



HM Government

The Digital, Data and Technology Playbook

Government guidance
on sourcing and
contracting for digital,
data and technology
projects and programmes



June 2023



© Crown copyright 2023.

Produced by Cabinet Office.

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

Alternative format versions of this report are available on request from markets-sourcing-suppliers@cabinetoffice.gov.uk

Designed by Design102.

Contents

Foreword by Alex Chisholm	1	2 Successful relationships	22
Introduction – Right at the start	3	 Effective contract and portfolio management	22
What is new?	4	Building and maintaining supply chain relationships	22
Key policies	5	Flow down of contractual terms and conditions	23
Cross-cutting priorities	8	 Successful relationships and legacy IT	24
Taking an outcome-based approach	8	Strategic supplier relationship management	24
Avoiding and remediating legacy IT	8	 SME relationship management	24
Cyber security – Secure by design	8	3 Governance and approvals	26
Enabling innovation	9	Culture which manages risk and good governance	26
Driving sustainability	9	 Outcome-based Approach	26
Levelling the playing field for small and medium-sized enterprises (SMEs)	9	Project/Programme Outcome Profile	26
Procurement Reform	9	Cross-functional teams	27
Playbook flow diagram	10	Senior leadership buy-in	28
Applying the Digital, Data and Technology Playbook	12	Appropriately qualified SROs	28
Navigating the Digital, Data and Technology Playbook	13	Project Validation Reviews	28
 Preparation and planning	14	Government Major Contracts Portfolio	28
1 Pipelines and market management	14	DDaT assurance	29
Business strategy, priorities and demand	14	Technology Code of Practice (TCoP)	29
 Commercial Pipelines	14	Service assessments	29
Market management	15	4 Early engagement and enabling innovation	32
 Market health and capability assessments	15	 Early engagement	32
 The role of SMEs	16	 Enabling innovation	33
Using cloud to enable SME involvement	17	Technology Readiness Level (TRL) Scale	35
Artificial Intelligence (AI) and Machine Learning	18	Incentivisation	36
		SMEs	37
		 Clear, outcome-based specifications	38
		Product roadmaps	38

 Specifying cyber security requirements	38	 Publication	70
Transparency	39	8 Designing effective contracts with common data standards	70
The use of data in AI and Machine Learning	40	 Effective contracting	70
5 Delivery model assessments	48	Core Commercial Priorities	70
 Delivery model assessments	48	Risk allocation	70
Undertaking a DMA	49	Managing commercial risk	70
Agile delivery models	53	Key performance indicators	70
Benchmarking	53	Payment mechanism and pricing approach	72
Using Should Cost Models to understand whole life value	53	Onerous contracts	72
Using public sector demand strategically	54	Fair returns	72
6 Agile development – testing and learning	56	Digital, data and technology considerations	73
Iterative approaches to development	56	 Legacy IT and up-to-date products	73
Iterating against outcomes	56	Intellectual Property (IP)	74
 Testing and piloting solutions	59	 Cyber security risk	77
When to test or pilot	59	Physical and personnel security	77
Options for testing	59	 Open and interoperable data and software	78
Designing effective tests and pilots	59	 API technical and data standards	78
Testing data-based projects	60	Repair and reuse	79
Meeting the challenges of scaling	60	 Contractual terms and conditions for cloud	79
Design considerations	60	 Selection, evaluation and award	84
Commercial considerations	61	9 Developing evaluation criteria	84
7 Preparing to go to market	64	Ethos for evaluation	84
Commercial approach	64	Cost and quality	84
 Outcome-based approach	65	Robust evaluation processes	84
Contracting strategy	65	Testing evaluation criteria	85
Proportionality	66	 Delivering sustainability	85
Procurement procedure	66	Setting the tone	86
Use of frameworks	66		

Procurement timelines and transparency	86	 Contract end	102
Mandatory exclusion criteria	87	12 Exit planning and legacy IT	102
Prompt payment processes	87	 Preventing future legacy IT	102
Net zero	88	Exit planning	102
Modern slavery	88	Extensions	103
Applying minimum standards	88	Transition	104
 Cyber security	88	Data exchange	104
Evaluating social value	89	Evaluating and sharing success and lessons learned	105
Tailored evaluation	90	About this Playbook	106
Accessibility	90	Key terms	106
 Legacy IT	90	Who is the Digital, Data and Technology Playbook for?	106
Software licence terms	90	What is the scope of the Digital, Data and Technology Playbook?	109
Sustainable working practices	90	Implementation	109
10 Due diligence and contract award	92	Contacts	109
The selection process	92		
 Assessing the economic and financial standing of suppliers	92		
Keeping records and providing feedback	94		
Low-cost bid referrals	94		
 Contract implementation	96		
11 Resolution planning	96		
Resiliency through early planning	96		
 Cyber incident response plan	96		
Corporate resolution planning	98		
Contractual documentation	98		
Ongoing financial monitoring	99		
Terminating contracts with public sector dependent suppliers	99		



Foreword by Alex Chisholm



Technology offers an opportunity to transform public services for the better.

