customer will ask.

Drawn from the six principles in the UK Home Office statutory guidance, translated into the form they typically appear on a procurement questionnaire. Answer in your own words – use these as a template.

## Q1 Who in your organisation has formal responsibility for fraud prevention?

### STRONG ANSWER

Our [\[Finance Director / name\]](#), who reports directly to the Managing Director, has formal responsibility for fraud prevention. The responsibility is written into the role's remit and was confirmed by the board on [\[date\]](#). Fraud prevention is a standing item on quarterly leadership meetings.

### WEAK ANSWER

*"Our finance team handles this." Vague, no name, no governance.*

## Q2 Do you have a documented fraud risk assessment? When was it last reviewed?

### STRONG ANSWER

Yes. Our current assessment is dated [\[date\]](#) and covers risks across invoice payments, supplier bank detail changes, expense claims, payroll, refunds, and revenue recognition. It is reviewed quarterly. We can share a redacted summary on request.

### WEAK ANSWER

*"We assess risk on an ongoing basis." Means no.*

## Q3 Describe your invoice approval process.

### STRONG ANSWER

All invoices are approved through [\[workflow / system name – e.g. ApprovalMax\]](#), which enforces our delegation of authority matrix. Approvers are determined by spend category and value. Segregation of duties is built into the workflow – the person raising a payment cannot approve it. Every approval is timestamped and the audit trail is retained for [\[X\]](#) years. We can provide a sample audit trail under NDA.

### WEAK ANSWER

*"Invoices are approved by the finance team before payment." Doesn't address thresholds, segregation, or evidence.*

## Q4 How do you handle changes to supplier bank details?

### STRONG ANSWER

Changes are verified by a phone call to a previously-known contact at the supplier, using a number we hold on file – not one provided in the change request. Two people are required to authorise the change in our system.

### WEAK ANSWER

*"We confirm changes before processing." Doesn't address out-of-band verification.*

SECTION 05 · MODEL ANSWERS CONTINUED

**Q5** What due diligence do you perform on new suppliers and employees?

**STRONG ANSWER**

New suppliers are checked against Companies House, sanctions lists, and adverse media before onboarding. New employees in finance, procurement, and sales roles undergo right-to-work and reference checks; for senior finance roles we also run a basic credit and criminal record check.

**WEAK ANSWER**

*"We carry out standard checks."  
Standard to whom?"*

**Q6** What anti-fraud training do staff receive?

**STRONG ANSWER**

All finance, procurement, and sales staff complete annual anti-fraud training. The most recent session was delivered in [month/year] and covered invoice fraud, payment redirection, and our whistleblowing process. Completion is logged. New starters complete the training within their first 30 days.

**WEAK ANSWER**

*"Staff are aware of our policies."  
Awareness isn't training.*

**Q7** Do you have a whistleblowing route? How is it communicated?

**STRONG ANSWER**

Yes. Staff can raise concerns confidentially via [route], which reports directly to [named role]. The route is communicated in the staff handbook, in annual training, and on a poster in the office kitchen. We received [X] reports in the last 12 months, all investigated and closed.

**WEAK ANSWER**

*"Staff can raise concerns with their manager." Manager-only routes don't satisfy the principle.*

**Q8** How do you monitor that controls are working in practice?

**STRONG ANSWER**

Exception reports – failed approvals, manual overrides, duplicate payment flags – are reviewed monthly by the Head of Finance. The full control framework is reviewed quarterly by the FD. Findings are logged and tracked to closure.

**WEAK ANSWER**

*"We review controls periodically."  
Periodically means never.*

Want the strong answer to Q3 to actually be true of your business? **ApprovalMax** delivers the documented, enforced approval workflow the model answer describes – the delegation matrix, segregation of duties, and timestamped audit trail.

## SECTION 06

# The internal conversation.

If you're an FD or Ops Director, the hardest part of this work is often not the controls – it's getting the MD or board to agree to invest the time. Three objections, three responses you can use almost verbatim.

## 01 | *"We're not in scope. Why are we doing this?"*

### RESPONSE

You're right that the offence doesn't apply to us – the thresholds are 250+ employees, £36m+ turnover, or £18m+ on the balance sheet. **But our largest customers are in scope.** The statutory guidance is explicit that they should push fraud-prevention requirements down their supply chain. We're already seeing this in the contract renewals coming in from *[largest customer]*. If we can't answer a refreshed supplier questionnaire confidently, we put those renewals at risk. This isn't a legal compliance project – it's a revenue protection project.

## 02 | *"This is overkill for a business our size."*

### RESPONSE

It would be, if we were aiming for what a FTSE 100 company runs. We're not. **The guidance says procedures should be proportionate** – a one-page risk assessment, a delegation of authority matrix, a workflow tool that enforces approvals, three short policies, and quarterly reviews. Two weeks of focused work, then a quarterly maintenance cycle. The cost of not doing it is losing a renewal we can't afford to lose.

## 03 | *"What if customers don't actually ask?"*

### RESPONSE

Some won't. **The largest ones will** – and they're the ones with the most leverage on price. We also gain something either way: the same controls that satisfy a customer questionnaire protect us from fraud committed against us, which is a real and rising threat to businesses our size. The work pays back regardless of whether the questionnaire ever arrives.

## SECTION 07

# What to do this week.

If you do nothing else after closing this document, do these four things in the next seven days. None requires a budget approval, a project plan, or a vendor selection. They surface the gaps – which is the only place the work can start from.

## 01

### Send the scorecard to your FD and Ops Director

Ask each to complete it **independently**. Compare answers. The disagreements are where to start.

## 02

### Diarise a 90-minute risk-assessment meeting

Within the next fortnight. Use the template on page 05. Walk out with the document **completed, dated, and signed**.

## 03

### Print a sample of recent invoice approvals

Are they all running through a documented workflow? Is there a timestamped trail? **If not, that's your highest-priority gap.**

## 04

### Identify your top three customer accounts by revenue

Find out when each is due for contract renewal. **Those are your hard deadlines.**

#### THE TAKEAWAY

**The next renewal is when this becomes real.**

The Failure to Prevent Fraud offence is now live. Supplier questionnaires are now in circulation. The work in this toolkit takes weeks, not months – but only if you start it now.

CLOSE THE STEP 3 GAP

# The approval workflow your customers will ask **to see.**

ApprovalMax gives you the enforced approval workflow, segregation of duties, and timestamped audit trail this toolkit describes – in software, ready to demonstrate to a procurement team.

## Answer Q3 of any supplier questionnaire **with evidence, not assurances.**

- **The delegation matrix is enforced automatically** – no exceptions, no email bypass, no single-person approvals.
- **Every approval is timestamped** into a defensible audit trail you can share with a procurement team under NDA.
- **Supplier bank-detail changes require two people** every time – out-of-band verification built into the workflow.

Connect your accounting system, build your first approval workflow, and walk into the next contract renewal with the audit trail already in hand.

[Start free trial →](#)[Book a demo](#)