Counter Fraud Policy Guidance

BON ACCORD

ABERDEEN
CITY COUNCIL

Document Control

Approval Date	27/11/2025
Implementation Date	01/12/2025
Policy Number	POL-R-0003
Policy Author/s and Owner	Author: Matthew Dickson Owner: Chief Officer - Finance
Approval Authority	Audit, Risk and Scrutiny Committee
Scheduled Review	Biennial (2027)
Date and Changes: 12/09/2025 – Policy has been largely rewritten from the 2021 version to include obligations under specific legislation; to cover ALEOs and associated bodies; to assign specific responsibilities to Chief Officers; to require all future policies and procedures to evidence that fraud risks have been considered in their development; and to outline the way in which ACC manages fraud risk.	

Table of Contents

1 Introduction

The purpose of this document is to provide useful background and additional operational guidance to the Counter Fraud Policy (2025).

1.1 What is Fraud?

For the sake of simplicity, fraud in this document is used as an umbrella term which captures:

- Fraud
- Bribery
- Corruption
- Tax evasion
- Money laundering
- Embezzlement
- Any other illicit, acquisitive act committed against the council by a third party

This includes attempts at any of the above. These actions can be committed by both internal actors (e.g., employees, members and school staff) and external actors (e.g., members of the public, service users or suppliers).

1.2 Context

As a local authority, Aberdeen City Council has numerous legal obligations, including requirements to effectively manage budgets and spending whilst obtaining best value. Over the last thirty years, the UK public sector, including ACC, adopted the risk management tools used by the private sector. We now operate the Three Lines of Defence model (3LoD) across the Council and employ the standard suite of risk management tools (policy, risk appetite statement, multiple risk registers). This structure is reinforced with procedural controls and corporate policies, reviewed by Internal and External Audit, and overseen by relevant officers and Council committees. The overall stance of the Council is that it is averse to fraud risks.

As we saw with the incorporation of risk management into public sector planning, it is now recognised that there is a need for a systematic approach to fraud risk across local authorities. This is perhaps driven by the continual pressure on public spending and the increased prevalence of fraud, as measured by the UK Government, Police agencies and professional bodies. The recognised tools in managing fraud risk were also first developed by the private sector, particularly the regulated financial services. Further impetus has been provided by the introduction of Part 5 of the Economic Crime and Corporate Transparency Act

2023, which came into force in September 2025. Should any person employed by, or associated with, the Council commit a fraud offence which happens to benefit the Council in any way, the Council could be held liable for a separate offence of failing to prevent that fraud. An associated person under this legislation can be an agent, contractor, a subsidiary company, or an ALEO. The statutory defence against this charge is comprehensive management of fraud risks evidenced in top-level commitment, proportionate risk-based fraud prevention procedures, due diligence, communication, and monitoring & review. The Counter Fraud Policy places a duty on staff to demonstrate that they have assessed the risk of fraud within their business areas and processes. This includes when considering new projects or writing new policies.

2 Fraud Risk Management Framework

The Fraud Risk Management Framework exists within the above assurance and governance context and is comprised of a structure and processes. A new Integrity Group composed of officers from various Council services will monitor and review the administration of a Fraud Risk Register (FRR), which itself is informed by information from Council teams and Counter Fraud in the form of Fraud Impact Assessments (FRA), Initial Fraud Impact Assessments (IFIA), as well as data from other sources. Fraud risks are managed by the relevant risk owners, with support from Counter Fraud. The Integrity Group reports its activities to Risk Board, which also serves as the final escalation point when progress is blocked for any reason. Figure 1 shows a simplified structure, including the flow of information depicted by the blue arrows.

