Good practice guidance

Fraud and error

National Audit Office

March 2021

The guide is aimed at those interested in both the audit expectations for accountability and transparency around fraud and error and understanding how their organisation can tackle it.

We are the UK's independent public spending watchdog

Foreword

Before the COVID-19 pandemic, the Government Counter Fraud Function estimated that the level of fraud and error against government was already between £29.3 billion and £51.8 billion annually.

Our work over the past year has shown that the risk of fraud and error has risen significantly as a result of the government's response to the COVID-19 pandemic. In part, this is because some controls were no longer safe to operate, such as the Department for Work & Pensions' requirement for face-to-face meetings with applicants, or the need to provide support to people and businesses quickly. But our work has shown over time that government needs to do more to measure exactly how much fraud and error there is in the system, put in place cost-effective counter-fraud and error controls, and detect and pursue overpayments to protect the taxpayer's interest. This is now more important than ever.

This guide sets out the increased level of risk of fraud and error and how the National Audit Office (NAO) will ensure accountability and transparency over that level of risk through its audits. It also sets out insights from our recent work on fraud and error to show how more can be done to counter this risk.

Gareth Davies

Comptroller and Auditor General
March 2021

What is the guide about?

This guide is in four parts:

- The increase in fraud and error risk.
- Expectations on government in tackling fraud and error.
- How the NAO audits fraud and error.
- Good practice against our Fraud and Error Audit Framework.

Who the guide is aimed at:

The guide is aimed at those interested in both the audit expectations for accountability and transparency around fraud and error and understanding how their organisation can tackle it. It will be of particular interest to:

- those in central government and the wider public sector;
- senior decision-makers in organisations with a fraud risk; and
- non-executive directors and members of audit and risk committees.

This guide is not intended for:

- private sector recipients of government money interested in requirements on them for tackling fraud; or
- counter-fraud staff interested in the detail of how to tackle fraud and error or investigate specific cases.

Good practice guidance

Fraud and error

What this guide covers

The National Audit Office (NAO) scrutinises public spending for Parliament and is independent of government and the civil service. We help Parliament hold government to account and we use our insights to help people who manage and govern public bodies improve public services. The Comptroller and Auditor General (C&AG), Gareth Davies, is an Officer of the House of Commons and leads the NAO. We audit the financial accounts of departments and other public bodies. We also examine and report on the value for money of how public money has been spent. In 2019, the NAO's work led to a positive financial impact through reduced costs, improved service delivery, or other benefits to citizens, of £1.1 billion.

If you would like to know more about the NAO's work on fraud and error, please contact:

Joshua Reddaway
Director, Fraud and Error
Value for Money Audit

joshua.reddaway@nao.org.uk
020 7798 7938

Claire Rollo
Director, Fraud and Error
Financial Audit

claire.rollo@nao.org.uk
0207 7798 1846

If you are interested in the NAO's work and support for Parliament more widely, please contact:

Parliament@nao.org.uk
020 7798 7665

Design & Production by NAO External Relations ● DP Ref: 10381-001

Part One: The increase in fraud and error risk

Explains the fraud and error risk to taxpayers and government, including the recent upsurge driven by the COVID-19 pandemic.

The fraud and error landscape

The level of fraud and error against government was known to be significant even before COVID-19, and is likely to have increased by billions of pounds since the pandemic.

The Government Counter Fraud Function (GCFF) estimates that before the COVID-19 pandemic the public sector was losing between £29.3 billion and £51.8 billion a year from fraud and error, before any recoveries. This estimate includes a number of unknown variables. Around £26.8 billion is based on measurement of fraud and error in specific areas of income or expenditure. The rest is based on GCFF's assessment that fraud and error is likely to be in the range of 0.5% and 5% for the £503 billion where fraud and error has not been measured.

Before the pandemic, the highest levels of fraud known to government were within the tax and welfare system where there are well-established methods of estimating the level of fraud and error.

- Fraud and error in tax (known as the tax gap) decreased by 1.1 percentage points between 2015-16 and 2018-19.
- The Department for Work & Pensions' (DWP's) estimated overpayment rate for benefit expenditure, excluding State Pension, rose every year between 2014-15 and 2018-19 – from 3.6% to 4.6%.[1]
- Overpayments on Tax Credits were 4.9% in 2018-19, with underpayments at 0.7% of expenditure.

Elsewhere the level of fraud and error is unknown but the amount that was actually detected has risen as government has invested more in its Counter Fraud Function. The level of fraud and error the GCFF records as detected in areas outside tax and welfare rose from £105 million in 2015-16 to £205 million in 2018-19, and £310 million in 2019-20.

The risk of fraud and error has risen significantly as a result of the government's response to the COVID-19 pandemic.

This is because government has:

- spent more on things that are prone to fraud and error, such as welfare, business support and grants;
- often prioritised the need for speed when setting up new initiatives over reducing the risk of fraud and error;
- provided support to people and businesses that it does not have a prior relationship with (and therefore lacks information to verify claims);
- introduced new supply chains at pace to procure goods and services;
- relaxed or modified normal controls to enable remote working and remote access to services by citizens;
- prioritised its COVID-19 response over business-as-usual compliance activity; and
- increased its risk appetite for fraud and error, as shown by ministerial directions accepting risks identified by the civil service.

The GCFF has undertaken a Global Fraud Risk Assessment across 206 schemes in response to COVID-19. It has assessed the value for government of the schemes as announced as £387 billion. It has risk-assessed 16 of these schemes as having a high or very high fraud risk, accounting for 57% (£219 billion) of the £387 billion.[2]

Early indications are that fraud and error has risen by billions of pounds as a result. The actual amount will become clearer as departments measure the level of fraud and error across specific initiatives.

1 To reflect changes in methodology which DWP introduced in 2019-20, it chose to restate 2018-19 for comparative purposes, restating the overpayment rate, excluding state pension, as 4.4% in 2018-19. DWP has revised its estimation techniques and assumptions throughout this time series, with no previous restatements.

2 The National Audit Office's (NAO's) *COVID-19 cost tracker* currently records a total cost estimate of £271 billion for measures announced on or before 6 December 2020 for which central government departments are responsible (where data are available). The variance between GCFF's £387 billion figure and NAO's COVID-19 cost tracker is explained by the Global Fraud Risk Assessment's use of a broader definition of value, for example the amount loaned through loan schemes rather than the estimated cost to government of supporting such a scheme, or the amount of deferred tax in tax-deferral schemes.

Top fraud and error risks in COVID-19 schemes

The top fraud and error risks identified alone are likely to represent billions of pounds.

The Government Counter Fraud Function has assessed the following COVID-19 schemes as having the potential for high or very high risk of fraud.

