

Crime – Employee Fraud, Theft and Dishonesty - Fundamentals

The insider risk is often underestimated but poses a real threat to any organisation.

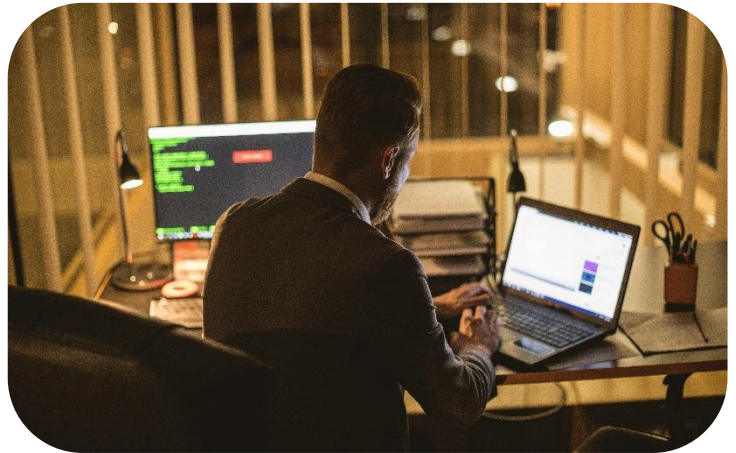
This Loss Prevention Standard highlights the key areas of risk to help support organisations

Crime – Employee Fraud, Theft and Dishonesty - Fundamentals

Introduction

Most organisations focus considerable effort on protecting themselves from the external threat of fraudsters, cyber criminals and organised crime groups. However, some of the most significant losses can originate from within the organisation itself.

Employee dishonesty and internal fraud occur when an employee, director, temporary worker, contractor or other trusted individual abuses their position for personal gain. This may involve the theft of money, stock, inventory, goods or other valuable assets. Whilst the vast majority of employees act honestly and responsibly, every organisation is exposed to some degree of internal fraud risk because business operations ultimately rely upon people, trust and access.



The impact of internal fraud often extends far beyond the immediate financial loss. Investigations can consume significant management time, disrupt operations, damage relationships with suppliers and customers, and create uncertainty amongst employees. In some cases, legal costs, disciplinary proceedings and recovery efforts may exceed the value of the original theft.

Fraud remains one of the UK's most significant crime challenges. According to Cifas, a leading UK fraud prevention organisation, fraud now accounts for approximately 41% of all recorded crime in the UK, whilst insider threats continue to present a persistent risk for organisations across multiple sectors¹.

One of the greatest barriers to effective fraud risk management is the belief that "it could not happen here". Organisations often take comfort from trusted employees, established procedures, a lack of previous incidents or controls that were strengthened following a past loss. Whilst these factors are important, none provide a guarantee against future fraud. Risks evolve as organisations grow, people move roles, responsibilities change and opportunities emerge.

Effective controls are an essential foundation for preventing employee dishonesty, but controls alone do not provide protection. Many organisations that suffer fraud losses already have policies and procedures in place. Real resilience comes from regular monitoring, testing and review of those controls to ensure they continue to operate effectively. The organisations most successful at preventing fraud are those that continually challenge existing arrangements, identify weaknesses early and adapt to changing risks.

¹ [\[cdn.prod.w...-files.com\]](https://cdn.prod.w...-files.com), [\[cifas.org.uk\]](https://cifas.org.uk)

When Internal Fraud Occurs

Most internal fraud does not occur because organisations employ dishonest people. More commonly, losses arise when opportunity, weak controls and inadequate oversight combine.

Many fraud investigations reveal an over-reliance on trusted individuals. Long-serving employees often accumulate significant knowledge, authority and autonomy within an organisation, and over time, managers may become less likely to challenge decisions, review transactions or question unusual activity. While trust is important in any business, trust alone should never replace effective controls.

Weak segregation of duties is another common factor. Problems arise when one individual can control an entire process, such as creating suppliers, approving invoices and authorising payments, or managing both physical stock and inventory records. Where independent oversight is limited, opportunities for fraud increase significantly.

