Cabinet Office

How to run a data analytics pilot for counter fraud

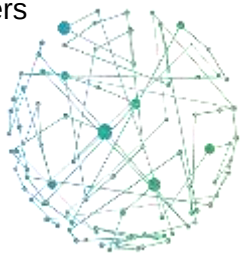
Why using data analytics for counter fraud is a good idea

The Best Practice Guidance – process and skills

Common Barriers to using data for counter fraud

The advantages of using data analytics to counter fraud

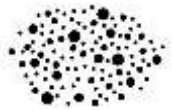
- Can be used to prevent or detect fraud
- Examine more cases (whole populations)
- Prevent human harm from fraud
- Identify Hidden Patterns / Connections
- Deal with different types of fraud taxonomies
- Connect to other data sets for broader insight
- Recovery of Assets from Fraud
- Faster checks and information corroboration
- Fill in gaps (fraud by omission)
- Improved user experience
- Keeps pace with increasingly data driven economies
- Reduces siloed working (fraud occurs in gaps)
- Repeatable methodologies (efficiency)
- Others



Cabinet Office

The context of using data analytics

The organisational context



- Data analytics capability across Government is inconsistent

- HM Revenue & Customs, the National Health Service, and a few other organisations have good capability to run analytical projects, but most are still maturing that capability.

- The structure of government has created silo working. There is no formal cross-government network for counter fraud analytics.

The challenges of using data analytics

Data, digital and technology challenges

- There is limited understanding of what data is available
- Data quality is varying and unclear
- There are differences in the speed of adoption of digital solutions.
- There is mixed understanding on how to access data and describe how it will be used

Legal and data protection challenges

- There were limited legal powers to share data
- Departments are overly protective of data

Cabinet Office

The Best Practice Guidance

The Best Practice Guidance (BPG)

Inconsistency, varied practices and a lack of capability

We worked with HMRC and the NHSCFA to find common themes, processes and considerations

Process and Skills documents

Cabinet Office

6 stages from the BPG process

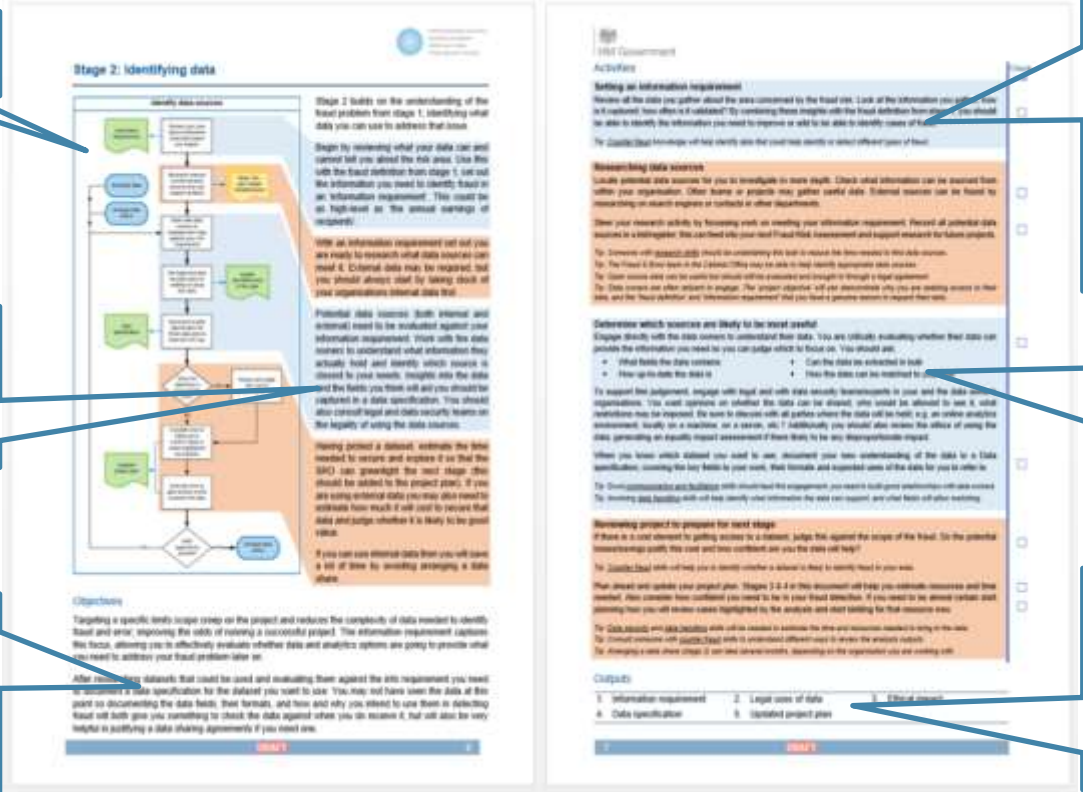
Stage 1: **Identifying & understanding fraud risks**	• Understand and prioritise the fraud risks your organisation faces. • Understanding the risk in detail and set a project objective.
Stage 2: **Identifying data**	• Review what information you need to address the fraud risk. • Research data sources that may be able to provide it.
Stage 3: **Arranging a data share**	• Review legal and security issues around sharing data. • Arrange a data sharing agreement with the data's owner.
Stage 4: **Evaluating the data**	• Check the data contains what you need and identify its weaknesses. • Confirm whether the data can be matched to yours.
Stage 5: **Designing the analysis**	• Set out how you will produce the information you need from the data
Stage 6: **Performing and evaluating your analysis**	• Perform the analysis as set out in previous stage. • Review results to see if any fraud has been identified.
Project closeout	• Document the project and update relevant parties on your findings.

