Overview of the role

Safeguarding an organization's assets, reputation, and trust by identifying and analysing potentially fraudulent activities.

Contents

[Hide menu](#)

Standard in development
L4: Fraud Control Specialist
Version 0.0

Title of occupation

Fraud Control Specialist

UOS reference number

ST1445

Core and options

No

Level of occupation

Level 4

Occupational maps data

Route: Protective services
Pathway: Protective services
Cluster: Protective service manager

Typical duration of apprenticeship

24 months

Target date for approval

31/10/2025

Resubmission

No

Would your proposed apprenticeship standard replace and existing framework?

No

Does professional recognition exist for the occupation?

No

Regulated occupation

Is this a statutory regulated occupation?

No

Occupational summary

This occupation is found in organisations within each sector of the UK economy, the UK Public, Private and Voluntary Sectors. In the context of this Fraud Control Apprenticeship the use of the word 'Fraud' is used to include the offences of Bribery and the wider conduct that may be classified as corrupt activity. Economic crime refers to a broad category of activity involving money, finance or assets, the purpose of which is to unlawfully obtain a profit or advantage for the perpetrator or cause loss to others. It covers an array of offences which include fraud, bribery, corruption, embezzlement, false accounting, insider dealing, intellectual property fraud, forgery, counterfeiting, money laundering, tax evasion and benefit fraud.

The spread of fraud to all sectors of the UK economy, and the legislative need by qualifying organisations to have procedures in place to prevent fraud, bribery and the facilitation of tax evasion means that a coordinated programme of work must be in place to minimise the effect of these crimes. Fraud, and other forms of economic crime, are not confined to specific industries or economic areas and therefore this apprenticeship has relevance to a wide range of workplaces and applications.

The broad purpose of the occupation is to complement an organisation's existing corporate governance arrangements. Corporate Governance is designed to direct and control an organisation's operations in such a way that they deliver their strategic and operational objectives lawfully, ethically, effectively and efficiently. In particular, Fraud Control Specialists will apply expert knowledge, skills and behaviours to enhance an organisation's internal control framework. In doing so, it will address a significant and growing threat - fraud loss. Traditionally, this has in part been delivered through fraud prevention specialists. However, changes in the professional and legal landscape have necessitated a more multi-disciplinary approach to counter fraud management. This involves the creation, and maintenance of a counter fraud culture, effective fraud prevention, fraud deterrence, fraud detection and fraud measurement.

In their daily work, an employee in this occupation interacts with a wide range of internal and external stakeholders. This is essentially an outward facing role and much of a Fraud Control Specialist's time will be spent working with other parts of their employing organisation. Key departments that they may come into contact with include human resources, procurement, finance, risk management, information technology, data protection and information services, internal and external audit, operational delivery and corporate governance. Some organisations contract out certain services. Fraud Control Specialists will therefore need to liaise with, and work alongside, core suppliers and contractors. Fraud Control Specialists will be expected to deliver prearranged specific tasks, either individually or as a part of a team. They will need developed interpersonal skills to build and maintain relationships with these groups and be able to present the results of their work to them; and to senior staff and other parts of the organisation and partner bodies as needed.

An employee in this occupation will be responsible for participating in the delivery of all aspects of Fraud Control which means that they will need significant influencing and drafting skills to deliver their duties effectively. They will also be working with specialists to identify and manage cyber and other technology related threats. In this respect they will also need to be familiar with the opportunities and risks associated with artificial intelligence. While this undoubtedly has significant benefits, it can be used to commit fraud by creating malware; generating false information; forging documents; generating counterfeit data which bypasses existing security measures; and, by creating false identities. Fraud is a fast-moving field in which fraudsters are continually adapting their modus operandi to circumvent controls and other security measures designed to protect corporate and personal assets and finances. Fraud Control Specialists therefore need a flexible approach to their work, modifying their procedures in the light of changing circumstances and being able to adapt to new technologies and processes as required.

Typical job titles

Counter fraud and risk business partner Financial crime manager Fraud prevention officer Global director integrity, ethics and counter fraud Senior proactive counter fraud response officer

Are there any statutory / regulatory or other typical entry requirements?

