Palantir

Rethinking public sector fraud

Proposing a counter-fraud operating system across government

Palantir Technologies
→ palantir.com

April 2022

Palantir

Introduction

Executive summary

The pandemic did not create the problem of public sector fraud, it has only intensified it. While the estimated £12 to £20 billion lost to fraud and error across Covid-19 support schemes[1] has attracted significant criticism, the Government was already losing an estimated £29.3 billion to £51.8 billion to fraud and error per year prior to the pandemic.[2]

The trade-off between speed and control imposed by Covid-19 could have been mitigated. If government departments were able to share information and collaborate more easily — and the right data was available at the right time — many simple fraud controls could have been implemented quickly, saving billions of pounds of taxpayer money.

Without concerted effort, levels of public sector fraud will only increase, sapping much needed financial resources that should be used to fund vital services and undermining trust in government. Departments' operations and supporting IT estates are struggling to keep up with new policy initiatives, making it hard to manage fraud risk. The push to make more government services digital is also creating new opportunities for cyber-crime and online fraud. For example, it is thought that a significant number of criminals have taken advantage of the relaxed controls during Covid-19 to enter the system and verify their digital identities with the government, thus increasing the risk of further fraud.

Tackling fraud effectively requires different teams to share information and work together, but this is currently hard to do. Essential data is stuck in siloes and governance regimes hinder collaboration both within departments and across government. In addition, front-line teams — often the best placed to spot new fraud patterns — are not empowered to make improvements to systems; rigid, inflexible IT systems further inhibit these improvements; and evaluating the effectiveness of counter-fraud measures is difficult.

A fundamental shift in thinking is required. Simply introducing more point solutions, more people and more processes will never achieve the necessary step change in the government's counter-fraud capacities. This kind of 'wicked problem' often breeds inertia because it seems beyond the power of any single player to solve. But significant levels of fraud do not - and should not - have to be accepted as simply a transaction cost of government.

Palantir

We propose a "counter-fraud operating system" that connects existing IT infrastructure and empowers teams to work together. Rather than building new infrastructure, we recommend deploying software that enables existing systems and teams to work together. This would enable government to make the most of its current counter-fraud capabilities — and enable improvements to be delivered quickly and cost-effectively, with minimal disruption.

We have already proven that this approach works in government. We have supported a number of UK public sector bodies to use our Foundry software to coordinate multiple teams and stakeholders, across different organisations, and deliver complex projects under immense time pressure, including The Cabinet Office, NHS England and the Ministry of Defence.

Understanding the problem

The pandemic has put the problem of public sector fraud back in the spotlight.

Over the past two years, public servants across the UK have overcome enormous challenges to deliver services which saved the lives and livelihoods of millions. [5]

These programmes shielded millions of people and businesses from hardship, but they came with a trade-off. The latest estimates suggest that more than £15 billion has likely been lost to fraud and error across various support schemes introduced or expanded during the pandemic[6]. That is enough to fund approximately 11,000 new homes for social renting,[7] or deliver a 10 percent pay-rise for front line NHS staff, while training an additional 185,000 nurses.[8]

The trade-off between speed and control was not inevitable.

Some have argued that the urgency imposed by Covid-19 inevitably entailed a trade-off between speed and control. Yet this trade off could have been minimised if civil servants had access to digital infrastructure that allowed them to collaborate and implement counter-fraud strategies rapidly.

As the National Audit Office has highlighted, many simple fraud controls could have been easily implemented within programmes like the Bounce Back Loan Scheme, saving billions of pounds in tax payer money if the right data was available at the right time.[8]

Public sector fraud is likely to get worse without decisive action.

Covid-19 intensified the challenge of public sector fraud, but it did not create it. In 2018-19 alone, the Cabinet Office estimated losses between £29.3 billion to £51.8 billion due to public sector fraud and error.[10]

Palantir

Without concerted effort, levels of fraud will only increase, as departmental IT and organisational systems struggle to adapt quickly enough to manage new policy imperatives and operational requirements. For example, based on the experience of past expansions, as Universal Credit expands in scope, fraud risks are likely to multiply.