Department	COVID-19 schemes with top identified fraud and error risks	Estimates of fraud and error
Department for Work & Pensions	**Universal Credit:** the number of claimants roughly doubled in 2020 and the Department suspended some controls such as face-to-face appointments to support vulnerable people during lockdown and manage demand.	9.4% (£1.7 billion) of Universal Credit payments were overpaid in 2019-20 before COVID-19. DWP accepts that a doubling of the Universal Credit caseload and relaxing controls will lead to a further increase in fraud and error levels. There is uncertainty around exactly how much fraud and error will rise but NAO believes that the increase is likely to be substantial.
HM Revenue & Customs (HMRC)	**Coronavirus Job Retention Scheme.** Around £46.4 billion of expenditure by December 2020.	HMRC's planning assumption is fraud and error of 5%–10%, or between **£2.32 billion and £4.64 billion**.
Department for Business, Energy & Industrial Strategy (BEIS) (in conjunction with the British Business Bank (the Bank))	**The Bounce Back Loan Scheme.** Around £44.7 billion of 100% government-guaranteed loans issued by January 2021.	BEIS and the Bank have estimated between 35% and 60% of the loans may not be repaid, with a currently estimated value of between **£16 billion and £27 billion** based on loans to date. This represents both credit and fraud risk. BEIS and the Bank are currently working to estimate what proportion is due to fraud.
Department of Health & Social Care	**Coronavirus Response Fund - Funding for the NHS: Procurement of medical equipment (including additional ventilators).** Primarily personal protective equipment to protect frontline staff. Expenditure of £10.2 billion by January 2021, with an estimated lifetime cost of around £15.2 billion. There is a high risk of fraud in procurement of personal protective equipment.	Estimates not yet available.

Source: Government Counter Fraud Function's Global Fraud Risk Assessment and National Audit Office analysis

The Counter Fraud Function has also assessed a further group of COVID-19 schemes as potentially at high risk of fraud. The Counter Fraud Function believes scheme owners need to do more work to fully quantify those risks.

Part Two: Expectations on government in tackling fraud and error

Sets out the role of the Government Counter Fraud Function and how accounting officers can demonstrate the effectiveness of their fraud and error strategies.

The Government Counter Fraud Function

The Counter Fraud Function is focusing on ensuring departments identify and react to emerging risks.

About the Government Counter Fraud Function

The Government Counter Fraud Function (GCFF) was established in 2018, to support government in delivering greater efficiency and effectiveness. It has a core Centre of Expertise in the Cabinet Office and and seeks to bring together the 16,000 people working in counter-fraud across government to allow best practice and knowledge to be shared.

The GCFF launched a Government Counter Fraud Profession (GCFP) which has around 6,600 members, and developed several initiatives across the public sector – including some pilot projects using data and analytics to identify and prevent fraud.

The GCFF has also developed and published a Government Functional Standard for counter-fraud work in addition to a range of other standards and guidance for undertaking counter-fraud work. These include Fraud: Risk Assessment; Investigation; and Leadership, Management and Strategy Standards. These can be accessed by emailing GCFP@cabinetoffice.gov.uk or via the knowledge hub for GCFP members.

Departments and public bodies can engage with the GCFF via the Centre of Expertise within the Cabinet Office.

For more information visit the gov.uk pages or contact FED@cabinetoffice.gov.uk.

The GCFF has said it wants to help ensure the UK is the most transparent government globally in how it deals with public sector fraud.

It agreed a five-year strategy in 2018-19 for tackling fraud across the public sector. Its strategic objectives are:

- building capability across government and supporting organisations to evolve;
- innovating in intelligence-sharing and the use of data;
- increasing understanding of risk and threat, and using this to design out opportunities for fraud where possible;
- close working with cyber security on shared threats and opportunities; and
- minimising loss in the areas where there is known loss.

Since COVID-19, the Counter Fraud Function told us it has:

- focused on ensuring quality assurance is undertaken in the highest risk areas, using the Global Fraud Risk Assessment, and advocated best practice for fraud measurement sampling and quality testing as provided by the Fraud Measurement and Assurance programme; and
- asked all departments to develop post-event assurance plans, identifying how they will measure, estimate and recover, where possible, fraud losses occurring as a result of COVID-19 financial support.

Expectations on government organisations

Accounting officers are responsible for managing their organisation's response to fraud and error risk as part of their overall control environment.

HM Treasury sets out the key responsibilities for accounting officers in its guide to *Managing Public Money (MPM)*. In respect to fraud and error this is to:

Minimise it	Put it right	Report on it
Organisations need to demonstrate cost-effective controls to deter and prevent fraud and error	**Organisations need cost-effective controls to detect and rectify fraud and error**	**Organisations needs to provide transparent reporting of fraud and error**
Accounting officers have a duty of ensuring value for money and controlling risks. They need to demonstrate that they have a cost-effective system of control that reduces fraud and error as much as possible. The basic control cycle is stipulated by MPM (MPM A4.9), which requires accounting officers to (MPM A4.9.2): ● assess the organisation's vulnerability to fraud; ● identify specific fraud risks; ● evaluate the scale of each risk; ● respond; and ● measure the effectiveness of the response. The system of control over fraud and error needs to apply across the organisation's supply chain including through contractual mechanisms (MPM 7.12) and grant agreements (MPM A5.1.6).	Deterrence and prevention are often more cost-effective than detection, correction and pursuit, but where fraud and error does occur, departments need to ensure that they: ● detect it (MPM A4.9.6); ● recover overpayments wherever possible (MPM A4.11.2); and ● provide restitution to citizens for underpayments (MPM 4.7.3). Departments also need to review the causes of errors to consider any systemic issues. Where systematic underpayments are identified departments may need to undertake a review of all such cases to identify those affected. This is known as a Legal Entitlements and Administrative Practices (LEAP) exercise.	The government's counter-fraud functional strategy states an aim to be the most transparent government globally in dealing with public sector fraud. Where there is an identified material risk of fraud and error, the organisation should measure and estimate the scale of fraud and error and disclose this in its Annual Report. In particular it must disclose: ● an assessment of any material fraud and error risk and any control weaknesses as part of the governance statement (MPM A3.1.4); and ● any material losses, overpayments and fraud in the accounts (MPM A4.10).

What is a cost-effective control environment?

Accounting officers' judgements of the cost-effectiveness of controls need to be explicit, evidenced and transparent.

Departments need to be able to demonstrate that they have cost-effective controls over the risk of fraud and error.

A cost-effective control environment is one where the department is doing everything it reasonably can to minimise fraud and error, and doing anything more would have a detrimental impact. A cost-effective control environment leads to the lowest level of fraud and error compatible with the policy intent.

A control environment is not necessarily fully cost-effective even if the department is making best use of its existing budget. If the department could 'invest to save' by spending more, it should gather the evidence to make the case to HM Treasury.