From registering to vote to data solutions for the NHS to laptops for our schools, delivering excellent digital, data and technology (DDaT) products and services is critical for the public services that we all rely on.

The UK tech sector is world leading and consistent growth across the industry saw it reach \$1 trillion in value in 2022, making it only the third country ever to hit this valuation, after the US and China. It contributes £150 billion to the UK economy and supports over 3 million jobs, making the sector a pivotal part of our future growth. Our relationship with industry is a key part of how the digital transformation of our public services will contribute to delivering skilled and better paid jobs across the country to grow the economy and achieve our 2050 net zero greenhouse gas emissions commitment.

Collaboration is the key to achieving this. We need to be better at setting up commercial relationships that enable us to take full advantage of the products and services that exist in the market. Equally, we also need to develop our in-house DDaT capabilities by ensuring that knowledge transfer is built in at all levels.

Through a considered approach to risk, focus on whole-life value and the consistent application of commercial best practice, we will:

- take an outcome-based approach to the delivery of products and services focusing on outcomes for the public, not specific solutions
- enable innovation by operating iteratively, ensuring services are continuously improved, as well as transformative new products and services
- level the playing field for SMEs to enable economic growth, employment and investment opportunities
- drive sustainability in our environment, commercial practices and economy
- avoid and remediate legacy IT to tackle our technical debt
- ensure cyber security to maintain operational resilience

This vision will only be achieved by working together across Government and with our supply chains. The refresh of the DDaT Playbook is the result of extensive collaboration across the public and private sectors and brings together expertise and best practice from across the sector.

Through this publication of the second iteration of the DDaT Playbook, we ensure that it remains relevant in a fast changing sector. We are committed to ensuring that the policies the DDaT Playbook sets out

are implemented across the public sector and that commercial capability continues to be developed.

The updated playbook continues to focus on the original policies to drive continuous improvement and continue to deliver value for money, while having a renewed focus on driving innovation. I am grateful to all those who contributed and delighted to support the Digital, Data and Technology Playbook and its recent refresh.

A handwritten signature in black ink, appearing to read 'A. M. Smith'.

Introduction – Right at the start

Digital, data and technology (DDaT) underpins everything we do and the Government provides vital services for millions of citizens every day. The public sector is estimated to spend up to £46 billion on digital in 2022/23.¹ To ensure that spend meets the needs of our users in this rapidly evolving world, we need to continually strive for excellence by thinking about our products and services in new ways.

The Digital, Data and Technology Playbook is focused on getting things right from the start. Setting projects and programmes up for success can take more time upfront but we know from past experience that this early investment can be repaid many times over by enabling us to avoid costly mistakes later on.

The updated DDaT Playbook sharpens our commercial focus on a number of key areas. These are AI and Machine Learning, Cybersecurity, Innovation, Agile Delivery, Risk Allocation and Management, and draws more robust links for commercial practitioners to digital best practice in a number of areas, such as sustainability.

The new Playbook also supports the Central Digital and Data Office's (CDDO) Transforming for a **Digital Future Roadmap**, and particularly mission six, a system that unlocks

digital transformation and the system reform programme. We are committed to putting in place the right conditions for government to digitally transform and improve outcomes for all.

The system reform programme aims to improve the day-to-day operations of government entirely, improving and enhancing agile delivery, as well as embedding digital readiness into policy making and design, meaning government can architect more digital products and services in house with greater ownership. Increased use of the Service Integrator model will enable government to move more quickly, ensuring we can benefit from the most innovative solutions in the market and play a part in the very development of these. The refreshed Playbook supports this vision, for example through the additional guidance on **Contracting for Agile**, which has been published alongside the Playbook and will evolve alongside the programme.

Continuing to develop our approach to procurement in the digital, data and technology sector will allow government to learn from successes and failures across industry. Increasingly, we need to move away from procurement through big projects and programmes, to developing products and services which are architected and owned

¹ Estimate based on top down calculation as a percentage of overall GDP

in-house and continuously improved, with government acting as the service integrator for these DDaT products and services.