The push to make more government services digital is also increasing the pressure on counter-fraud teams and creating new opportunities for cyber-crime and online fraud.

For example, a significant number of fraudsters took advantage of periods of reduced due diligence during the pandemic to enter the system, leveraging digital techniques to steal identities and validate them with the government's new online verification services.[11]

It is against this backdrop that the Public Accounts Committee has expressed its frustration at HMRC's lack of a clear plan to recover money lost to fraud or restore compliance activity back to even pre-pandemic levels.[9]

→ Real-world example: Covid-19 business support loans

The lack of ability to share information between organisations made it difficult to prevent fraud in the Covid-19 business support loan schemes delivered jointly by BEIS, the British Business Bank and various accredited lenders. Implementing even the basic counter-fraud controls of cross-referencing loans against corporate registry data (held by BEIS), corporate taxation records (held by HMRC) and miscellaneous law enforcement data sources took almost a year in some cases — by which point more than half of the total loan value had already been distributed.[12] This constraint on information sharing is prevalent across government, hampering counter-fraud efforts even in long-established programmes.

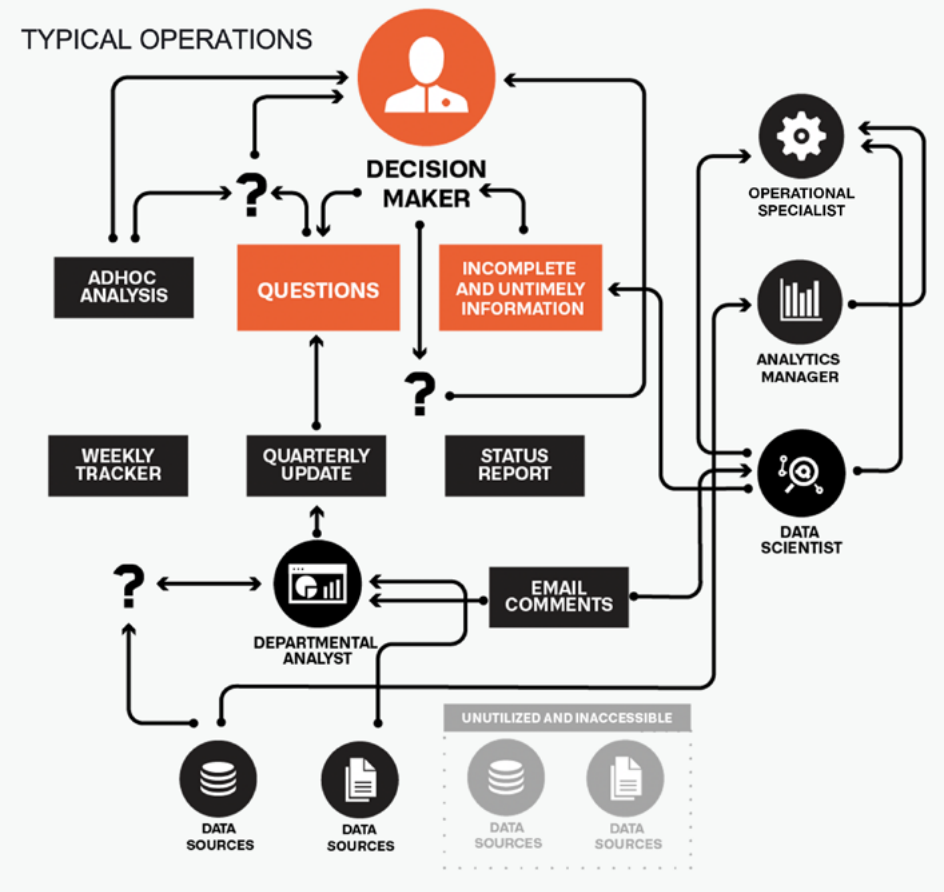

Figure 1: What data-driven operations typically look like under the hood

Palantir

Despite the best efforts of government counter-fraud teams, existing systems make it hard to tackle the challenge:

1 Data is stuck in siloes

Essential counter-fraud data is stuck in siloes within and across organisations, often locked in incompatible formats or in IT systems which struggle to interoperate. Even when information from different systems can be brought together, this usually takes a significant amount of time and resources, which means it is difficult to understand and respond to fraud risks quickly.