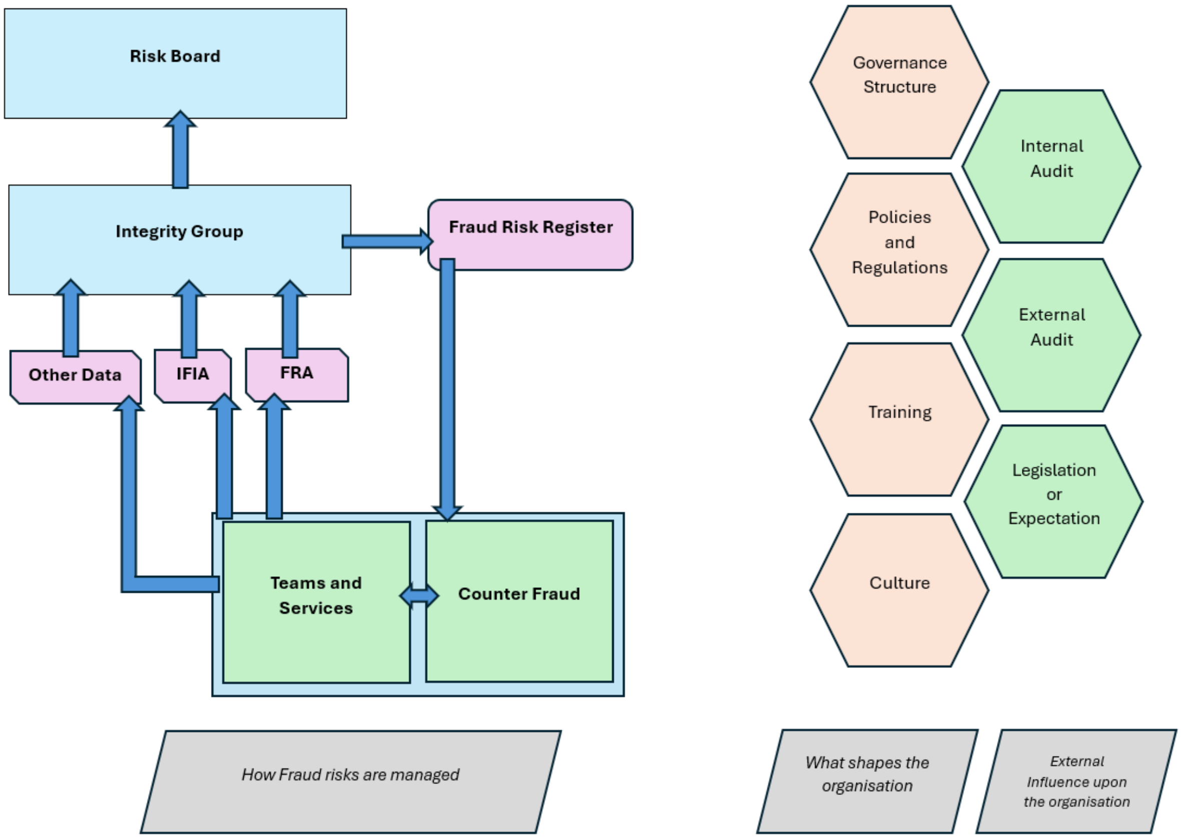


Figure 1, Risk Management Framework and context

2.1 Fraud Risk Management Documents

This policy creates two documents to be used throughout the Council. The first is the **Initial Fraud Impact Assessment (IFIA)**. Current best practice is exemplified in the guidance from the UK Government Public Sector Fraud Authority, and we draw from that guidance here. The IFIA is used at the scoping stage of a project, business case, or when considering spending as part of a scheme, in order to capture fraud-related impacts at a high level. The Senior Responsible Officer (SRO) involved in the project is responsible for completion of the IFIA.

Using the IFIA to proactively identify fraud impacts enables discussion with stakeholders and counter fraud officers to prioritise spend areas or project stages which require the greatest attention in order to reduce fraud impact. An example is attached at Appendix 1.

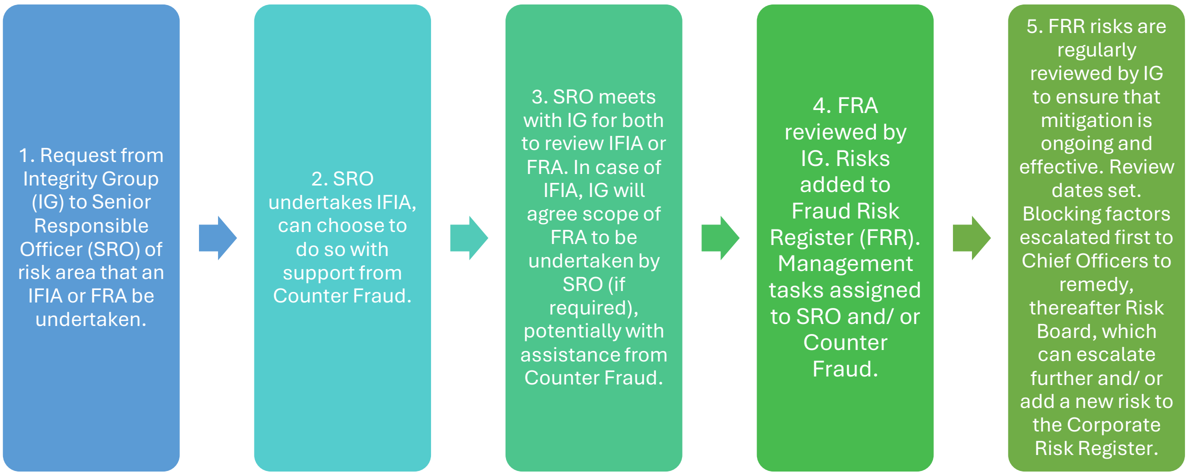
The second document is the **Fraud Risk Assessment (FRA)**. The data used to inform the FRA can come from the IFIA, horizon scanning, experience or knowledge. The purpose of the FRA is to capture specific risks, how they can occur and whom they can be perpetrated by; existing controls; controls which will be implemented; and the officer(s) responsible for ensuring this is done. The likelihood and impact of the risk occurring are represented using the Council's standard 4x6 Risk Matrix. The score is arrived at through qualitative assessment, although there may be isolated instances where a quantitative assessment is more appropriate. Ideal risk mitigations are those which are easily integrated and do not require substantial resourcing. It is recognised that there is a law of diminishing returns in what can practically be achieved when managing a risk, as opposed to terminating or transferring it.

