RESOURCE GUIDE · HERMIT BUSINESS SOLUTIONS

Sarbanes-Oxley Principles for a Small UK Business

It's a US law that you don't have to follow but the habits behind it are worth borrowing ***anyway.***

Why this matters

The Sarbanes-Oxley Act (SOX) is a US federal law from 2002, written after the Enron and WorldCom scandals to stop company insiders lying about the numbers. It does that through four ideas: keep records that can be trusted, don't tamper with them, protect anyone who reports wrongdoing and make someone personally accountable for the accounts. SOX itself has no legal reach into a UK small business. It is American securities law. But those four ideas aren't American - they're just good financial discipline and UK law already covers a surprising amount of the same ground through other routes. This guide translates the principle into what a small UK business already has to do and what's worth doing anyway.

The same idea, the UK version

Each SOX principle has a UK law doing similar work, sometimes already binding on you, sometimes not (yet).

SOX principle	The UK equivalent for a small business
Keep records that can be trusted	Companies Act 2006 requires every UK company to keep accounting records that show and explain its transactions, for at least three years, six in practice because HMRC's tax rules require six.
Don't tamper with or destroy records	Already a criminal offence here too, under the Theft Act 1968, the Fraud Act 2006 and false accounting offences in the Companies Act 2006. No size threshold, it catches every business.
Protect staff who report wrongdoing	The Public Interest Disclosure Act 1998 already protects any worker who reports suspected fraud or wrongdoing, from day one, in a business of any size. Most small firms just don't have a policy written down.
Someone is personally accountable for the numbers	A director's duties under the Companies Act 2006 (s.172, s.174) already make you personally answerable for the accounts and personally liable if you keep trading while insolvent. Sole traders are obviously personally liable as the business and owner are one and the same legal entity.

SOX principle	The UK equivalent for a small business
Reasonable procedures to prevent fraud	New ground: since 1 September 2025, ‘failure to prevent fraud’ is a criminal offence for large organisations (roughly, two of: turnover over £36m, balance sheet over £18m, 250+ staff). Most small businesses fall outside it today but it shows the direction that UK law is moving in.
Independent testing of internal controls	Only required for public and large private companies. Small companies can claim audit exemption. This is the one part of SOX that genuinely has no UK small-business equivalent and doesn't need one. Internal controls are an important concept for efficiently operating a company even without a law.

Why bother if none of it is compulsory

Two rows in that table are already the law for the UK, whistleblower protection and the record-tampering offences, whether you've written a policy or not. The rest is genuinely optional for a small business. So why adopt any of it voluntarily?

Because the people who decide whether to lend to you, invest in you or buy your business increasingly expect to see it anyway. A bank renewing a facility, an investor doing due diligence before a funding round or a buyer's accountant going through your books before a sale, all move faster and trust the numbers more readily when they can see segregated duties, a written record-keeping habit and a clear paper trail. You're not filing anything with a regulator but you're building the kind of business that survives someone else looking closely.

A small business's path to control maturity

Most small UK businesses only need the first three tiers. Tier 5 is worth the cost once a sale, funding round or rapid growth toward the large-organisation thresholds is realistically on the horizon.

A QUICK REMINDER

We are not lawyers and this isn't a compliance obligation for most of the small businesses that we work with. What we do see is that the businesses that sail through a lender's or buyer's checks are the ones already doing tiers one to three above, as a habit, not as a scramble the week before year-end.

Where to start

- Open a dedicated business account and reconcile it monthly. Don't mix personal and business spending
- Split responsibility so that the person who approves a payment isn't the same person who raises or sends it
- Write down your record-keeping habit against the six-year HMRC rule and your approval limits, even a one-page policy beats none
- Put a short whistleblowing or 'speak up' policy in writing. You're covered by the law, most small firms just haven't written it down
- Get an outside set of eyes (an accountant or bookkeeper) to check your controls at least once a year
- If a sale, funding round or rapid growth toward 250 staff or £36m turnover is realistically on the horizon, start building fuller documentation well ahead of time, not the month due diligence begins