Accounting officers, as part of their value for money assessments, need to undertake a holistic assessment of what is cost-effective. They will need to consider more than simply the cost of the control and include such matters as the impact on customer service and policy intent (**see box opposite**).

While it is for accounting officers (and those they delegate to) to make the judgement about what is cost-effective, they should ensure that their judgements are:

- **explicit:** normally set out in writing in advance when making proposals about changes to controls, policies or regulations that affect fraud and error;
- **evidenced:** based on the best information about the impact on fraud and error; and
- **transparent:** available to decision-makers. For example, when proposing new regulations to Parliament, it might be appropriate for the department to publish a fraud and error impact assessment.

Things accounting officers may wish to take into account when considering the cost-effectiveness of a control

Benefits	Costs
The expected reduction in fraud and error	The internal resource costs of implementing and maintaining the option.
The deterrent effect	False negatives – stopping legitimate grant payments.
Information from trialling new approaches	External costs – costs to other organisations.
User and public confidence in the system	Any negative impact on policy objectives, such as: • degradation of customer service, for example reduced payment timeliness; • the burden and cost to the grant recipient; and • reduced take-up of the grant.

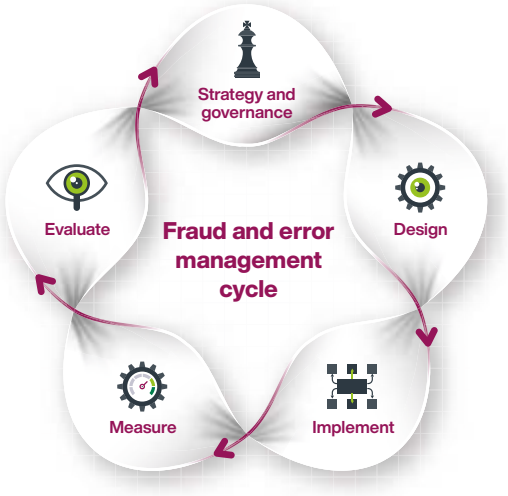
The impact of a cost-effective control environment on fraud and error

A cost-effective control environment leads to the lowest level of fraud and error compatible with the policy intent.

The NAO is often asked what we think the lowest achievable level of fraud and error in an area of expenditure might be. But it is often impossible to eliminate all fraud and error or to determine the minimum level of fraud and error that can be achieved in advance. Instead, we ask whether the department can demonstrate that it has a cost-effective control environment by iterating the management cycle (we use this as the basis of our Fraud and Error Audit Framework – see pages 13-18). If it can show that it is properly assessing the risk, designing and implementing controls accordingly, measuring the impact of those controls and reassessing its strategy quickly enough to iterate its approach and react to new risks and opportunities, then it can show that whatever fraud and error remains is the lowest that it can reasonably be.

Achieving a cost-effective fraud and error control environment

Iterate around the management cycle to demonstrate that the control environment is cost-effective...



...to achieve the lowest reasonable level of fraud and error possible.

The level of fraud and error produced by different control environments

Non-cost-effective control environment. Level of fraud and error with a control environment with known weaknesses.

Short-term target – the level achievable if the current rate was reduced as expected by existing initiatives.

A resource constrained cost-effective control environment – the lowest level achievable within the constraints of the current resources available to the department

A cost-effective control environment – the lowest level achievable that is not resource-constrained, and therefore, where all cost-effective options have been exhausted. This level would, however, allow for further investment not to be pursued where it would conflict with wider policy objectives.

Counter-productive control environment – a level that could only be achieved by making further investments that are not cost-effective. These might reduce fraud and error but have wider costs such as poor customer service.

0%

Part Three: How the NAO audits fraud and error

Sets out how NAO reports on fraud and error, including reporting on regularity and materiality in our financial audit work and how we assess the value for money of organisations' counter-fraud and error efforts using the Fraud and Error Audit Framework.

NAO audit and reporting requirements on fraud and error

We consider fraud and error as part of our financial audit and value for money work.

The NAO assesses how government departments are managing fraud and error across the range of our work:

- **True and fair opinion:** The NAO seeks reasonable assurance that the financial statements are free from material misstatement. Fraud and error may give rise to misstatement where it means transactions are not correctly recorded in accordance with the financial reporting framework.
- **Regularity opinion:** The NAO will seek sufficient appropriate evidence to obtain assurance over regularity, that is to say that transactions in the financial statements must be in accordance with the relevant framework of authorities. Income or expenditure arising due to fraud is always irregular. Income or expenditure arising due to error which represents non-compliance with the framework of authorities will also be irregular.
- **Reports on irregular expenditure:** The Comptroller and Auditor General (C&AG) may present a report alongside the regularity opinion on any irregular expenditure found. This will include any detailed findings on the nature of the irregular expenditure such as material levels of fraud and error. For example, we produce an annual Report on Accounts for DWP looking at fraud and error in benefit expenditure.
- **Value for money reports:** The NAO undertakes around 60 value for money studies a year looking at the economy, efficiency and effectiveness by which government uses its resources. The reports are published and presented to Parliament. Value for money reports range in topic across anything government spends money on, and consider how departments are managing the level of fraud and error wherever it is material to the topic in question.

Assessing the impact of fraud and error on the audit opinion

The Comptroller and Auditor General (C&AG) will qualify his regularity opinion on any account with a material level of fraud and error, but the assessment of materiality will include both quantitative and qualitative factors.

As part of our audit of accounts, the NAO assesses departments' estimates of the extent of fraud and error in income and expenditure to assess the value and nature of irregular transactions.

In 2019-20, the C&AG qualified his opinion on three accounts due to material levels of irregular expenditure: Department for Work & Pensions, HM Revenue & Customs and Child Maintenance Client Fund Accounts (1993 and 2003 schemes). New schemes set up in response to the COVID-19 pandemic, with the increased risk of fraud and error, may result in further qualifications for the 2020-21 accounts.

In determining whether the level of fraud and error is material the C&AG has said that he will take account of whether the department has:

- demonstrated that it has a cost-effective control environment to prevent fraud and error;
- ensured transparent reporting of fraud and error; and
- engaged Parliament on the fraud and error risk in its expenditure, for instance through fraud and error impact assessments to disclose the nature of the risk as expenditure is authorised.

What is the regularity of expenditure?

Regularity is the concept that transactions that are reflected in the financial statements of an audited entity must be in accordance with the relevant framework of authorities.

The Government Resources and Accounts Act 2000 requires the C&AG to give a regularity opinion on the accounts and satisfy himself that:

- money provided by Parliament has been expended for the purposes intended by Parliament;
- resources authorised by Parliament to be used have been used for the purposes in relation to which the use was authorised; and
- the department's financial transactions are in accordance with any relevant authority.

What is a material level of fraud and error?