FRAs are scalable, being an appropriate tool to use at any level of the organisation (e.g., from team to enterprise level) and for any scope (e.g., from a single process all the way up to a broad theme). An example is attached at Appendix 2.

Over time, these documents are likely to evolve, so up-to-date templates will be available on the Fraud SharePoint site.

2.2 Process

When directed by the Integrity Group, the IFIA/ FRA process looks like this:



1. Request from Integrity Group (IG) to Senior Responsible Officer (SRO) of risk area that an IFIA or FRA be undertaken.

2. SRO undertakes IFIA, can choose to do so with support from Counter Fraud.

3. SRO meets with IG for both to review IFIA or FRA. In case of IFIA, IG will agree scope of FRA to be undertaken by SRO (if required), potentially with assistance from Counter Fraud.

4. FRA reviewed by IG. Risks added to Fraud Risk Register (FRR). Management tasks assigned to SRO and/ or Counter Fraud.

5. FRR risks are regularly reviewed by IG to ensure that mitigation is ongoing and effective. Review dates set. Blocking factors escalated first to Chief Officers to remedy, thereafter Risk Board, which can escalate further and/ or add a new risk to the Corporate Risk Register.

Figure 2, Directed Process

The SRO can self-initiate the process by starting at point 2.

The process for self-initiating an IFIA is:

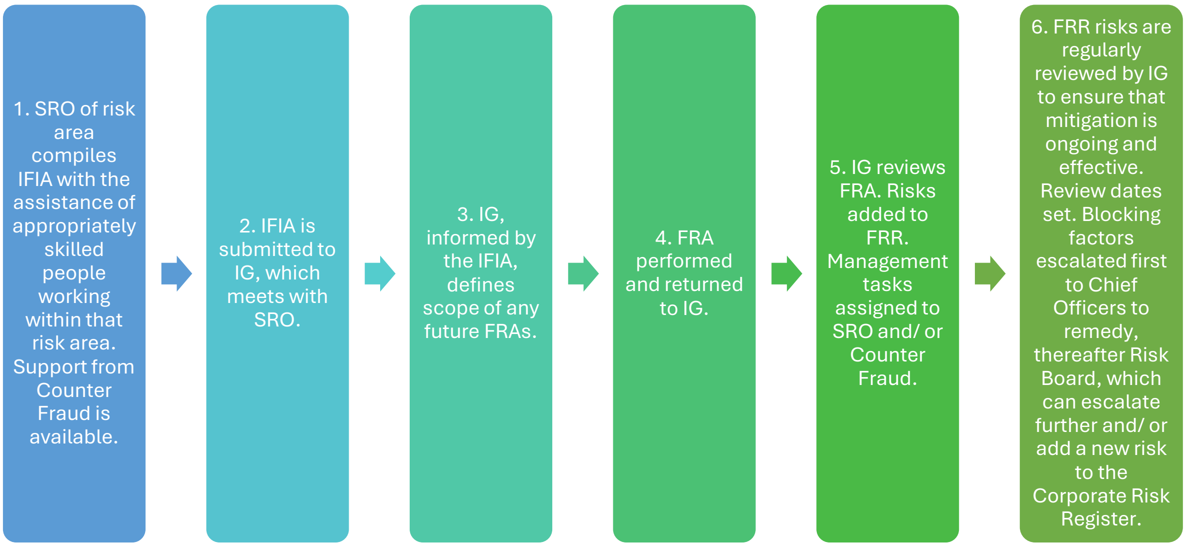

1. SRO of risk area compiles IFIA with the assistance of appropriately skilled people working within that risk area. Support from Counter Fraud is available.
2. IFIA is submitted to IG, which meets with SRO.
3. IG, informed by the IFIA, defines scope of any future FRAs.
4. FRA performed and returned to IG.
5. IG reviews FRA. Risks added to FRR. Management tasks assigned to SRO and/ or Counter Fraud.
6. FRR risks are regularly reviewed by IG to ensure that mitigation is ongoing and effective. Review dates set. Blocking factors escalated first to Chief Officers to remedy, thereafter Risk Board, which can escalate further and/ or add a new risk to the Corporate Risk Register.