Periods of organisational change can also create vulnerabilities:

- Rapid growth.
- Restructuring.
- Mergers and acquisitions.
- Staff turnover.
- Resource constraints.

By placing pressure on existing controls and reduce management oversight.

Employees rarely set out to commit fraud, however, changes in their personal circumstances such as financial pressures, increased debt, gambling issues, addiction or other events, may further increase the temptation to exploit weaknesses where opportunities exist.

Ultimately, fraud is most likely to occur where access, opportunity and insufficient challenge coexist.

Examples of Losses

Internal fraud can affect organisations in any sector and often exploits routine business activities that would not normally raise suspicion. Because fraudulent activity is frequently disguised as legitimate business transactions, losses can continue for months or even years before they are identified.

Payment Diversion. Payment diversion or theft of cash is one of the most common forms of internal fraud. Employees with access to financial systems may manipulate accounting records, delay reconciliations or create false journal entries to conceal missing funds. As the transactions often appear legitimate, the fraud can remain hidden until a review or investigation uncovers discrepancies.

- In 2025, [a UK finance manager was sentenced to imprisonment](#) after stealing approximately £185,000 from her employer through a combination of unauthorised company credit card spending and fraudulent invoices. The losses remained concealed until routine account reviews identified unusual transactions.

Stock and inventory Theft. This is another significant exposure, particularly within manufacturing, retail, warehousing and distribution operations. Losses may begin with the removal of small quantities of goods or materials, but repeated theft over an extended period can result in substantial financial impact. High-value products, tools, spare parts and raw materials are particularly attractive targets because they can often be resold easily.

- In June 2026, a group of employees were found guilty of conspiring with an external accomplice to [steal almost 49 tonnes of tin ingots valued at approximately £1.2 million](#). The fraud continued over a prolonged period and involved multiple employees abusing their trusted positions, knowledge of site operations, security arrangements and stock handling processes.

Supplier Collusion. Colluding with suppliers presents a further risk. This occurs when an employee works dishonestly with a supplier, contractor or other third party for mutual financial gain. Examples include accepting kickbacks for awarding contracts, approving inflated invoices, paying for goods that were never delivered or bypassing procurement procedures to favour a particular supplier. These schemes can be particularly difficult to detect because both parties may actively conceal the activity and create documentation that appears genuine.

- A facilities manager at a solicitors firm colluded with the director of a supplier and generated more than [£1 million of fake invoices over a three-year period](#). The employee controlled supplier relationships and invoice processing. The supplier director knowingly participated in the scheme. Fake companies were established and invoices submitted for work never performed. Both parties received prison sentences.

Procurement Fraud. This can arise where employees have significant purchasing authority and limited oversight. Common schemes include fictitious suppliers, duplicate payments, inflated invoices and undisclosed conflicts of interest. Weak supplier onboarding procedures and inadequate approval controls often contribute to these losses.

- In 2024, [an employee was jailed for fraudulently ordering IT equipment worth approximately £483,000](#), directing deliveries to personal addresses and selling the goods.

Payroll and Expenses Fraud. This continues to generate significant losses for many organisations. Examples include fictitious employees, manipulated overtime claims, duplicate expense submissions or personal expenditure disguised as business costs. Whilst individual transactions may appear relatively small, repeated abuse can accumulate into material losses.

- In 2026, [a UK payroll manager was convicted](#) after creating fictitious employees and arranging for salary payments to be directed into accounts under their control. The fraud exceeded £500,000 before it was discovered, highlighting the risks created when payroll records and payment processes are controlled by a single individual without independent oversight.

Theft or Misuse of Negotiable Instruments. Theft of such items, and other items with financial value, is another area of concern. Cheques, gift cards, vouchers and similar instruments may be vulnerable where physical security, access controls and monitoring arrangements are inadequate.

- In 2024, a finance manager at a UK business [manipulated company payment facilities and financial transactions, contributing to losses exceeding £300,000](#). Investigators noted that the fraud not only created significant financial loss but also placed considerable strain on company directors and threatened the financial stability of the business.