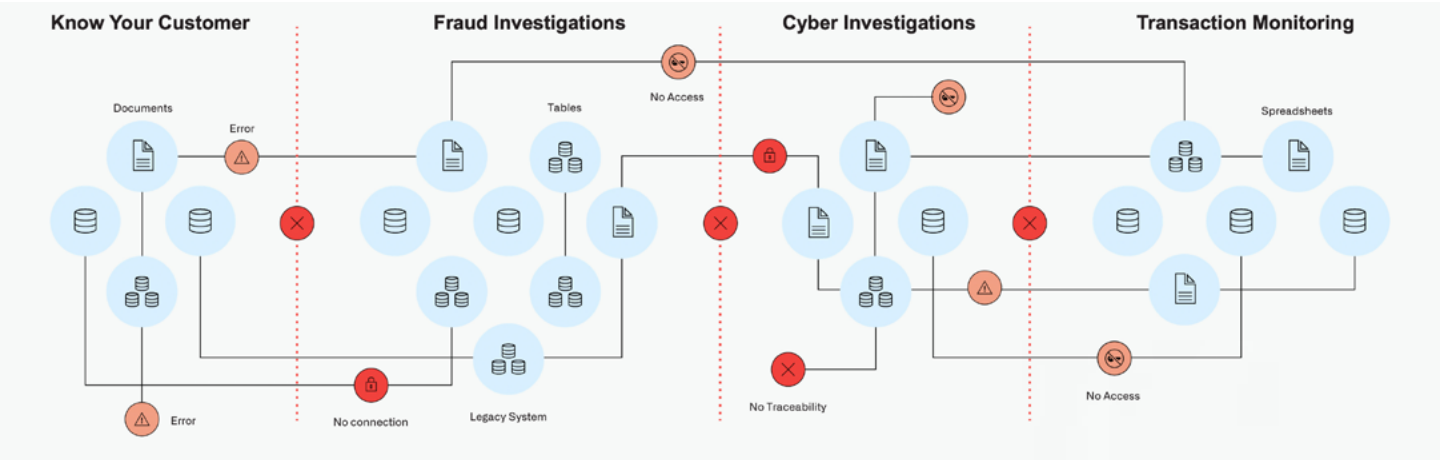

Figure 2: Siloes across typical fraud functions making access to data and collaboration difficult

2 Departments struggle to manage the governance required to enable data sharing and collaboration

Fraud investigators often need access to highly sensitive data such as tax records, meanwhile data controllers must be able to tightly control who accesses sensitive personal data in order to protect individuals' privacy. Unfortunately, current access control tooling makes this hard to achieve this, instead often producing an 'all-or-nothing' dynamic. Overworked data controllers are forced to choose between provisioning overly broad access to data, or simply denying access wholesale.

3 Front-line teams are disempowered

Operational staff such as caseworkers, investigators and commercial professionals are best- placed to spot gaps in the system and identify new fraud threats. However, this knowledge is often lost because there is no direct feedback loop between most departments' operational and analytical functions. Hard won counter-fraud insights developed by front-line teams cannot easily be encoded as business logic and generalised across the organisation, usually due to overly regimented IT systems that create bottlenecks.