Figure 3, Self-Initiated IFIA Process

2.3 When the IFIA is required

Disbursement of a specific budget or grant: The IFIA should be compiled and submitted to IG when funding is secured/ approved. At least one FRA will be required over the lifespan of the subject, possibly more, depending on the scope and duration of the activity. The IG will provide further guidance on this.

Business case/ capital projects/ service redesign: IFIA should be submitted prior to, or at the same time as, the business case. The need for FRAs is dependent on the impact and value of the activity. The IG will provide further guidance.

2.4 Fraud considerations in new policies/ policy updates

Policy authors should consider possible fraud risk and impact. This will be an area of consideration by the finance representative who sits on both the Policy and Integrity groups.

3 Roles of Specific Officers under the Policy

3.1 Counter Fraud Officers (CFO)

With oversight from the Chief Officer – Finance and Risk Board, CFOs will act as Key Contacts and administer the National Fraud Initiative within ACC.

Subject to review and feedback, CFOs will develop the necessary counter fraud tools used by the Integrity Board and the wider Council. This includes templates and training materials, all of which will be hosted on the Fraud SharePoint site.

Any allegations of fraud committed against the Council should be referred to the CFOs, either directly or via the Chief Officer – Finance. This should be done before any other Council process is initiated, e.g., Managing Discipline. CFOs are responsible for conducting investigations under the Counter Fraud policy and the Financial Regulations. Investigations under other policies are considered on a case-by-case basis.

CFOs will liaise with external agencies in connection with the prevention and detection of fraud, as well as reporting to the Crown Office when authorised by the Chief Officer – Finance.

In undertaking fraud investigations, CFOs may make specific requirements of staff, as laid out in the Council's Financial Regulations. Failure to comply with these requirements may result in disciplinary action.

- At any reasonable time, to access any premises, personnel, assets and documents considered necessary by the CFO.
- To provide any information or explanation considered by the CFO, and within a timescale specified by the CFO.

3.2 Chief Officer – People & Citizen Services

This officer will make arrangements for a representative of People & Organisation Development (P&OD) to engage with CFOs to triage employee allegations received at P&OD, in order to identify serious allegations which may have a fraud component prior to any action being pursued under another policy. This triage will take place regularly, with the frequency of meetings to be agreed on the basis of referral volume.

Should P&OD receive an allegation against a member of staff which is immediately considered to relate to internal fraud against the Council (as defined in the Policy), they will immediately refer the matter to the Chief Officer – Finance for review before taking any further action.

3.3 Chief Officers

Chief Officers are responsible for encouraging an anti-fraud culture through their actions, messaging and commitment to continuous improvement in the area of fraud risk management. The cooperation of Chief Officers is welcomed in ensuring that their leadership teams fully engage with the Integrity Group and CFOs; and that their staff are aware of this Policy, fully comply with it, and undertake the mandatory Fraud Awareness training.

4 Useful Concepts

Fraud: Fraud involves the use of deception in order to obtain something to which the fraudster would not otherwise be entitled. This deception can be through lie or omission. Fraud can be perpetrated by individuals, groups, or even corporate bodies. Aside from common law fraud, various statutory fraud offences exist, e.g., ones which relate to benefit fraud, intellectual property and use of a 'blue badge.' Fraud can be prosecuted as a crime, but redress can also be sought through civil procedure.

Bribery: This is the act of mis-performing one's job in exchange for personal gain. The 2010 Bribery Act creates offences of offering bribes, being bribed or soliciting bribes. The Act lays out specific scenarios which reflect these offences.

Corruption: This is when a person abuses their power within an organisation for personal gain. It often involves multiple people covering for each other's illicit activity. As there is often a *quid pro quo* involved, prosecutions are frequently under the Bribery Act.

Tax Evasion: This is the deliberate act of failing to pay the correct amount of tax due. There are specific criminal offences which deal with tax evasion.

Money Laundering: In relation to the proceeds of crime, it is illegal to conceal criminal property; disguise it; convert it (e.g. from cash to cryptocurrency); to transfer ownership; and to remove it from the UK. It is an offence to acquire, use or possess any criminal property. There are further offences of failing to report that you suspect someone of money laundering, and of letting someone know that they are being investigated for money laundering.