In many cases, the wider consequences of a fraud can be as damaging as the theft itself. Management distraction, legal costs, operational disruption, regulatory scrutiny and a breakdown of trust within teams can have long-lasting effects on the organisation.

How Internal Fraud Is Discovered

Contrary to popular belief, internal fraud is rarely uncovered through sophisticated investigations or advanced technology. More often, it is identified through routine management activities, audits, stock reconciliations, financial reviews or concerns raised by employees.

Whistleblowing remains one of the most effective methods of uncovering occupational fraud. Employees are often the closest to day-to-day operations and may notice unusual behaviour, control weaknesses or suspicious transactions long before management becomes aware of them. Organisations that encourage employees to raise concerns and provide confidential reporting channels are often better positioned to identify issues at an early stage.

Similarly, routine activities such as stock counts, compliance reviews, management reporting, bank reconciliations and supplier audits frequently expose irregularities that warrant further investigation.

Many frauds are discovered only when an employee takes annual leave, changes role or leaves the organisation altogether, allowing another individual to perform their responsibilities and identify issues that were previously concealed.

Whilst no single indicator proves dishonesty, organisations should remain alert to warning signs such as:

- Reluctance to take annual leave or share responsibilities.
- Excessive control over key processes.
- Resistance to oversight or independent review.
- Unexplained lifestyle changes.
- Inventory discrepancies or unexplained stock losses.
- Frequent accounting adjustments or write-offs.
- Missing documentation.
- Duplicate payments or unusual supplier activity.
- Repeated overrides of established controls.

The key lesson is that unusual activity should not be dismissed simply because it involves a trusted employee.

Actions to Reduce Internal Fraud Risk

While there is no single control capable of eliminating fraud risk, organisations can significantly reduce their exposure by focusing on a number of core areas:

Recruit Carefully and Screen Appropriately

Effective fraud prevention begins before an individual joins the organisation. Pre-employment screening should be viewed as a core fraud prevention control, particularly for roles involving access to money, procurement activities, stock, payments or valuable assets. Organisations should:

- Verify employment history and references.
- Investigate unexplained gaps in employment.
- Confirm qualifications and professional memberships.
- Verify identity and right-to-work status.
- Conduct criminal record checks where appropriate and legally permissible.
- Screen against relevant fraud prevention databases where available.

The use of artificial intelligence (AI) has also introduced new recruitment challenges. Organisations should be aware of AI-generated documents, deepfakes and synthetic identities designed to circumvent traditional screening processes. Enhanced identity verification and document authentication tools may help identify manipulated documents and AI-enabled deception. Enhanced verification may be as simple as an in-person meeting, rather than a virtual meeting to verify identity, or metadata analysis of ID documents, and independent sourcing of references and qualifications.

Higher-risk positions may also benefit from periodic re-screening during employment.

Segregate Responsibilities and Strengthen Controls

Few controls are more effective than ensuring no single individual has complete control over a transaction or business process. Organisations should:

- Separate supplier setup, invoice approval and payment functions.
- Independently review payroll amendments.
- Require dual authorisation for higher-value transactions.
- Regularly reconcile bank accounts and key balance sheet accounts.
- Monitor unusual transactions, refunds and write-offs.

Fraud often occurs when one individual can initiate, approve and conceal a transaction without challenge.

Protect Stock, Assets and Financial Resources

Financial losses are not limited to cash. Good practice includes:

- Regular stock takes and cycle counts.
- Investigation of all significant discrepancies.
- Restricted access to high-value goods or assets.
- Appropriate CCTV and physical security measures.
- Independent review of stock adjustments and write-offs.

Organisations should pay particular attention to assets that are portable, valuable and easily resold.

Manage Third-Party and Supplier Risks

Suppliers, contractors and outsourced service providers can introduce additional fraud exposures if relationships are not effectively managed. Organisations should:

- Undertake appropriate due diligence before engagement.
- Maintain clear procurement procedures.
- Monitor supplier activity and payment patterns.
- Require conflicts of interest to be disclosed.
- Periodically review higher-risk supplier relationships.