No

Occupation duties

Duty	KSBs
Duty 1 Uphold organisational values and ethical standards and frameworks and develop and maintain a strong counter fraud culture.	K1 K2 S1 S2 B1 B2 B3 B4 B5 B6
Duty 2 Work constructively with stakeholders and counter fraud professionals to deliver all aspects of fraud control.	K1 K2 K3 K4 K5 K6 K7 K8 K9 K10 K11 K12 K13 K14 K15 K17 K26 S2 S3 S4 S5 S6 S7 S8 S9 B1 B2 B3 B4 B5 B6 B7
Duty 3 Support the development of fraud risk management and assist in the delivery of	K18 K19 S10 B6

Duty	KSBs
risk assessments.	
Duty 4 Apply counter fraud measures and support an organisation to integrate these within internal control structures and systems.	K6 K7 K8 K9 K10 K11 K13 K16 K20 K21 K22 K23 K24 K25 K27 K28 K31 S11 S12 S13 S14 B6 B7
Duty 5 Liaise with, and support, operational teams in the development of internal controls, and detection routines, to address fraud risk.	K1 K2 K3 K4 K5 K6 K7 K9 K10 K11 K12 K13 K14 K15 K16 K18 K19 K20 K21 K22 K23 K26 K28 K29 K30 K31 K32 S1 S4 S5 S6 S7 S8 S10 S15 S16 S17 S18 S19 S20 S21 S25 B1 B2 B3 B4 B5 B6 B7
Duty 6 Support an Organisation to implement their counter fraud policy, response plan and protocol document and the proactive	K1 K2 K6 K7 K8 K9 K10 K11 K12 K13 K14 K15 K17 K20 K21 K22 K23 K24 K25 K26 K27 K28 K29 K30 K31 K32 K33 S1 S21 S22 B1 B2 B3 B4 B5 B6 B7

Duty	KSBs
and reactive tasks to prevent fraud.	
Duty 7 Contribute to, and promote, activities which are designed to measure the level of fraud in organisations.	K11 K13 K16 K20 K25 K27 S14 S23 B6
Duty 8 Contribute to the production of Initial Fraud Impact Assessments for proposed policies, programmes, projects, systems and procedures prior to live use.	K6 K10 K13 K14 K15 K23 K28 K29 K30 K32 S15 S16 S24 B1 B2 B6 B7
Duty 9 Work collaboratively to review policies, programmes, projects,	K1 K3 K4 K5 K6 K7 K9 K10 K12 K14 K15 K23 K29 K32 S6 S8 S19 B1 B2 B3 B4 B6 B7

Duty	KSBs
systems and procedures that have been subject to fraud to strengthen them and minimise the likelihood of recurrence.	
Duty 10 Work with counter fraud colleagues, law enforcement and other agencies to disrupt ongoing frauds.	K10 K11 K22 K28 K31 S11 B6 B7
Duty 11 Liaise with, and support, Information Technology and Cyber Specialists to assist in the management of digitally enabled fraud risks.	K3 K4 K5 K6 K10 K12 K14 K15 K16 K18 K19 K22 K23 K26 K29 K32 S20 S25 B2 B3 B4 B6 B7
Duty 12 Liaise with, and	K1 K3 K4 K5 K6 K7 K9 K10 K12 K14 K15 K16 K18 K19 K22 K23 K26 K32

Duty	KSBs
support, those parts of the organisation outside of counter fraud, whose activities contribute to the management of fraud risk.	S18 S20 S25 B1 B2 B3 B4 B6 B7
Duty 13 Develop and deliver fraud awareness programmes across an organisation, their supply chain and other external stakeholders.	K1 K2 K3 K4 K5 K6 K7 K8 K9 K10 K11 K12 K13 K14 K26 S2 S3 S4 S5 S6 S7 S8 B1 B2 B3 B4 B5 B6 B7
Duty 14 Contribute to reviews, audits, and assessments of the extent to which counter fraud policies and practices are being complied with	K1 K2 K3 K4 K5 K6 K7 K8 K9 K10 K12 K13 K14 K15 K16 K17 K18 K19 K20 K21 K23 K25 K26 K27 K28 K29 K30 K31 K32 K33 S6 S9 S14 S15 S16 S17 S24 S26 B1 B2 B3 B4 B5 B6 B7

Duty	KSBs
across the organisation.	
Duty 15 Undertake continuous professional development and maintain a record of the learning achieved.	K34 S27 B6

KSBs

Knowledge

K1: Legislation and organisational policies relating to equity, diversity and inclusion in the workplace.