'Failure to Prevent' offences: These are offences where an organisation and/ or specific managers within an organisation, can be held criminally liable for dishonesty offences committed by the organisation or someone linked to it. Failure to prevent bribery is a corporate offence under the Bribery Act 2010; failure to prevent tax evasion is similarly covered by the Criminal Finances Act 2017; and the organisational failure to prevent fraud is dealt with by the Economic Crime and Corporate Transparency Act 2023.

Theft/ Asset Misappropriation: Theft is the felonious taking of property with intent to permanently deprive the owner. It can be premeditated, or the decision can be made at some point after legitimately taking possession of that property, e.g., when an employee chooses not to return their work laptop after leaving the organisation.

Embezzlement: This is when someone who is professionally entrusted with the goods or assets of another intentionally misappropriates them without consent. For instance, the treasurer of a charity is entrusted with the finances of that charity but instead takes those funds and uses them himself.

Collusion: In the context of this document, this is when separate people or entities secretly act together with a shared purpose, e.g., to override a segregation of duties.

4.1 Fraud Models

Fraud models: these are ways to explain the motivation of offenders to defraud. The better known include:

- **The Fraud Triangle**. The offender has a non-sharable pressure (usually financial, but it could be coercion, for example); has the opportunity to commit the crime; and can rationalise his actions as justified. Removing any side of the triangle will prevent the crime from occurring.
- **The Fraud Diamond**. The offender has an incentive; the opportunity; the capability to take advantage of this opportunity; and can rationalise his actions.
- **The Fraud Pentagon**. the offender has a non-sharable pressure; has the opportunity to commit the crime; has the competence to commit the crime; displays arrogance/ self-entitlement; and can rationalise his actions.

It has been theorised that these models can be best applied at different levels of the organisation. The triangle for an employee with little responsibility, the diamond for a middle manager, and the pentagon for a senior officer.

It is worth considering what motivates potential fraudsters because this allows the organisation to better manage the risks they pose. Organisational culture is one of the greatest moderating influences on offender motivation (e.g., where there is zero tolerance to fraud, colleagues are alert to fraud risks and behave ethically).

ABC: This relates to fraud committed within an organisation and is a consideration of the extent of fraud. Is the fraud limited to the actions of one bad **A**pple; a **B**ushel (i.e., a group colluding to commit fraud); or the whole **C**rop (i.e., the whole organisation is corrupt)? One bad apple is most likely, but lowest impact, whereas a bad crop is the least likely but has the greatest negative impact.

4.2 Potential Indicators of Occupational Fraud

The Association of Counter Fraud Examiners (ACFE) publishes an annual report on occupational (employee) fraud using data provided by its global membership. A focus of this report is the identifying common behavioural characteristics of internal fraudsters, and ACFE has developed the following list of potential "red flags."

- Living beyond means
- Financial Difficulties
- Unusually Close Association with a Supplier/ Customer
- Control Issues, Unwillingness to Share Duties
- Irritability, Suspiciousness or Defensiveness
- "Wheeler-dealer" Attitude
- Bullying or Intimidation
- Divorce/ Family Problems
- Complained about Inadequate Pay
- Addiction Problems
- Excessive Pressure from Organisation to Meet Targets
- Refusal to Take Holidays
- Past Legal Problems
- Complained about Lack of Authority
- Other Employment-related Problems
- Excessive Family/ Peer Pressure for Success
- Excessive Lateness or Absenteeism
- Social Isolation
- Instability in Life Circumstances
- Excessive Internet Browsing

The existence of any of these red flags does not mean that someone *will* defraud the organisation, but it is an important data point in managing fraud risk. For instance, if you have a member of staff who routinely has access to Council payment systems and you happen to know they have a problem with debt (as opposed to just having debt), that employee may be more motivated to defraud the Council and extra checking may be warranted. This is the same principle that many organisations already employ in background checks for particular posts.

4.3 Tools/ Considerations

Tone at the top (TATP): this refers to the behaviour and messaging from an organisation's senior leadership. This feeds through the organisation to create an ethos which is representative of that tone. Ethical leadership promotes an ethical culture. Poor TATP can be viewed as a risk factor by auditors.

Culture: this is developed through TATP and reinforced by the collective behaviour of staff. This culture supports positive behaviour and discourages negative behaviours. Developing a sense of shared ownership of the team or the organisation can help shape this and enable you to better defend against fraud. For instance, following a fraud event, discussion of the audit findings with your team allows them to be vigilant to similar factors being allowed to materialise in the future.

Whistleblowing: When an employee cannot raise concerns via normal reporting methods and fears retribution, whistleblowing can legally protect that employee from retaliation. According to ACFE, most frauds are detected by this means, so employees should be aware of the policy and procedure and encouraged to raise concerns. Studies have shown that employees are more likely to 'blow the whistle' in organisations which are merit-based, and where the action of reporting is framed as preventing further harm, rather than producing a positive outcome.