Palantir

4 Inflexible IT systems inhibit improvement

Public sector bodies typically rely on either black box IT systems that require a third party to manage or bespoke software that hard codes specific counter-fraud processes and workflows, making them hard to modify. Either option can make it difficult and expensive to reconfigure systems or introduce new functionality. As a result, it is hard to change tack in response to emerging fraud patterns.

5 Evaluating the effectiveness of counter-fraud measures is difficult

Counter-fraud and error measures should be evaluated for their effectiveness and value for money, while taking into account other policy objectives. Yet departments struggle to measure the true costs and benefits, because the systems used to detect and prevent fraud don't connect with those used to action cases or track departmental activity and downstream impact. It is also hard to identify whether counter-fraud activity in one part of government results in savings in another, e.g. when fraudsters tackle multiple departments, as this data is usually not shared.

Emerging counter fraud challenges

→ The Department for Business, Energy & Industrial Strategy (BEIS) is set to play a key role in the government's Net Zero Strategy, investing billions of pounds in decarbonisation initiatives, which could create new opportunities for fraudsters. For example, in the latest spending review, the government announced more than £3.9 billion in funding for homeowners, local authorities and other entities seeking to make improvements which support decarbonisation. Such schemes tend to be highly vulnerable to fraud, with authorities often struggling to confirm that qualifying work has actually taken place.

→ Following its successful rollout, the Department for Work and Pensions (DWP) is preparing to expand the scope of Universal Credit (UC), integrating more benefits and support schemes into UC, including tax credits which are currently managed by HMRC. As UC expands in scope to support an ever greater number of citizens, fraud risks (and the administrative burden of managing them) will inevitably multiply.

→ The Cabinet Office has been charged with coordinating and developing the counter-fraud function across government. It also has direct operational counter-fraud responsibilities in certain areas like grant management. To achieve these goals it needs to be able to understand a broad range of public sector fraud risk and deliver capabilities that departments can use to address them. It is therefore placing a strong emphasis on data sharing and analytics, sponsoring pilots across government to promote greater interdepartmental cooperation.

Palantir

- → In order to support cutting-edge research, HMRC has committed to reforming tax credits for research and development (R&D), in part by expanding qualifying expenditure to include data and cloud costs. However, the increasing scope and value of these tax credits will create additional compliance risks. For example, to capture the full benefits of the policy and reduce fraud, HMRC must be able to validate that the R&D activity companies claim for is actually taking place in the UK and not overseas.

- → The Department of Levelling Up, Housing and Communities (DLUHC) has been tasked with delivering the levelling up agenda. This will involve shifting resources to local authorities so that they can deliver vital public goods like better integrated public transport systems, full 5G broadband coverage, and improved health and educational outcomes. Consequently, they will be managing more resources across a wider breadth of policy areas, often without additional administrative capacity. This will create additional fraud risks which DLUHC and local authorities must be able to contain.

Achieving a step change: visualising a common operating system for fraud

In our experience, the UK public sector has extremely capable fraud experts. Often the biggest challenge is how to connect this expertise both within and across departments.

Tackling fraud effectively requires much deeper integration across the government counter-fraud enterprise, including operational teams like field agents and investigators; the analytics and data science teams that develop new fraud indicators; the data engineering and technical teams that manage operational systems; the governance and compliance teams that ensure all activity remains appropriate and proportional; and the policy teams that design services and set overall counter-fraud strategy.

This integration has to happen at two levels: technical (i.e. bringing data and IT landscape together), and operational (i.e. connecting processes and workflows to enhance collaboration and continuous learning).

Delivering this kind of transformation requires dealing with a great deal of complexity. Each department has its own set of unique processes, digital infrastructure, information repositories, policy imperatives and organisational structures.

Removing this complexity, for example by replacing government IT systems wholesale, is not realistic. Instead, we propose a pragmatic solution that enables officials to work together within this complex domain.

Below we describe how this approach can deliver step change improvements, drawing on our experience of working on fraud reduction programmes and complex data challenges across the public and private sectors.