This mixed model of delivery is key. We will use the market's expertise and capability to supplement agile teams and our commercial processes must be designed to enable this. Following the policies and principles in this Playbook, we will work with our suppliers to take an outcome-based approach and deliver innovative solutions which are focused on the user and create the best possible value for our citizens.

The Digital, Data and Technology Playbook sets out 11 key policy reforms which will continue to build public sector commercial capability in how we assess, procure and manage our products and services. This includes:

- online public services such as applying for a driver's licence
- business systems ranging from simple database applications through to large transactional systems supporting, for example, the operation of tax collection and benefits payments
- back office systems such as finance, human resources, and facilities management systems
- infrastructure that provides all the basic tools of the modern working environment such as computers and email

We will continue to work together across Government and industry to implement and drive the consistent application of the best practice and policies set out in this Playbook and deliver transformational change.

Gareth Rhys Williams and Megan Lee Devlin

What is new?

Version 2 of the DDaT Playbook builds on original version to provide both new and refreshed and refined content on:

- Innovation
- Agile Delivery
- AI and Machine Learning
- Cybersecurity
- Sustainability
- Intellectual Property Rights

Key policies

Commercial pipelines

Contracting authorities should publish commercial pipelines which are effective in helping suppliers to understand the government's long-term demand and prepare themselves to respond to contract opportunities. This means publishing pipelines with sufficient detail and certainty, and a minimum of 18 months ahead.

Market health and capability assessments

Contracting authorities should conduct an assessment of the health and capability of the market early on during the preparation and planning stage. Contracting authorities should use early market engagement to develop clear, outcome-based specifications which enable innovation.

Delivery model assessments

Contracting authorities should follow a proportionate, evidence-based process to decide the most appropriate delivery model and structure for a specific project or programme.

The right delivery model, including a mix of insourcing and outsourcing, enables clients and industry to work together to deliver the best possible outcomes including improved DDaT capability. A Should Cost Model should be produced as part of that assessment to better understand whole life costs and value.

Cyber security assessment

As part of the selection process, projects will apply a robust and appropriate level of cyber-security assessment to better safeguard public data and the delivery of public projects. Contracting authorities should assess their own and suppliers' cyber security in addition to understanding how any procurement impacts the ability to continue to meet the appropriate government profile under the NCSC's Cyber Assessment Framework.

The cyber security assessment should inform contract design and a requirement that suppliers meet the expectations set out in the appropriate government profiles under the NCSC's Cyber Assessment Framework. This should be embedded into contracts to maintain the security of public sector data throughout the commercial lifecycle.

There is no catch-all solution for cyber security and each product or service should be evaluated to determine the level of security and specific cyber security services required, as well as whether the organisation has the expertise to judge the efficacy of said cyber security. Consequently, commercial professionals should, where possible, seek specialist advice from suitably qualified personnel as early as possible and adopt a collaborative approach to ensure appropriate measures are taken.

Testing and learning

Where a service is being delivered in a new way, contracting authorities should undertake a programme of iteration to understand the environment, constraints, requirements, risks and opportunities. Testing and learning can also provide a wealth of quality data to help inform technical specifications.

Effective contracting

Contracts should be structured to drive collaboration, improve value for money, and deliver a sustainable, resilient and effective relationship, focussed on outcomes and the safeguarding of public data. This includes ensuring risks are allocated appropriately and that the pricing and payment mechanism corresponds with the approach to risk and incentivises the desired behaviours and outcomes.

Open and interoperable data and code

The ability to exchange and share information and data between contracting authorities and suppliers and across government is key for long-term success. Software should be open-source and designed to allow access in a platform-agnostic way. Data should be shared using consistent methods, and primarily with APIs which conform to Central Digital and Data Office API technical and data standards, satisfy the requirements of the Technology Code of Practice (TCoP), and are well documented. Operating in this consistent way will allow the interoperability between systems which fuels innovation.

Legacy IT and up-to-date products

Our DDaT products and services should be modern and fit for purpose, and preventing future legacy IT is essential to achieving this. Contracting authorities should ensure that all software is kept up-to-date and in mainstream support for the duration of the contract and plan early for when contracts end, including any extensions.



Assessing the economic and financial standing of suppliers

The economic and financial standing of bidders for the DDaT projects will be considered as part of the selection process, including on frameworks for non-critical contracts. As well as informing the selection itself, financial assessments and ongoing monitoring of financial performance should inform risk-management activity during the life of the project.

Consistently applying a transparent, objective and non-discriminatory assessment, which is tailored and proportionate to the project risk, followed by ongoing monitoring, will provide a better understanding of financial risk and leave us better able to safeguard the delivery of DDaT projects.