The auditor's assessment of what is material is a matter of judgement and includes both quantitative and qualitative considerations. This is because the users might have an interest in breaches of authority even where the sums of money involved may be small in relation to the overall expenditure in the financial statements.

As a benchmark for schemes with a known risk of fraud and error, we consider the level of fraud and error is likely to be material if it is around or above the level of materiality set for the financial statements as a whole.

But we also take into account wider factors such as the nature of the fraud and error, the level of transparency around it, and whether a department is doing all it can to minimise the risk and engage Parliament on the nature of the risk.

Assessing the value for money of efforts to tackle fraud and error

The NAO will use its Fraud and Error Audit Framework to audit departments' efforts to tackle fraud and error and assess whether they are cost-effective.

The NAO assesses how an audited body is managing fraud and error as part of our value for money studies, if it is material to the topic we are reporting on.

We use the Fraud and Error Audit Framework (the Framework) to assess whether the organisation can demonstrate that it has cost-effective controls to achieve the minimum reasonable level of fraud and error in its expenditure.

The NAO developed the Framework around 10 years ago for our internal use based on best practice in government and the private sector for tackling fraud.

Fraud and error risk is continuously evolving. The Framework thus focuses on how management uses an iterative approach to measure the effectiveness of its counter-fraud and error activities and to continuously improve its controls.

The Framework is designed to enable us to audit the effectiveness of this iterative approach, and is fully compatible with the guidance set out in *Managing Public Money* (page 7).

This is the first time we are publishing the full Framework, including the detailed questions, which now capture our most recent learning from the COVID-19 pandemic.

How do you manage fraud and error in a one-off programme?

The NAO's Fraud and Error Audit Framework is based on good practice in tackling fraud and error in areas of sustained expenditure such as benefits, banking and grants. These areas allow you to test and learn, iterate and continuously improve practice over time.

Much of government's COVID-19 pandemic responses are one-off programmes that do not have as much opportunity to iteratively improve over time. However, we would still expect organisations setting up a one-off programme that has a fraud and error risk to:

- assess that risk at the start;
- design controls around that risk;
- implement those controls;
- measure the fraud and error risk and monitor whether the controls are working, as best as they are able; and
- refine the programme as they go along.

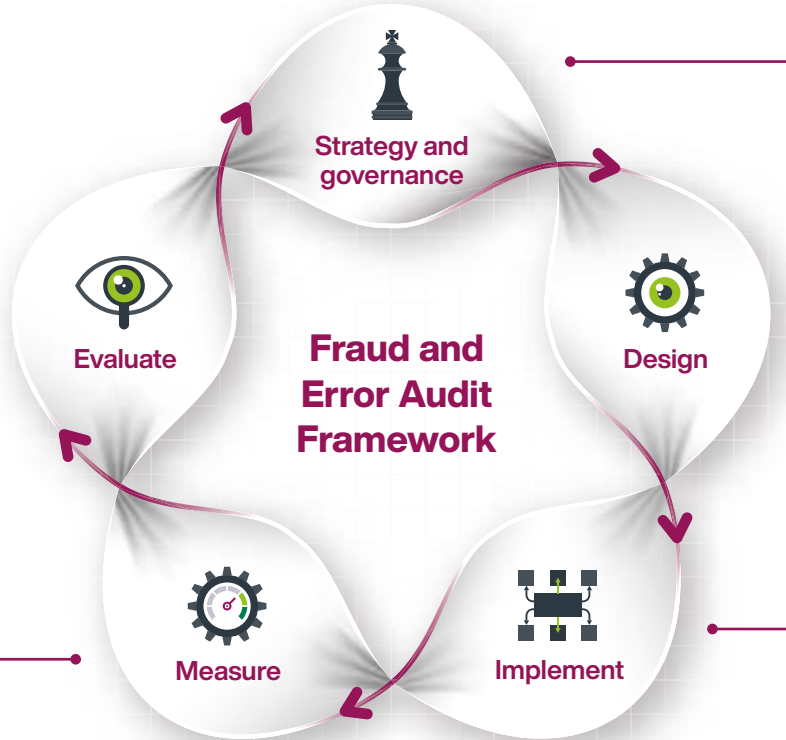
Organisations will need to ensure that they have the appropriate flexibility in commercial, contractual, regulations and grant agreements to adapt the approach and improve controls as they get more information on the nature of the fraud and error risk.

How do you prioritise limited resources?

A fully cost-effective control environment is one that has exhausted all avenues to improve controls. But, in reality, organisations will often find they need to prioritise improvements due to resource constraints, or change capacity in the organisation. The Fraud and Error Audit Framework provides an audit approach to test how the organisation does this.

The NAO Fraud and Error Audit Framework

The NAO assesses an organisation's progress in tackling fraud and error against the core components of the Framework.



Strategy and governance

Is there a strategy for tackling fraud and error risk, based on robust evidence and analysis, leading to clear prioritisation?

Are options for tackling key risks considered in a timely manner to keep pace with emerging threats and opportunities?

Are fraud and error trade-offs with other policy impacts considered?

Is the governance structure providing effective oversight of the fraud and error strategy, including clear reporting and performance measurement, and ensuring adherence across the organisation?

Has the organisation set clear targets towards a cost-effective control environment?

Design

Are fraud and error risks and entry points understood?

Are controls designed to effectively prevent and detect known fraud and error risks?

Is the expected cost and impact of each control understood?

Implement

Are processes in place to ensure that controls are implemented as designed?

Does the organisation have checks in place to detect and correct implementation issues?

Are individual resourcing decisions made with an understanding of the cost and impact on fraud and error?

Measure

Is a measure of fraud and error properly estimated?

Is the estimate appropriately reported?

Are other relevant measurements captured that supplement the overall estimate?

Are individual controls properly measured?

Evaluate

Are controls evaluated to look at how risks are being tackled and to identify new and emerging risks?

Are controls evaluated against each other to assess the cost-effectiveness of different methods for tackling fraud and error?

Has the organisation demonstrated that it is doing all it can to achieve the cost-effective level of fraud and error?

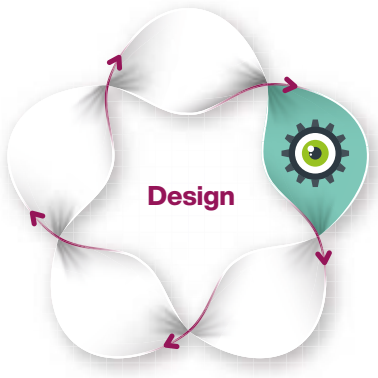
Part Four: Good practice against our Fraud and Error Audit Framework

Sets out good practice guidance based around the Fraud and Error Audit Framework's principles and provides examples of how the Framework can be applied, using case studies from our recent work.