How to deliver it

1 Start small and demonstrate impact quickly

The scale and scope of counter-fraud activity is usually too large to tackle all at once. Different teams inevitably have different priorities, which makes it difficult to generate alignment. Projects can quickly get bogged down with internal politics or lose steam as more urgent issues take up attention.

In our experience, it is best to start with a pressing, well-defined problem that generates energy and focus. It should also be associated with a measurable outcome so that value can be demonstrated in the space of weeks, rather than months. Nothing builds momentum like getting results.

Establishing proof-of-concept quickly is essential to overcome resistance to change and the natural tendency of individuals and organisations to revert to the status quo.

→ Real-world example: preventing $22 billion of fraud at a US Federal Agency

At the start of the pandemic, a major US Federal Agency was tasked with administering economic support schemes similar to those delivered in the UK. Within a matter of weeks, it had more than 30 million loan applications amounting to more than $1 trillion in loan value. The agency used Palantir's Foundry software to prevent organised criminals from committing serious fraud, without compromising the speed at which legitimate applicants received vital aid. Within a few weeks, the agency had integrated more than 50 data sources, linked billions of records of new information to the loan applications, and made this available to more than 2,000 field agents via an easy-to-use interface. This data asset was pivotal in enabling agents to flag more than $22 billion of suspected fraudulent transactions before any payment was made.

2 Build a business-centric view of the relevant data landscape — old and new — in real-time

The systems that hold critical information on fraud risk may vary considerably depending on the entity in question, the specific fraud typologies being addressed and the use-cases that need to be supported.

Rather than seeking to replace these different systems, government needs to build a system that interconnects them. This must go beyond traditional data lakes and warehouses that all too often leave the users navigating a large swamp of data with little idea of what data to trust. The system needs to translate the underlying data into the language that end users are already familiar with, rather than abstract rows and columns that require a steep learning curve to work with.

Another advantage of this approach is that for each analysis the software draws data from the underlying databases, which continue to be maintained by their owners as usual. This enables the user to get a real-time picture of fraud risk, rather than creating duplicate databases that require constant upkeep and quickly get out of date.

Palantir

3 Share data without sacrificing control

Technically integrating data is only the start. Organisations also need the capacity to make data available to users in compliance with governance policies. This will require cross-governmental governance frameworks that enable departments to share information both internally and with each other as appropriate.

Our approach to this is to embed a technical framework which we call Purpose Based Access Controls (PBAC). The PBAC mechanism allows controllers to control not only who can access what data, but also place limits on how the data can be used by associating all access with a specific processing rationale. This ensures that data access is provisioned in a way that is proportionate to the purpose, for a defined period of time, with all access fully auditable to detect any intentional or unintentional misuse.

At the Cabinet Office, Foundry's PBAC framework is being used to facilitate data sharing across five government departments — the Home Office, HMRC, Defra, DIT and DfT — to ensure that the UK's borders continue to function well following Brexit.

→ Real-world example: enabling the NHS England to share sensitive data in a highly controlled way

Through the pandemic, the NHS England has had to effectively and fairly allocate PPE, ventilators and vaccines. The team has used Foundry to build a national data asset that integrates more than 350 data source systems from hundreds of hospitals and Trusts, as well as loose Excel files on GPs' computers. It was essential to find a controlled way of managing access to this sensitive data, which included public health records. For this purpose, data governance officers at the NHS England relied on Foundry's PBAC model. Having this kind of sensitive governance capacity built into the software meant it was much easier to approve appropriate requests and enable collaboration. Within the NHS England, it allowed over 16,000 users to interact with 450 data assets in a compliant manner and develop intelligent applications to support the Covid-19 response.

Palantir

4 Build in feedback loops

Putting in place the technical and governance mechanisms to share data is essential, but it is not enough. An effective counter-fraud system needs to enable all the different players involved to collaborate, from risk intelligence and fraud investigation teams, to cyber security, data science and data engineering teams. The ideal is to establish powerful counter-fraud 'hive mind' where insights and innovation are shared continuously and ubiquitously.

