COUNTER FRAUD AND ENFORCEMENT UNIT

FRAUD COMPLIANCE REPORT

Forest of Dean District Council
Cotswold District Council
West Oxfordshire District Council
Tewkesbury Borough Council
Cheltenham Borough Council
Stroud District Council

Introduction

The Counter Fraud and Enforcement Unit (CFEU) Fraud Risk Strategy was adopted by the partner Councils in 2022. As part of this strategy, the CFEU has committed to assessing the Councils' compliance with the fraud risk assessment checklists outlined in the Fighting Fraud and Corruption Locally (FFCL) 2020[1] strategy and the Government Functional Standard for Counter Fraud (GovS013)[2].

Another objective is the development of organisational and service-specific fraud risk registers. Widely recognised as a key component of a robust governance framework, the registers will help the organisation better understand its vulnerabilities to fraud and error, the likelihood of such fraud being realised, and the potential impact on the organisation. By identifying these vulnerabilities, the Councils can implement effective controls and allocate resources to prevent fraud or mitigate its likelihood and impact should it occur.

Fraud Risk

Fraud risk can be defined as a 'situation in which a Local Authority is exposed to the potential for financial loss due to wrongful or criminal deception'. Identifying fraud risk is essential for understanding specific vulnerabilities, evolving patterns in fraud and corruption threats, and the potential consequences for the Councils. While intent (dishonesty) is a key factor in determining fraud, it may not always be evident or possible to prove. To protect public funds, the Council considers the risk of error alongside the risk of fraud during the fraud risk assessment process. Therefore, references to fraud risk should also encompass the risk of error, which accounts for losses where there is insufficient evidence to establish intent.

Fraud Risk Assessment

The purpose of a fraud risk assessment is to proactively identify an organisation's vulnerabilities to fraud from both internal and external perpetrators. Each fraud or loss scenario is evaluated against the likelihood of its occurrence and the potential impact on the organisation in the absence of any controls (inherent risk). Internal controls are then implemented to eliminate the organisation's vulnerabilities to fraud and error. Where vulnerabilities cannot be eliminated, control measures should aim to mitigate the likelihood of fraud occurring and its impact on the organisation to an acceptable level of tolerance (residual risk). The process can be broken down into the following four risk steps:

[1] Fight Fraud and Corruption Locally

[2] Gov S013 - Counter Fraud

Identification: Research, identify, and record known and potential/hypothetical fraud risks.

Analysis: Assess the level and likelihood of risk occurrence.

Evaluation: Evaluate potential consequences, outcomes, and exposure to inherent risks.

Response: Implement controls or mitigation strategies for identified risks and evaluate residual risk.

Accurately assessing risk is a professional exercise that demands knowledge of fraud methods and risk management processes. Risk identification is a creative process that requires a mindset oriented toward defrauding the system. Therefore, it is crucial that fraud risk assessments involve engagement and collaboration among counter-fraud professionals, internal audit teams, and representatives from various service areas, all of whom should have a thorough understanding of their processes and systems. Risk assessment exercises should be conducted regularly and viewed as an ongoing process rather than a one-time task. This approach ensures that new and emerging risks, as well as changes in the risk levels of known risks, are identified, assessed, and reflected in the risk register accordingly.

A 5x5 heat map matrix is used to assess fraud risk based on both likelihood and impact. Values ranging from 1 to 5 are assigned to the likelihood of the inherent risk being realised and the perceived impact on the organisation should the fraud or error occur. The risk score is calculated by multiplying these values (impact x likelihood), which determines the priority for addressing the risk within the organisation. Government professional standards recommend at least four response levels for the process to be effective. It is essential to agree on impact definitions and to subdivide actions and responses within the risk rating categories where necessary. For example, the response for risk ratings of 16 to 20 will differ from that for a rating of 25.

Heat Map Matrix

Risk Rating	**Value**
Immediate Priority	**16 - 25**
High Priority	**12 - 15**
Medium Priority	**5 - 8**
Low Priority	**1 - 4**

			Risk				
Impact	Critical	5	5	10	15	20	25
	Severe	4	4	8	12	16	20
	Major	3	3	6	9	12	15
	Moderate	2	2	4	6	8	10
	Minor	1	1	2	3	4	5
			1 Very low	2 low	3 Medium	4 High	5 Very High
			Likelihood				

Fraud Risk Register

The fraud risk registers provide a comprehensive overview of all known fraud risks to the organisation and the controls in place to mitigate those threats. It is a live document, subject to ongoing review by the CFEU in collaboration with relevant lead officers / heads of service. The register enables service areas and managers to monitor and understand known fraud risks and vulnerabilities within their domains, guiding future audit and counter-fraud efforts to enhance fraud prevention measures. The register will:

- Satisfy a key principle outlined in the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption[3].
- Ensure compliance with counter-fraud best practices as specified in the FFCL and GovS013.
- Complement and support the positive counter-fraud initiatives already implemented across the Councils.

Compliance with Fighting Fraud and Corruption Locally (FFCL) Strategy and Government Standard (GovS013)

The FFCL serves as the counter-fraud and corruption strategy for local government, while GovS013 outlines the central government standard for managing fraud, bribery, and corruption risks, both the FFCL and GovS013 include an organisational-level fraud risk

[3] CIPFA Code of practice on managing the risk of fraud and corruption

assessment/checklist. The Councils have used the FFCL checklist to evaluate their compliance with the best practice and guidelines established by local government and counter fraud experts. The table at Appendix 1 details the Council's current compliance status with the FFCL strategy, categorised as compliant, partially compliant, or non-compliant, with the recommendations outlined in the FFCL. Justifications for the assigned compliance scores are included, along with the Council's plans to achieve full compliance.

The GovS013 basic organisational checklist is not included because its requirements are either specifically targeted at central government or are already comprehensively covered in the FFCL checklist. However, the CFEU plans to conduct a broader review of the GovS013 checklist to assess its compliance with central government requirements as part of its application to become an accredited member of the Public Sector Fraud Authority[4].

[4] Public Sector Fraud Authority