Sustainability

Ensuring our DDaT services are sustainable is essential for long-term success. Contracting authorities should ensure products and services comply with obligations to improve environmental, economic and social sustainability and organisational strategies should be put in place and regularly assessed to measure progress against these.

Resolution planning

There will now be a requirement for suppliers of critical DDaT contracts to provide resolution planning information. Although major natural and cyber security and commercial disasters are infrequent, this will ensure that government is prepared for any risk to the continuity of critical public services, projects and programmes posed by the insolvency of critical suppliers.

Cross-cutting priorities

Cross-cutting priorities set out the ethos for the government's DDaT work and underpins what we need to consider as we undertake commercial activity. These are important government priorities which will be enabled through the best practice and key policy reforms set out in this Playbook.

Taking an outcome-based approach

Government needs to be able to respond quickly to policy changes and the needs of the public. Agile ways of working allow solutions to be tested and iterated, allowing us to learn quickly to ensure that we put users first and continually improve our public services. An outcome-based approach is essential to delivering products and services which meet user needs.

Avoiding and remediating legacy IT

Legacy IT refers to systems and their component software and hardware that are outside of vendor support, on extended support and/or on bespoke support arrangements. This is a burden on the public and has a significant impact on cyber and national security, the operational resilience

of critical systems, and value for money. Preventing future legacy IT and remediating what already exists is key to the future of the government's DDaT strategy.²

Cyber security – Secure by design

As we modernise and transform our products and services towards end-to-end digitisation, we need to design our approach to security from the start of each new initiative. Cyber security is about more than just supplier activity, but is based on the whole-life relationship between contracting authorities and the supply chain. The Government is fully committed to meeting the aims of the Government Cyber Security Strategy. Departments shall assess their cyber resilience against the appropriate government profile under the NCSC's Cyber Assessment Framework (CAF). This should be conducted in accordance with the guidance and policy under the HMG GovAssure cyber assurance regime and the Government Cyber Security Policy Framework.

² More detailed information can be found in the Legacy IT Guidance Note.

Enabling innovation

Innovation is not an end but a means through which we achieve better outcomes. This is led by user needs and is often cyclical, ranging from continuous improvement of our ways of working to transformative new products and services, often facilitated by open and interoperable standards. Innovation is closely tied to risk appetite and we will look to be innovative where appropriate, adjusting our approach to risk to harness the opportunities that an innovative approach can provide.

Driving sustainability

Government is fully committed to improving environmental, economic and social sustainability. Through guiding how we undertake procurement, we will build on the Social Value model to use the collective buying power of the public sector to drive progress in the delivery of sustainable DDaT projects and programmes for long-term benefits to our citizens.

Levelling the playing field for small and medium-sized enterprises (SMEs)

SMEs and voluntary, community and social enterprises (VCSEs) make a considerable contribution to the DDaT industry and often

lead the way on innovation. This can have significant impacts on economic growth, employment and investment opportunities in the UK. They are vital to our ambition to realise Strategic Advantage through science and technology. Government remains fully committed to supporting start-ups, SMEs and VCSEs through government procurement to support a healthy, diverse and competitive market and levelling-up.

Procurement Reform

The new rules that will be introduced as a result of the enactment of the Procurement Bill and its associated regulations (which is currently going through Parliament) will have implications for the policies set out within this Playbook for contracting authorities in England, Wales and Northern Ireland, and reserved procurements undertaken in Scotland. The details of these changes cannot be known until that process has completed (likely to be towards the end of 2023) but we have attempted here to highlight what effect the proposed rule changes may have. Please note that this is still subject to change. The Playbooks will be updated to reflect the new regulations in due course.

Playbook flow diagram

Figure 1: Where this Playbook fits within a typical procurement process

Commercial lifecycle	Typical commercial activities	Chapter	Key Policies
Define	 <p>Preparation and planning Chapters 1–7</p>	1	<ul style="list-style-type: none"> △ Commercial pipelines △ Market health and capability assessments
		2	<ul style="list-style-type: none"> △ Effective contract and portfolio management △ Building and maintaining supply chain relationships
		3	<ul style="list-style-type: none"> △ Outcome-based approval
		4	<ul style="list-style-type: none"> △ Enabling innovation △ Outcome based approach △ Cyber security
		5	<ul style="list-style-type: none"> △ DMA (inc. agile sourcing)
		6	<ul style="list-style-type: none"> △ Testing and piloting solutions
		7	<ul style="list-style-type: none"> △ Outcome based approaches