Stage 1 from the process map

Process map of the stage

Description of the process

What you are trying to achieve in the stage



A detailed description of what should be done at this stage

Skills that should be engaged in each activity

The **outputs** you should be producing in this stage.

Question

What skills are required at each stage of the process?

Tip: consider both specialist and generic skills.

Skills

Stage 3: **Arranging a data share**	Establish a legal gateway to secure external data. Review data security issues. Use the templates to develop a Privacy Impact Assessment (PIA) and if required, a Data Sharing Agreement (DSA), or Memorandum of Understanding (MoU).
Stage 4: **Evaluate their data**	Using the data sample(s) from Stage 3 consider gaps, quality or formatting issues that impact data matching or analysis (the BPG can help with this), ensuring the PIA, DSA or MoU are updated as required.

Skills

- Counter Fraud Knowledge
- Data Analysis
- Data Handling
- Data Matching
- Data Security
- Fraud Risk Assessment
- Fraud Risk Management
- Legal Knowledge
- Business Knowledge
- Communication and Facilitation
- Research Skills
- Project Management

Cabinet Office

Barriers to running data analytics pilots for counter fraud

Cabinet Office

Barriers to counter fraud data analytics and how to overcome them (top tips)

The Lesson

How To Apply It

A deep understanding of the fraud problem, the business process and the data around it leads to the development of a specific successful solution with the right data sources and can overcome privacy concerns

Use the fraud business analysis tool in the early stages of a pilot before you finalise your solution design. Critically: what piece(s) of information did you not know/could you not verify that allowed a fraud to happen?

Large scale pilots are overly complex and slow down delivery and are challenging to resource.

Design data pilots that are small enough to manage within other government department priorities, but large enough to make an impact.

Pilots having mutual benefits for all parties drives delivery.

Investing time to agree and identify reciprocal benefits and showing the counter fraud, impact and efficiency value of data analytics to senior decision makers (Advantages of Counter Fraud Data Analytics)

Lawyers and legal policy officials can be overly risk averse or generalists who usually do not understand criminology or privacy laws in sufficient detail.

Challenge legal decisions (myths!) that data sharing is not permissible.

- Fraudulent acts usually outweigh privacy concerns as long as the data share is proportionate and considered. (Clapoom legislation)
- Secrecy provisions often have exemptions for counter-criminality detection or investigation
- Consider requesting a public interest certificate from your departmental legal team