Sanctions: Ultimately the organisation must be willing to take action when unethical behaviour has been uncovered. Some organisations are unwilling to do this, which risks repeat occurrences, financial loss and reputational damage. In order to dissuade perpetrators from "trying their luck, "any sanction should leave the sanctioned party in a worse position than had the fraud not been attempted.

Target Hardening: This is the process of making it more difficult to successfully commit a crime, making it too risky for a rational offender to attempt, or reducing the likely reward for committing that crime. Simple examples might include limiting employee building or system access to a minimal level, etching of serial numbers onto high-risk items, CCTV coverage of high-risk areas, or frequent cash uplifts from a safe to prevent a large amount of cash at rest.

Routine Activity Theory (RAT): This is a commonly accepted theory within situational crime analysis. Once understood, you can use it to harden targets. It posits that a crime occurs when a motivated offender and a poorly defended target exist in the same place and time. This can be visualised as *The Crime Triangle* (Figure 4). Some factors can increase the likelihood of the crime occurring by influencing each of these elements, such as the offender having a grievance towards the target or its owner; a lack of witnesses in that place; or the target being unprotected. We can use RAT to visualise how to prevent fraud by ensuring that the offender has a "handler," which could mean that his activity is moderated by his manager or colleagues; by the target having a "guardian," which could be solid internal controls; and the place (the organisation), being “managed,” e.g., by sound corporate governance, policies, procedures and training.

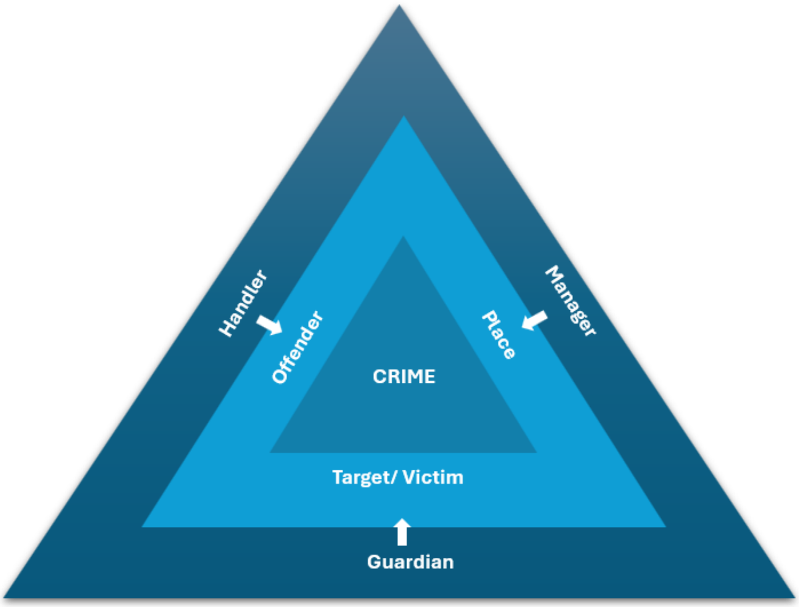
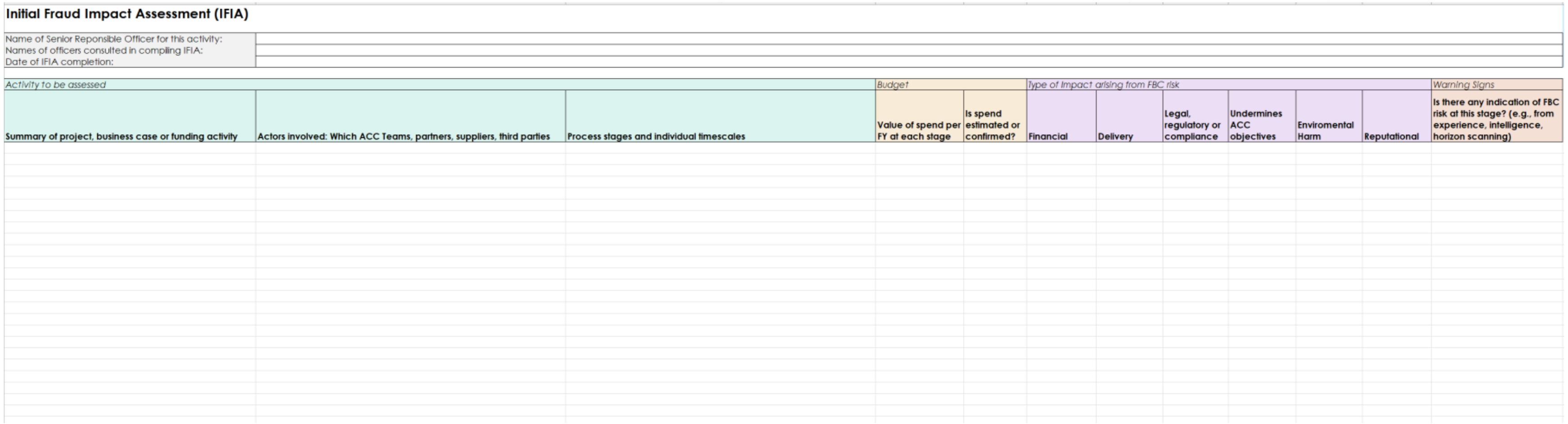