Good practice against our Fraud and Error Audit Framework: Strategy and governance

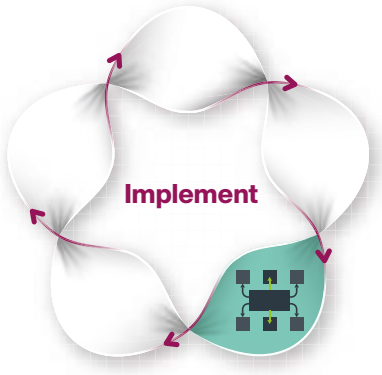
Strategy and governance	What would 'good' look like?
1 Is there a strategy for tackling fraud and error risk, based on robust evidence and analysis, leading to clear prioritisation?	• Material fraud and error risk is treated as a key strategic issue and prioritised at Board level. • The overall strategy for tackling fraud and error prioritises activities based on evidence of their cost-effectiveness. • The key fraud and error risks have been identified based on robust evidence and analysis. • The organisation's fraud and error risk appetite is clearly agreed with relevant partners and documented.
2 Are options for tackling key risks considered in a timely manner to keep pace with emerging threats and opportunities?	• The fraud and error risk register is regularly refreshed using the best available evidence. • Where new risks and opportunities are identified, options for new controls are evaluated on a cost-benefit basis and introduced on a timely basis.
3 Are fraud and error trade-offs with other policy impacts considered?	• There is clear dialogue between those responsible for fraud and error and those responsible for policy design. • The fraud and error impact of all changes to policy and operations are considered. Where an increased risk of fraud and error is accepted as a trade-off with other policy objectives this is explicitly laid out. • Fraud and error risks are communicated with senior decision-makers, including ministers and Parliament.
4 Is the governance structure providing effective oversight of the fraud and error strategy, including clear reporting and performance measurement, and ensuring adherence across the organisation?	• A governance structure is in place over fraud and error risk, with a clearly defined remit and ability to hold other parts of the organisation to account for implementing the fraud and error strategy. • There is timely and comprehensive reporting to those charged with governance over fraud and error risk. • Those responsible for measuring fraud and error are independent of those responsible for delivery. • There is a strong counter-fraud and error culture at all levels within the organisation.
5 Has the organisation set clear targets towards a cost-effective control environment?	• The organisation publishes and reports against targets for fraud and error, based on its expectation of the intended impact of its counter-fraud and error initiatives over time.

Good practice against our Fraud and Error Audit Framework: Design



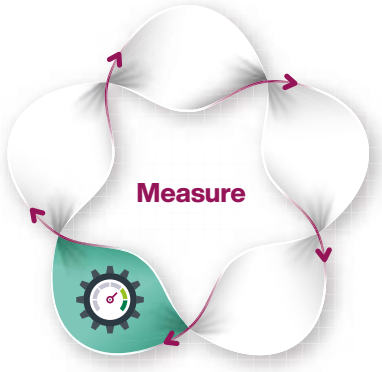
Design	What would 'good' look like?
1 Are fraud and error risks and entry points understood?	• The strategy has defined the key fraud and error risks. This should include the different types of fraud and error, where those risks enter the system and what causes the error, for example whether it is organisation error, customer error or fraud.
2 Are controls designed to effectively prevent and detect known fraud and error risks?	• A control framework is maintained which lists key controls and the risks which they mitigate. • Controls are designed to tackle each key risk and point of entry. • Controls cover the deterrent, prevention, detection and correction of fraud and error. • Controls make the best use of government's data, including data-sharing, where appropriate. • Control processes are automated where possible to mitigate against the risk of human error. • Controls processes are fully documented. • Controls are designed to be flexible to enable modifications where required. • Changes to controls are quality-assured and signed off at the appropriate level. • Controls are assigned a responsible owner who is responsible for their implementation and performance.
3 Is the expected cost and impact of each control understood?	• The cost-effectiveness of each control is assessed as part of its design or modification. • The relative cost-effectiveness of each control is assessed. • The appropriate balance between deterrent, prevention and detection activities is evaluated.

Good practice against our Fraud and Error Audit Framework: Implement



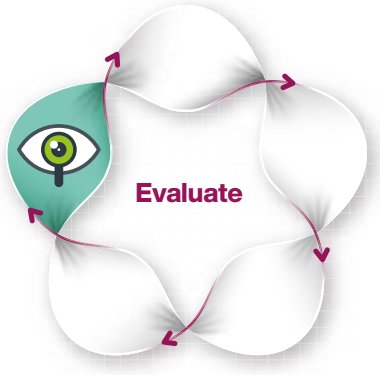
Implementation	What would 'good' look like?
1 Are processes in place to ensure that controls are implemented as designed?	• Staff operate controls as designed, with appropriate training and guidance. • Cases are worked accurately and productively. • Workarounds are minimised.
2 Does the organisation have checks in place to detect and correct implementation issues?	• Quality checks are routinely and independently performed to identify any implementation issues. • Where controls are automated, system failures are easily identifiable. • Quick, appropriate action is taken to resolve identified implementation issues.
3 Are individual resourcing decisions made with an understanding of the cost and impact on fraud and error?	• Controls are resourced adequately to deal with the level of demand. • Resources are used across different controls to maximise the impact on reducing fraud and error. • Controls are designed in such a way that they are resource-efficient; for example, prioritising automation over manual controls.

Good practice against our Fraud and Error Audit Framework: Measure



Measurement	What would 'good' look like?
1 Is a measure of fraud and error properly estimated?	• Material levels of fraud and error are measured regularly using robust estimation techniques. • The measurement is properly documented and quality-assured. • Where fraud and error is not measured, a clear rationale is set out for why not, such as proof that it is immaterial. This needs to be reassessed regularly to ensure that it remains the case. • Measurement of fraud and error is further sub-categorised by cause and type – for example, organisation error, customer error, or fraud. • The process for measuring fraud and error is regularly reviewed to ensure it is appropriate. • Any significant changes to the measurement are quality-assured and appropriately signed off.
2 Is the estimate appropriately reported?	• The fraud and error estimate is disclosed in line with reporting requirements, such as inclusion in the Annual Report and Accounts. • Significant variances over time and between cause and type are explained. • Any limitations in the measurement are clearly understood and explained. • Where appropriate, an additional statistics publication is produced, accompanied by a published methodology. • Performance against targets is reported.
3 Are other relevant measurements captured that supplement the overall estimate?	• There is regular measurement of detected fraud and error, including both overpayments and underpayments. • Supplementary 'real-time' key performance indicators are measured and monitored, such as the number of staff and public fraud referrals to provide additional intelligence on fraud and error risks.
4 Are individual controls properly measured?	• Key performance indicators are set out for each control measured. • New data sources are regularly considered to incorporate into the measurement of control performance. • Measurement is conducted on a regular basis appropriate for that control. • Measurement of controls should allow comparison of the cost-effectiveness of controls.