Effective management of third parties does not end at onboarding; ongoing monitoring and oversight are essential.

Encourage Challenge, Reporting and Independent Review

Many frauds are identified because someone questioned unusual activity. Organisations should:

- Deliver regular fraud awareness training and keep employees up to date on emerging fraud risks, red flags and reporting expectations.
- Maintain confidential reporting and whistleblowing arrangements.
- Investigate concerns consistently and fairly.
- Conduct regular audits and compliance reviews.
- Review high-risk transactions and exception reports.
- Test the effectiveness of existing controls periodically.

The ability to detect fraud quickly can be just as important as preventing it. Regular, up-to-date fraud awareness training can help employees recognise evolving fraud techniques, understand their role in fraud prevention, and identify suspicious activity before losses escalate. Maintaining awareness is an important complement to formal controls and oversight.

Key Takeaways

Employee dishonesty is a risk faced by organisations of every size and sector. Whilst strong controls remain essential, experience shows that fraud is often enabled not by the absence of controls, but by a failure to monitor whether they remain effective.

Most frauds exploit routine business processes and weaknesses in oversight rather than sophisticated criminal techniques. Recruitment screening, segregation of duties, supplier governance, whistleblowing arrangements and regular independent review all play an important role in reducing exposure.

Ultimately, the most resilient organisations are those that recognise fraud prevention as an ongoing process rather than a one-time exercise. By combining strong controls with effective monitoring, challenge and oversight, organisations can significantly reduce opportunities for fraud and improve their ability to detect issues before they develop into significant losses.

Contact Information

Canada

Please visit [Aviva Risk Management Solutions | Aviva Canada](#) or email us at arms.canada@aviva.com

Ireland

Please visit [Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland](#) or Email us at armsireland@aviva.com

United Kingdom

Please visit [Aviva Risk Management Solutions](#) or email us at riskadvice@aviva.com. To speak to one of our advisors, call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Aviva have created a network of Specialist Partners to complement our in-house capabilities and to enable our policyholders to benefit from a wide range of risk management solutions at preferential rates and terms. Together, we provide solutions to help with the significant challenges of modern-day risk management.

Note: These partner relationships are wholly for the benefit of our policyholders with no income to Aviva.

Canada

For more information please visit: [Our Specialist Partner Network | Aviva Canada](#)

Ireland

For more information please visit: [Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland](#)

United Kingdom

For more information please visit: [Aviva Risk Management Solutions - Specialist Partners](#)

Standards, Sources and Useful Links

Canada

- [Canadian Anti-Fraud Centre](#)
- [National Cybercrime and Fraud Reporting System](#)

Ireland

- [National Cyber Security Centre](#)

United Kingdom

- [Credit Industry Fraud Avoidance System \(CIFAS\)](#)
- [National Fraud Intelligence Bureau](#)
- [UK Finance Fraud Report 2026](#)
- [FraudTrack 2025 | UK Fraud News - BDO](#)
- [CIFAS Guide - Prevent Fraud for Organisations | Private, Public and Charity](#)

Other

- [Internet Crime Complaint Center](#)

Loss Prevention Standards

These documents set out best practice recommendations to help reduce the likelihood and impact of losses.

Relevant Aviva Loss Prevention Standards include:

- **Payee Verification Policy**
- **Social Engineering fundamentals**
- **Social Engineering Fraud – Sim-swap and Ghost-pairing**
- **Crime – Mergers & Acquisitions Exposures**
- **Cyber – Mergers & Acquisitions Exposures**

Please visit [Loss Prevention Standards](#) to view the full library.

Aviva Risks Training Solutions (United Kingdom Only)

Aviva Risk Training Solutions, delivered through our Specialist Partner, SafetyCulture, provide free, bite-sized learning modules exclusively for Aviva policyholders.

Relevant courses include:

- **Social Engineering**

Please visit [Aviva Risk Training Solutions](#) for further guidance.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. By extension, any links to third-party websites do not constitute marketing by Aviva and are included solely for the reader's information and educational purposes. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

7th October 2026

Version 1.0

ARMSGI5212026

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.

Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.