Figure 4, the Crime Triangle of Routine Activity Theory

You needn’t necessarily use RAT; any tool which helps you understand how to prevent and detect fraud is worth using.

Appendix 1, Sample Initial Fraud Risk Assessment (IFIA)



Initial Fraud Impact Assessment (IFIA)

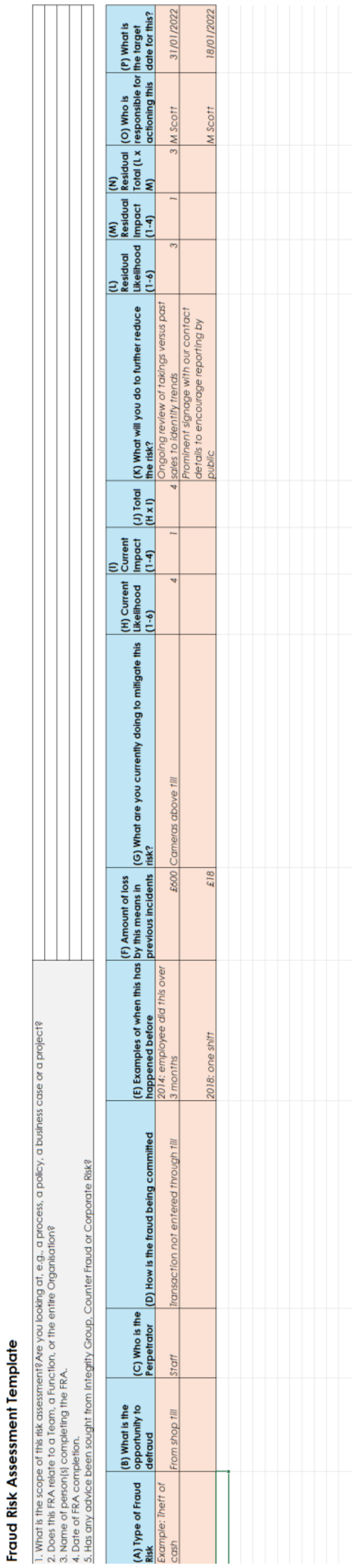
Name of Senior Reponsible Officer for this activity:

Names of officers consulted in compiling IFIA:

Date of IFIA completion:

Activity to be assessed			*Budget*		*Type of Impact arising from FBC risk*						*Warning Signs*
Summary of project, business case or funding activity	**Actors involved: Which ACC Teams, partners, suppliers, third parties**	**Process stages and individual timescales**	**Value of spend per FY at each stage**	**Is spend estimated or confirmed?**	**Financial**	**Delivery**	**Legal, regulatory or compliance**	**Undermines ACC objectives**	**Enviromental Harm**	**Reputational**	**Is there any indication of FBC risk at this stage? (e.g., from experience, intelligence, horizon scanning)**