Good practice against our Fraud and Error Audit Framework: Evaluation



Evaluation	What would 'good' look like?
1 **Are controls evaluated to look at how risks are being tackled and to identify new and emerging risks?**	• Each control is evaluated against its key performance indicators, the measures of fraud and error, supplementary information and feedback from staff. • Root cause analysis is used to identify any new fraud and error risks. • Key performance indicators are updated in light of the evaluation. • Internal and external assurance are used effectively to evaluate the control environment. • The risk assessment methodology is reviewed when there are significant differences between the preliminary assessment of fraud and error risk and the measured level.
2 **Are controls evaluated against each other to assess the cost-effectiveness of different methods for tackling fraud and error?**	• The cost-effectiveness of each control is evaluated. • Evaluation of different controls is based upon consistent measurement where possible. • Evaluation clearly sets out whether controls are preventing and detecting fraud and error.
3 **Has the organisation demonstrated that it is doing all it can to achieve the cost-effective level of fraud and error?**	• The organisation has processes in place to consider what might be the cost-effective level of fraud and error and regularly evaluates its progress towards that level. This evaluation would be supported by robust evidence. • The organisation evaluates (at least annually) its progress in reducing fraud and error to the cost-effective level. • Gaps between the cost-effective level and the actual level of fraud and error are evaluated to understand how the control environment might need to be refined. • The strategy is regularly refined to consider results from the fraud and error estimate and other available analysis. • The organisation benchmarks itself against other relevant bodies.

Case study 1: Bounce Back Loan Scheme

Our 2020 *Investigation into the Bounce Back Loan Scheme* considered the credit and fraud risks of the Scheme. Government worked at pace to set up the Scheme and accepted a high level of financial risk in order to facilitate faster lending. It did this by removing the requirement for key approval checks and providing a 100% guarantee on loans granted by commercial lenders. The Department for Business, Energy & Industrial Strategy (BEIS) and the British Business Bank's (the Bank's) preliminary estimate was that the loss could be between 35% and 60% (£16 billion to £27 billion using the amount lent as at January 2021 of £44.7 billion). Government has implemented some changes to tackle known risks, but it remains unknown how much of the loans will not be repaid.

About the Bounce Back Loan Scheme

The Scheme is aimed at the smaller end of small- and medium-sized enterprises (SMEs). It provides registered and unregistered businesses with loans of up to £50,000, or a maximum of 25% of annual turnover, to maintain their financial health during the pandemic.

The Scheme launched on 4 May 2020 and, after extensions, is open to applications until 31 March 2021.

HM Treasury developed the Scheme with BEIS and the Bank. HM Treasury, in conjunction with BEIS, identified the need and set the Scheme's policy and overarching terms, such as the interest rate and 100% guarantee.

The Scheme was launched less than two weeks after the Chancellor of the Exchequer proposed it to BEIS and the Bank.

HM Treasury data show that, as of 24 January 2021, the Scheme had delivered almost 1.5 million loans to businesses, totalling £44.7 billion.

Selected findings from our report

Strategy and governance: Ministers accepted a high degree of fraud and error risk in order to facilitate faster lending to smaller businesses. The pre-Scheme fraud risk review found that, while some risks can be mitigated, there remained a "very high level" of residual fraud risk caused by self-certification, multiple applications, lack of legitimate business, impersonation and organised crime. BEIS's accounting officer (AO) sought a Ministerial Direction before the Scheme's launch on all four accounting officer assessment criteria: regularity; propriety; value for money; and feasibility because of the level of credit and fraud risk and uncertainty associated with the Scheme. The Bank raised similar concerns through a Reservation Notice to BEIS's AO.[3]

Design: The government imposed less strict eligibility criteria for the Bounce Back Loan Scheme than other COVID-19-related business loan schemes, to improve quick access to finance for smaller businesses. It relies on businesses self-certifying application details with limited verification and no credit checks performed by lenders for existing customers. This lower level of checks presents credit risks as it increases the likelihood that loans are made to businesses which will not be able to repay them, leading to losses of taxpayers' money. The Bank and BEIS developed their approach over time to tackle some known credit and fraud risks. For example, lenders initially had no way of identifying multiple applications made across lenders. The Bank worked with lenders and counter-fraud groups to develop a methodology to tackle this risk, which it subsequently implemented on 2 June 2020, within a month of the Scheme's launch. At the end of September 2020, BEIS put in place a service level agreement with the National Investigation Service to support it identifying and responding to fraud within the COVID-19 loan schemes.

Measurement: BEIS and the Bank will not know the full extent of loss until the loans are due to be repaid. They made a preliminary estimate that 35% to 60% of borrowers may default on the loans, based on losses observed in previous programmes which are most similar to the Scheme. Using the amount lent as at January 2021 of £44.7 billion, this would imply a potential cost to government of £16 billion to £27 billion, but these estimates are highly uncertain.[4] Since reporting, BEIS and the Bank are in the process of using a loan book sampling approach to produce an estimate that isolates losses due to fraud.

Debt recovery: The loans are due to start being repaid from 4 May 2021. Government provides a 100% guarantee to lenders owing to the absence of credit checks, but this reduces the lenders' incentives to recover money from borrowers. If a borrower does not repay the loan, lenders are still expected to try to recover the loan, but they can claim on the government's guarantee "within a reasonable time period" or if no further payment is likely. Any outstanding debt collected by the lender after the guarantee has been claimed should be paid back to the government.

3 A Reservation Notice is a mechanism in the Bank's constitution through which it may raise concerns on particular grounds.

4 The preliminary estimate does not reflect changes to the Scheme announced by the Chancellor of the Exchequer on 24 September 2020, including extending the end date of the Scheme. Changes also included flexibility for the borrowers in difficulty to take payment holidays, temporarily pay only the interest on the loans or extend the repayment period.

Case study 2: Renewable Heat Incentive

Our 2018 report on *Low-carbon heating of homes and businesses and the Renewable Heat Incentive* (RHI) considered government's response to the risk of non-compliance with the scheme. Our report found that Ofgem's estimate for non-compliance was not reliable and that the governance processes in place did not effectively facilitate BEIS's oversight of the level of non-compliance, and therefore overall value for money, of the scheme. Ofgem and BEIS have subsequently made improvements in respect of the report's findings. This has led to improvements in the management of compliance on the RHI schemes.

About the RHI Scheme

The RHI scheme seeks to encourage a switch from fossil fuel heating systems to renewable and low-carbon alternatives. It was designed to support government meeting EU renewable energy obligations and UK statutory carbon reduction targets.

BEIS is responsible for the design, performance and overall value for money of the RHI in Great Britain.