However, each of these teams are typically confined to their own analytical and operational environments. It is these environments that hold existing information about tactics, techniques, and procedures of fraudsters and innovative counter-fraud approaches developed by individual teams.

→ Real-world example: enabling teams to work together to quickly develop new fraud indicators

One of the challenges for the US Federal Agency that we have been working with during the pandemic is that its counter-fraud analysts, field agents, and data scientists are based in different cities, with many working from home. This made collaboration laborious and ineffective. The teams used Foundry to develop and deploy new fraud indicators within a few weeks by combining their collective knowledge. These new indicators automatically surfaced more than 100,000 high conviction leads amounting to billions of dollars in potential fraud. As they go about investigating these leads, their decisions and the outcomes of investigations is fed back as data into the system. As a result their risking models and quality of indicators continue to improve over time.

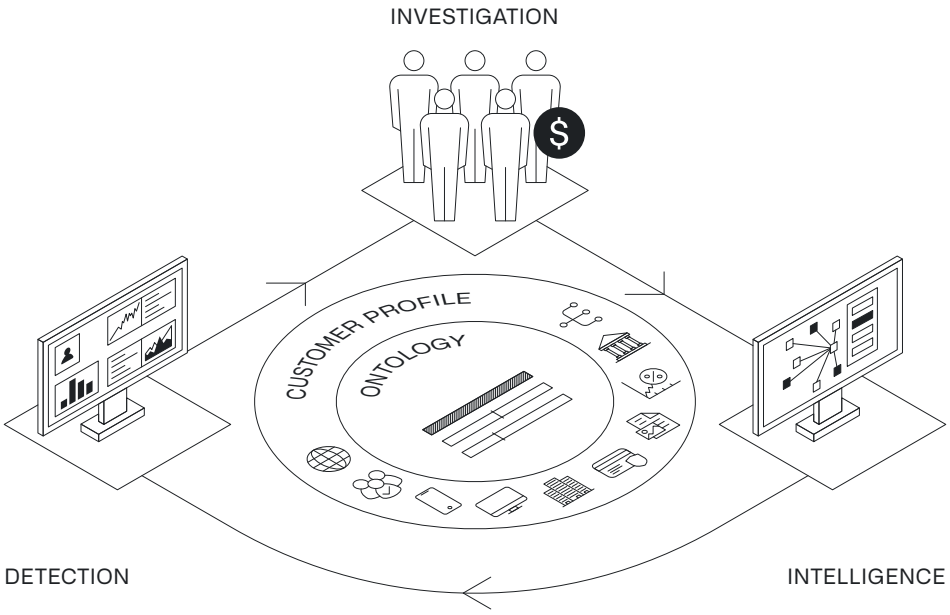

Figure 3: A model for integrating analytical and operational counter-fraud systems

A common operating system for counter-fraud needs to act like a connective tissue that enables these different environments to feed into one another. Rather than relying on separate teams or long iterations with vendors to implement and refine control strategies, each team needs to be empowered to identify and make improvements to the overarching control regime directly.

This means that all users need to be able to take full advantage of their department's internal data asset, quickly develop and deploy new risking and fraud detection strategies and capabilities, and incorporate information sourced externally from other departments and entities.

This will allow counter-fraud systems to not only identify new patterns quickly, but also provide signals to improve processes and react to new fraud risks in an agile way.

Our work with the UK government

We have already supported a number of UK public sector bodies to deliver complex projects under immense time pressure using our Foundry software and the approach outlined above. We helped them create a common data foundation and enable multiple teams (and organisations) to collaborate and track the impact of their decisions. This includes:

→ The Cabinet Office, which delivered the Border Flow Service in four months. This brought together data from five border-facing departments and enabled different agencies to collaborate to ensure the smooth flow of passengers and trade over the UK border post-Brexit.