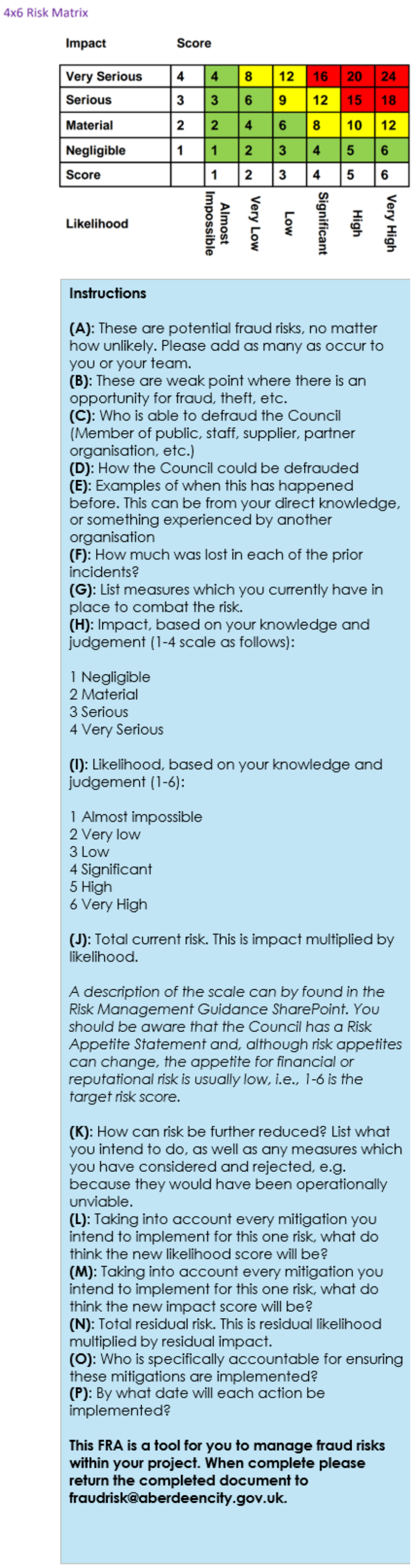
Appendix 2, Sample Fraud Risk Assessment (FRA)



Fraud Risk Assessment Template

1. What is the scope of this risk assessment?Are you looking at, e.g., a process, a policy, a business case or a project?	
2. Does this FRA relate to a Team, a Function, or the entire Organisation?	
3. Name of person(s) completing the FRA.	
4. Date of FRA completion.	
5. Has any advice been sought from Integrity Group, Counter Fraud or Corporate Risk?	

(A) Type of Fraud Risk	(B) What is the opportunity to defraud	(C) Who is the Perpetrator	(D) How is the fraud being committed	(E) Examples of when this has happened before	(F) Amount of loss by this means in previous incidents	(G) What are you currently doing to mitigate this risk?	(H) Current Likelihood (1-6)	(I) Current Impact (1-4)	(J) Total (H x I)	(K) What will you do to further reduce the risk?	(L) Residual Likelihood (1-6)	(M) Residual Impact (1-4)	(N) Residual Total (L x M)	(O) Who is responsible for actioning this	(P) What is the target date for this?
Example: Theft of cash	*From shop till*	*Staff*	*Transaction not entered through till*	*2014: employee did this over 3 months*	*£600*	*Cameras above till*	*4*	*1*	*4*	*Ongoing review of takings versus past sales to identify trends*	*3*	*1*	*3*	*M Scott*	*31/01/2022*
				2018: one shift	*£18*					*Prominent signage with our contact details to encourage reporting by public*				*M Scott*	*18/01/2022*



4x6 Risk Matrix

Impact	Score						
Very Serious	4	4	8	12	16	20	24
Serious	3	3	6	9	12	15	18
Material	2	2	4	6	8	10	12
Negligible	1	1	2	3	4	5	6
Score		1	2	3	4	5	6
Likelihood		Almost Impossible	Very Low	Low	Significant	High	Very High

Instructions

(A): These are potential fraud risks, no matter how unlikely. Please add as many as occur to you or your team.
(B): These are weak point where there is an opportunity for fraud, theft, etc.
(C): Who is able to defraud the Council (Member of public, staff, supplier, partner organisation, etc.)
(D): How the Council could be defrauded
(E): Examples of when this has happened before. This can be from your direct knowledge, or something experienced by another organisation
(F): How much was lost in each of the prior incidents?
(G): List measures which you currently have in place to combat the risk.
(H): Impact, based on your knowledge and judgement (1-4 scale as follows):

1 Negligible
2 Material
3 Serious
4 Very Serious

(I): Likelihood, based on your knowledge and judgement (1-6):

1 Almost impossible
2 Very low
3 Low
4 Significant
5 High
6 Very High

(J): Total current risk. This is impact multiplied by likelihood.

A description of the scale can by found in the Risk Management Guidance SharePoint. You should be aware that the Council has a Risk Appetite Statement and, although risk appetites can change, the appetite for financial or reputational risk is usually low, i.e., 1-6 is the target risk score.

(K): How can risk be further reduced? List what you intend to do, as well as any measures which you have considered and rejected, e.g. because they would have been operationally unviable.
(L): Taking into account every mitigation you intend to implement for this one risk, what do think the new likelihood score will be?
(M): Taking into account every mitigation you intend to implement for this one risk, what do think the new impact score will be?
(N): Total residual risk. This is residual likelihood multiplied by residual impact.
(O): Who is specifically accountable for ensuring these mitigations are implemented?
(P): By what date will each action be implemented?

This FRA is a tool for you to manage fraud risks within your project. When complete please return the completed document to fraudrisk@aberdeencity.gov.uk.