Ofgem administers the two parts of RHI on BEIS's behalf:

- payments to homeowners, self-builders and private and social landlords are administered under the Domestic RHI (DRHI) scheme; and
- payments to industry, businesses and public sector organisations are made under the Non-domestic RHI (NDRHI) scheme.

The NDRHI scheme closes to new applicants on 31 March 2021 and the DRHI scheme will close to new applicants on 31 March 2022. Between November 2011 and August 2017, total payments under the RHI amounted to £1.4 billion. Final payments for applicants are set run to 2028-2029 for DRHI and 2040-41 for NDRHI, by which time total RHI payments are expected to have cost £23 billion.

Under RHI, Ofgem pays accredited participants money in the form of a tariff for each unit of heat produced from renewable sources using eligible technologies. Examples of non-compliance include: using the heat for an ineligible purpose; using an unsustainable fuel source; not providing the correct, up-to-date, information about installation to Ofgem; and incorrectly metering the amount of heat used.

Selected findings from our report

Strategy and governance: The part of Ofgem that administers RHI, including accrediting the scheme, was also responsible for estimating rates of non-compliance. BEIS holds Ofgem to account on how effectively it administers the scheme (including minimising rates of non-compliance), so there was consequently a risk to independence and objectivity. BEIS did not review Ofgem's estimate and was unaware of its unreliability. Since we reported in 2018, Ofgem has restructured its governance by separating the part of Ofgem responsible for RHI accreditation from its audit and compliance teams and creating a central assurance team to provide an independent perspective on its audit and compliance work. Furthermore, Ofgem now uses a separate Analytical Assurance Team to quality-assure its estimate of non-compliance and BEIS has increased its oversight of the estimate, including requiring its analytical team to review the methodology.

Measurement: NAO identified several issues with Ofgem's non-compliance estimate and the way in which it was reported, for example:

- Ofgem did not ensure its audit sample was representative of the overall scheme population;
- there were weaknesses in key assumptions underpinning the estimate for overpayments under NDRHI;
- Ofgem reported its estimate of non-compliance to BEIS as a single 'point estimate', which ignores the significant uncertainty inherent in the sampling methods used; and
- NAO identified a significant understatement error in the estimated non-compliance rate for the DRHI scheme.

Since reporting, Ofgem has worked to address each of the issues listed above. BEIS reported in its 2019-20 accounts that the most likely estimated value of non-compliance for 2019-20 was £17.3 million or just under 3% of the RHI scheme spend in that financial year, representing a fall in the estimated rate against 2018-19.

Evaluation: Without a reliable estimate of the financial impact of non-compliance to provide a baseline, Ofgem was unable to measure the effectiveness of the actions it took to reduce non-compliance. Where Ofgem identified non-compliance with a large financial impact through audits, its subsequent actions to address the root cause were often incomplete, and sometimes not present at all. Performing more audits without addressing the root causes of non-compliance is unlikely to reduce non-compliance as the same errors will continue to occur. The recent improvements made to governance arrangements and statistical methodologies for the estimate should contribute to Ofgem developing a more reliable baseline to assess the effectiveness of its non-compliance activity. Ofgem told us that it is now working to apply these lessons to inform its wider risk strategy for other government schemes it administers.

Case study 3: HMRC's Employment Support Schemes

In our 2020 report *Implementing employment support schemes in response to the COVID-19 pandemic*, we considered government's response to the fraud and error risks of the employment support schemes that it set up to provide financial support in the wake of the pandemic to protect jobs. We reported that HM Revenue & Customs (HMRC) and HM Treasury set up the schemes quickly and accepted a higher level of fraud and error risk than normal in order to do so. HMRC conducted a detailed initial risk assessment on both schemes to establish the key risks and the departments used the existing tax system to mitigate some of the risks identified. Despite mitigations, control weaknesses mean that initial estimates of fraud and error on the schemes are significant. Further measurement will support accountability and provide the opportunity to inform the design of future services.

About the Employment Support Schemes

Coronavirus Job Retention Scheme (CJRS): CJRS enables employers to continue to employ workers during the pandemic by placing them on furlough and claiming government support. Employers can claim back employee wages up to a maximum of 80% of their wages or £2,500 per month. The scheme began on 20 April 2020 and, after extensions, is currently set to end at the end of April 2021. By December 2020, the scheme had supported 9.9 million jobs at a cost of £46.4 billion.

Self-Employment Income Support Scheme (SEISS): SEISS was initially set-up to ensure that the self-employed could get income support during the pandemic if their business was adversely affected. Self-employed taxpayers were invited to apply for the scheme and HMRC calculated their entitlement based off the taxpayer's previous tax returns submitted. By December 2020, SEISS had at least 2.6 million claims, totalling £18.5 billion.

Key fraud and error risks associated with the schemes include:

- employers claiming money while their furloughed employees continue to work;
- self-employed individuals inflating their claims in late Self Assessment returns; and
- organised criminals hijacking agents' details to submit fraudulent claims.

Selected findings from our report

Strategy and governance: HMRC conducted a detailed initial risk assessment on both schemes to establish the key fraud and error risks. It recognised it would need to make trade-offs, accepting higher risk levels in order to ensure that money reached claimants quickly (a ministerial priority) as it did not have time to put in place all relevant controls before the schemes started.

Design: HMRC reduced the fraud and error risk by ensuring claims were linked to existing tax records. Furlough fraud, such as where employers claimed CJRS despite their employees still working, was assessed as highly likely. HMRC had limited controls over employers' arrangements with employees and considered that pre-payment checks were impractical within the required timeframes to provide support quickly. Therefore, HMRC was mainly reliant on whistleblowing and retrospective compliance work to detect furlough fraud.

Measurement: Despite mitigating some known risks, the scale of fraud and error on the schemes is likely to be considerable, particularly for CJRS, but HMRC will not know the actual levels for some time. HMRC's initial analysis assumed fraud and error rates of 5% to 10% for CJRS and 1% to 2% for SEISS. HMRC is looking to understand the full scale of fraud and error but it does not expect to have a complete estimate until the end of 2021 at the earliest.

Evaluation: HMRC and HM Treasury are unable to fully evaluate the effectiveness of the approach taken without a full fraud and error estimate. HMRC has, however, reacted to emerging evidence of furlough fraud by introducing new controls and more transparency on the use of CJRS; it told us that employees are now being made directly aware of their furlough status and data on which companies are claiming furlough payments are being made public.

Debt recovery: At the time of reporting, HMRC had made three arrests in relation to suspected CJRS fraud. It plans to redeploy 500 full-time equivalent staff to enable post-payment compliance work and assessed that this work would bring in around £275 million. The work offers a positive return on investment (we estimate around 9:1), but will be subject to opportunity costs from staff redeployment.