→ NHS England, which stood up one of the UK's largest supply chains to manage the Covid-19 response within less than six weeks using Palantir's Foundry software. This spanned manufacturers, ports, freight forwarders, hospitals, trusts, and GPs, and delivered more than two billion articles of PPE. The same approach was subsequently used to deliver every single vaccine dose administered in England to date.

→ The Ministry of Defence, which is responding to a rapidly changing geo-political climate and working to ensure the continuing safety and security of the UK and its people abroad.

Conclusion

Building data driven counter-fraud operations requires a shift in thinking. A narrow focus on individual point solutions that solve a specific sub-set of the overall problem will never achieve the necessary step change in the government's counter-fraud capacities.

What is required is a connective tissue that brings tools, data, and teams together in a way that fuels collaboration — a common operating system. If the government can break down siloes between teams, technology and processes — using tightly governed interoperable software — it will be able to roll out new policy initiatives much more quickly and save billions of pounds in money lost to fraud.

Our experience of working with NHS England and the Cabinet Office, as well as with government agencies in the US, shows what is possible when this connective software and an institutional commitment to collaboration is in place.

Palantir Technologies UK, Ltd. stands ready to support UK Public Sector in the fight against fraud

If you would like to find out more, please contact

↘

ukgov@palantir.com

Palantir

References

This paper is intended for informational and discussion purposes only. Nothing herein constitutes a guarantee, representation, or warranty of any kind, including as to any future outcomes. These materials may contain data, estimates and forecasts that are based on external publications or other publicly available information, as well as other information based on internal resources and estimates. This information involves many assumptions and limitations. Palantir has not independently verified the accuracy or completeness of the data contained in these industry publications and other publicly available information. Accordingly, it makes no representations as to the accuracy or completeness of that data nor does it undertake to update such data after the date of these materials. The inclusion of such references to publicly available data or other information does not constitute an endorsement of such referenced materials or the underlying, third-party data or information.

[1] House of Commons Committee of Public Accounts, COVID-19 cost tracker update (HC 2021-22 640), pg. 12.

[2] House of Commons Committee of Public Accounts, Fraud and Error (HC 2021-22 253), pg. 3.

[3] National Audit Office, The Bounce Back Loan Scheme: an update

[4] See for example: National Audit Office, Universal Credit advances fraud (HC 2019-21 105), which describes how it took DWP over five months to identify the magnitude of an emerging pattern of fraud and then a further six months to develop a response strategy.

[5] By mid-April 2021, the Department of Work and Pensions (DWP) had fielded nearly one million new Universal Credit applications - a ten-fold increase on pre-pandemic levels. Over the course of the pandemic, more one in four UK employees were supported by the furlough scheme at some point; and businesses were backed by nearly £80 billion of emergency loans. Sources:
Andrew Mackley, Coronavirus: Universal Credit during the crisis, House of Commons Library Briefing Paper (CBP 8999), January 2021
HM Revenue & Customs, Coronavirus Job Retention Scheme statistics: 16 December 2021
Georgina Hutton and Matthew Keep, Coronavirus business support schemes: Statistics, House of Commons Library Briefing Paper (CBP 8938), January 2022

[6] HC 2021-22 640

[7] Based on estimate prepared by the National Housing Federation cited in House of Commons Housing, Communities and Local Government Committee, Building more social housing (HC 2019-21 173), pg. 35

[8] For the estimate on cost of payrise, see London Economics, The net Exchequer impact of increasing pay for Agenda for Change staff, January 2021
For the figure for the cost of training nurses is derived from Health Education England, Workforce Plan for England 2015/16

[9] House of Commons Committee of Public Accounts, HMRC Performance in 2020–21 (HC 2021-22 641)

[10] HC 2021-22 253

[11] National Audit Office, Report on Accounts: Department for Work & Pensions (July 2021)

[12] NAO, Bounce Back Loan Scheme: an update