K2: Key legislation affecting all fraud control operations: the Computer Misuse Act 1990, The Employment Rights Act 1996, in relation to protected disclosures, The Human Rights Act 1998, The Public Interest Disclosure Act 1998, The Freedom of Information Act 2000, The Proceeds of Crime Act 2002, The Fraud Act 2006, The Serious Crime Act 2007 - ss 68-72, The Equality Act 2010, The Identity Documents Act 2010, The Bribery Act 2010, The Enterprise and Regulatory Reform Act 2013, in relation to protected disclosures, The Criminal Finances Act 2017, The Digital Economy Act 2017, The Data Protection Act 2018 and The Economic Crime and Corporate Transparency Act 2023.

K3: The roles and responsibilities of internal and external stakeholders and partner organisations.

K4: The importance of building and maintaining internal and external professional relationships and the impact these can have on an organisation's counter fraud culture.

K5: The techniques for building and maintaining internal and external professional relationships: Positively Influencing Others, Active Listening, Information Delivery, Negotiation, Conflict Management, Diversity Issues and Memoranda of Understanding.

K6: Fraud, Bribery and Corruption, their relationship to one another, their scale and impact, how these are managed in the UK, and how these affect both personal and organisational finances and assets.

K7: How fraud, bribery and corruption control is embedded within an organisation's Governance and other activities.

K8: How the terms prevention and deterrence differ and why both are important to fraud control.

K9: Principles of good governance, governance structures and fraud control oversight: two-way communication channels, an accountable board level risk owner and structures for dissemination of policies, information and decisions.

K10: Theories explaining why people commit fraud, bribery and corruption and the countermeasures to tackle these: motivation, opportunity, pressure, capability and personal integrity.

K11: The indicators that show fraud, bribery and corruption are present and how to manage false positives.

K12: Approaches to educate staff and other stakeholders on how to spot and deal with fraud, bribery and corruption and other forms of economic crime.

K13: How personal observation, data analysis, and technology are used to detect fraud, bribery and corruption.

K14: How to use software packages to maximise understanding of intended purpose to meet planned objectives: digital documents, spreadsheets, databases and presentations.

K15: How to research a subject, identify and prioritise the key issues, summarise these cogently and concisely and produce workable recommendations.

K16: The different sources of data, analysis and reporting on fraud, bribery and corruption and other forms of economic crime, and the strengths and weaknesses of each.

K17: The term "Best Practice", and how this applies to Fraud, Bribery and Corruption Management.

K18: The Fraud Risk Lifecycle and how it is used by organisations for fraud, bribery and corruption control.

K19: How a Fraud, Bribery and Corruption Risk Assessment is created and incorporates an organisation's fraud risk appetite and tolerance to fraud.

K20: The different approaches to deter fraud, bribery and corruption using fraud detection and preventative techniques: internal controls, victim management, local and national campaigns, protected disclosure policies and software.

K21: The term "Fraud Health Check" and what this entails and how this is implemented across an organisation.

K22: The term enabler, the different types of enablers, how enablers facilitate fraud, bribery and corruption and other forms of economic crime and how enablers can be disrupted.

K23: The techniques needed to perform a review of a specific system or process having regard to the three lines of defence mode: controls, managers and internal audit.

K24: The Crime Reduction Planning process.

K25: How data from system and procedure reviews, combined with data analytics, can be used to measure the level of fraud, bribery and corruption and other forms of economic crime, within an organisation.

K26: How organisations prevent fraud, bribery and corruption threats from own staff and from third parties including pre-employment vetting and due diligence checks on third parties.

K27: The procedures used to measure the effectiveness of fraud, bribery and corruption prevention and detection activities within a defined timescale.

K28: How counter fraud knowledge can be applied to the design of new policies, programmes, projects, systems and procedures.

K29: The different approaches and technologies employed to counter cyber and other digitally related fraud, bribery and corruption threats including artificial intelligence.

K30: The purpose and content of an Initial Fraud, Bribery and Corruption Impact Assessment and its role in fraud management.

K31: How to implement the Fraud, Bribery and Corruption Prevention and Deterrence End to End Process.

K32: The digital platforms and electronic devices used by organisations, the cyber enabled threats they face and how these are exploited by fraudsters.

K33: The content of the Counter Fraud, Bribery and Corruption Policy, Response Plan and Protocol document and the role they have in fraud management within an organisation.

K34: The use of reflective practice theories and techniques to inform professional development of an individual and improve approaches to practice.