Case study 4: Packaging Recycling Obligations

Our 2018 report on *The packaging recycling obligations* considered the risk of non-compliance with the associated regulations. We reported that the Environment Agency performed significantly less compliance visits than it planned but still believed its compliance approach to be proportionate. The Environment Agency did not estimate the level of non-compliance in the system and therefore could not demonstrate that its approach to tackling non-compliance was cost-effective. It informed us that since our review it has made significant changes to its approach to tackling fraud and error, including introducing quality checks on compliance visits.

About the packaging recycling obligations

The government introduced the packaging recycling obligations in 1997 in order to implement an EU Directive requiring member states to meet packaging recycling targets. In 2017, obligations applied to 7,002 companies in the UK that made and sold packaged goods (such as supermarkets) or manufactured packaging.

The regulations allow for packaging to be collected, sorted and recycled as part of the normal management of waste in the UK. Accredited recyclers (companies that recycle material in the UK or export it for recycling abroad) can then issue recovery notes for the amount of packaging they have recycled and sell these notes to obligated companies or compliance schemes. In 2017, 93% of producers were registered with compliance schemes that will take on its legal obligation in exchange for membership fees.

The Department for Environment, Food & Rural Affairs is responsible for waste and packaging policy in England, and for monitoring of overall progress against the UK-wide packaging recycling targets. The Environment Agency is responsible for enforcing the regulations in England.

Examples of where compliance risks arise include:

- obligated companies do not self-register with the packaging recovery notes system as required;
- obligated companies (or the compliance scheme of which it is a member) inaccurately reports the amount of packaging produced; and
- recyclers over-issue recovery notes.

Selected findings from our report

Implementation: The Environment Agency performs compliance visits to check that recyclers make accurate claims for the amount recycled. In 2016-17 the Environment Agency carried out less than 40% of the number of compliance visits it planned to (124 visits compared with a target of 346). The total number of visits performed had fallen significantly in prior years. The Environment Agency did not carry out any central checks on the quality of compliance visits that would enable it to identify control weaknesses.

Since reporting, the Environment Agency told us that it has now established a central team to carry out quality checks, and therefore ensure consistency, on its compliance visits. It also told us that it has significantly increased the effectiveness of inspections, with an estimated £30m of fraud prevented in 2019 and 21 of the 47 formal enforcement interventions since 2012 taking place in the last few months of 2020.

Measurement: The Environment Agency had not estimated the amount of fraud and error in the system and the Department for Environment, Food & Rural Affairs had not requested this analysis to inform its oversight. We found that the Environment Agency has particularly low visibility and control over waste that is sold for recycling abroad. In 2017 these exports accounted for 50% by weight of material recycled through the scheme in the UK. The Environment Agency told us it believed its compliance approach to be proportionate despite the absence of an estimate.

Evaluation: Without measuring the financial impact of fraud and error risks, the Environment Agency is unable to evaluate whether its approach to tackling fraud and error is cost-effective. For example, the Environment Agency identified a large number of 'free riding' companies that may have an obligation to pay into the system but have not registered. However, without an understanding of how significant the financial risk of 'free riding' is, the Environment Agency does not have the information required to assess whether its compliance approach is proportionate. Since we reported, the Environment Agency told us that, although it still does not have a quantified estimate for fraud and error in the system, one way which it iterates its approach to tackling fraud and error is by using the results from completed compliance visits to inform its risk assessment that it uses to target future visits.

Case study 5: Department for Work & Pensions' Benefit Expenditure

Fraud and error in benefit expenditure is at its highest recorded level and is expected to continue to rise. The Department for Work & Pensions (DWP) does, however, have a good understanding of what types of fraud and error occur. It is committed to tackling fraud and error and is taking steps to embed a counter-fraud and error culture across the Department, in addition to investing in new data technologies.

About DWP's benefit expenditure

DWP is responsible for administering the benefit system. In 2019-20, DWP spent £191.8 billion on benefit payments to claimants.

The Comptroller and Auditor General has qualified DWP's accounts every year since 1988-89 due to the material level of fraud and error in benefit expenditure, providing an explanation for his qualification in his annual report on DWP's accounts.

In 2019-20 DWP estimated that it overpaid £4.6 billion and underpaid £2 billion of benefits, recording rates of 4.8% of overpayments (its highest ever recorded rate) and 2% of underpayments across all benefits, excluding State Pension which is believed to have very low levels of fraud and error.

The rate of fraud and error has been rising for the past few years despite efforts by DWP to tackle it. This is in part due to the roll-out of benefits with more complex entitlements, some new risks from digitalisation and, in places, prioritising efforts relating to other policy priorities, such as payment timeliness, ahead of efforts to tackle fraud and error.

DWP made changes to benefit delivery in response to COVID-19 when the number of people on Universal Credit rose from 2.9 million in February 2020 to 5.6 million by August 2020. This included turning off some controls (also referred to as easements) used to mitigate the risk of fraud and error. The increase in caseload and DWP's easement of controls mean the rate of fraud and error is expected to increase substantially in 2020-21.

Selected findings from our recent work

Strategy and governance: DWP's Fraud, Error and Debt strategy focuses on understanding and addressing the systemic causes of fraud and error. It produces 'heat maps' at an overall level and for individual benefits that are measured in-year which show the monetary value of fraud and error (MVFE) relating to each key eligibility criteria. This enables operational teams to focus in on the risks specific to the benefits they manage. DWP has recently committed to set a fraud and error target once it has established a clear baseline in the wake of the COVID-19 pandemic.

Design: DWP has made good use of data-matching to prevent and detect fraud and error; for example, it has been using HMRC's Real Time Information feed since 2013, which provides regular information on claimants' employment and pension income. For some key risks, however, it lacks access to accurate and timely data that would help it perform effective data-matching and is looking into new data sources where existing sources are insufficient.

Implementation: Where DWP has increased resources in controls it has improved detection rates. Our *Investigation into overpayments of Carer's Allowance* found that the DWP detected 93,000 overpayments in 2018-19 compared with an average of 41,000 a year detected in the previous five years. Notably, DWP increased the number of full-time equivalent staff investigating data matches on Carer's Allowance to an average of 52 in 2018-19 from an average of around 12 per year dating back to 2011-12.

Measurement: DWP has ensured good transparency over its levels of fraud and error and performs a significant annual sampling exercise (MVFE) to inform its published estimate; it reports this estimate in its Annual Report and Accounts and a separate statistics release. However, the sampling does not cover all benefits, meaning some estimates are out of date, and the estimate is also concentrated on risks that DWP is confident it can measure. There is less focus on risks, such as cybercrime, that are inherently more difficult to detect.

Evaluation: DWP's next step is to understand fraud and error risk at a control level so that it can assess the cost-effectiveness of individual controls and target improvements and investment accordingly. Lessons from the easements to controls in response to COVID-19 will help DWP to evaluate the effectiveness of controls as it understands the impact of removing or reducing, then reintroducing controls.