Skills

S1: Follow legislation and policies that support and promote equity, diversity and inclusion in the workplace.

S2: Promote high standards by following legislation, Codes of Practice and organisational policies that support the behaviours and working practices expected from fraud, bribery and corruption control professionals.

S3: Build, maintain and manage working relationships with stakeholders and partners to meet both organisational and team objectives.

S4: Apply influencing techniques to achieve fraud, bribery and corruption control goals and objectives. This will include managing challenging communications using language and style that reflect the situation and audience.

S5: Create and deliver presentations using communication skills and strategies to maximise understanding of the need to manage fraud, bribery and corruption amongst all stakeholder groups.

S6: Communicate financial and other information succinctly and clearly meeting the needs of the target audience when using verbal and written reports and spreadsheets.

S7: Use IT software packages to communicate with, and support, partner organisations, regulators and senior management: word processing, spreadsheet, presentation and database software packages.

S8: Work with stakeholders to arrive at agreed solutions to identified issues and problems and avoid conflict.

S9: Form judgements that are: rooted in evidence and based upon critical thinking; unbiased; and can withstand challenge.

S10: Complete a fraud, bribery and corruption risk assessment.

S11: Implement and maintain the measures needed to deter, detect, prevent and disrupt fraud, bribery and corruption and counteract the motives to commit these offences.

S12: Recommend and implement changes to fraud, bribery and corruption processes and controls which improve an organisation's governance arrangements.

S13: Measure an organisation's fraud, bribery and corruption losses and develop a crime reduction plan for an organisation, tailored to its specific fraud and economic crime offence needs, to tackle these.

S14: Use data analytics in support of fraud, bribery and corruption prevention, measurement, detection and deterrence objectives.

S15: Implement a system or procedure review.

S16: Prepare Initial Fraud, Bribery and Corruption Impact Assessments.

S17: Apply appropriate fraud, bribery and corruption management methodologies to control failures and other system weaknesses.

S18: Work collaboratively as a part of a team and, in doing so, be aware of the impact on others.

S19: Review policies, programmes, projects, systems and procedures that have been subject to fraud, bribery or corruption or present an elevated risk of fraud, bribery and corruption.

S20: Provide advice to other parts of the organisation about the identification, management and control of fraud, bribery and corruption risks.

S21: Follow legislation and policies that are relevant to particular fraud, bribery and corruption control tasks.

S22: Deliver all aspects of the fraud, bribery and corruption prevention process as specified in the annual fraud, bribery and corruption prevention plan.

S23: Detect fraud bribery and corruption when using relevant indictors and relevant detection techniques.

S24: Produce Initial Fraud, Bribery and Corruption Impact Assessments for new policies, programmes, projects, systems and procedures.

S25: Liaise with internal departments that provide counter fraud, bribery and corruption services such as pre-employment vetting, due diligence checks and cyber security management.

S26: Produce a fraud, bribery and corruption health check for an organisation.

S27: Engage in self-reflection, feedback and professional development activities to improve own professional practice.

Behaviours

B1: Display the behaviours and standards expected when undertaking official responsibilities and dealing with others: acting objectively, openly and honestly at all times while respecting the values and views of others.

B2: Act with confidence and integrity.

B3: Embrace and value equity, diversity and inclusion, treating everyone with dignity and respect.

B4: Comply with codes of conduct for own role.

B5: Challenge unsafe or inappropriate behaviours and practices.

B6: Be a reflective and resilient practitioner.

B7: Display a stakeholder focussed mindset which drives service delivery.

Qualifications

English and maths

English and maths qualifications must be completed in line with the [apprenticeship funding rules](#).

Does the apprenticeship need to include any mandated qualifications in addition to the above-mentioned English and maths qualifications?

No

Consultation

Progression routes

[ST0556 Improvement leader L6](#)

[ST0385 Operations or departmental manager v1.2 L5](#)

[ST1322 Resilience and emergencies professional v1.0 L6](#)

Management Consultant Level 6

Supporting uploads

Mandatory qualification uploads

Mandated degree evidence uploads

Professional body confirmation uploads

Involved employers

Defra, Lambeth Local Authority, First Connect, Oxfam GB, Ernst and Young, The Post Office, Allianz / LV Insurance, Aviva Insurance, Insolvency Service, Her Majesty's Revenue and Customs, Department for Work and Pensions, Kent County Council and the National Health Service.

Other involved stakeholders

Subject sector area

1.4 Public services