Commercial lifecycle	Typical commercial activities	Chapter	Key Policies
Procure	 <p>Publication Chapter 8</p>	8	<ul style="list-style-type: none"> △ Effective contracting △ Legacy IT and up-to-date products △ Cyber security risk △ Open and interoperable data and software △ Payment Mechanism and Pricing Approach
	 <p>Selection, evaluation and award Chapters 9 and 10</p>	9	<ul style="list-style-type: none"> △ Delivering sustainability
	 <p>Contract implementation Chapters 11</p>	10	<ul style="list-style-type: none"> △ Assessing the economic and financial standing of suppliers
Manage Construct and operate	 <p>Contract implementation Chapters 11</p>	11	<ul style="list-style-type: none"> △ Cyber incident response plan
	 <p>Contract end Chapter 12</p>	12	<ul style="list-style-type: none"> △ Preventing future legacy IT

Applying the Digital, Data and Technology Playbook

The Digital, Data and Technology Playbook applies to all new DDaT projects. It is mandated for central government departments and arm's-length bodies (ALBs) on a 'comply or explain' basis and, recognising that there is no one-size-fits all model, it is expected to be taken into account by the wider public sector (see About this Playbook).

The Digital, Data and Technology Playbook describes what should be done, from policy inception through to the operation of DDaT projects and programmes. This framework should be embedded proportionally through the structure of an organisation, from governance through to the delivery of individual products and services.

For central government, compliance with the Digital, Data and Technology Playbook is being driven through departments' governance processes, central Cabinet Office controls (projects over £20 million per transaction) and the Treasury Approvals Process. The Cabinet Office Markets, Sourcing and Supplier Team will work with in-scope organisations to embed the Digital, Data and Technology Playbook within local governance forums and approval processes.

Applying the principles and policies set out in this Playbook, following the mandatory Green Book principles, using the best practice Five-Case Business Model and applying the principles of the Orange Book will result in improved outcomes for public sector DDaT projects and programmes.

Navigating the Digital, Data and Technology Playbook

The Digital, Data and Technology Playbook provides an end-to-end guide to the commercial process for DDaT projects and programmes and has been structured around the main stages of a typical procurement and project lifecycle:

- preparation and planning
- publication
- selection
- evaluation and award
- contract delivery

There are 12 chapters, each setting out best practice for specific topics with six cross-cutting priorities flowing through the Playbook setting out our ethos for DDaT projects. These are underpinned by a spine of 11 key policies which are the reforms or actions that will have the greatest impact in improving how we deliver DDaT products and services.

The Digital, Data and Technology Playbook follows the Sourcing, Consultancy and Construction Playbooks developed by the Cabinet Office Sourcing Programme. Each Playbook has a common backbone of key policies which are good commercial practice, and these have been adapted for the Digital, Data and Technology Playbook alongside new key policy reforms for the DDaT sector.

The symbol for a key policy is a Playbook icon and each time this appears it flags an important policy that practitioners should take note of. Figure 1 overleaf shows where each chapter sits within the procurement lifecycle, how they align to the main commercial stages and where the key policies appear.



1 Pipelines and market management

Getting it right starts by having clear and transparent commercial pipelines and by having a good understanding of the market to identify where we can drive investment to level the playing field for start-ups, SMEs and VCSEs.

Business strategy, priorities and demand

Taking a strategic approach to commercial activity is key to setting procurements up for success. Contracting authorities should have a documented commercial strategy aligned to organisational objectives incorporating both short and long-term targets in line with leading industry practice. This should also reflect resource plans, including plans to develop in-house DDaT capability, and take into account organisational DDaT strategy. The requirement of commercial professionals is set out in section 1.1 of the Commercial Continuous Improvement Assessment Framework.

Commercial Pipelines

One of the most important things we can do is to prepare, maintain and publish comprehensive pipelines of current and future government contracts and commercial activity.

Publishing commercial pipelines enables suppliers to understand the likely future demand across government. By sharing early insights on planned activities, we can expect to achieve wider participation and greater diversity in our supply chains, including SMEs, and support capability-building for the longer term. Effectively signalling upcoming

demand across government will drive better innovation and enable the market to respond effectively.

Published commercial pipelines should look ahead three to five years (and a minimum of 18 months) to be truly effective. It may not be feasible, or appropriate, to have clearly defined longer-term plans when procuring capability or undertaking mixed-model delivery (see **Chapter 5**) to support agile working. In these cases, contracting authorities should publish the overarching requirements and any known elements of upcoming demand, indicating the level of certainty in these plans.

We recognise that priorities and plans change and pipelines must be kept up-to-date in order to be effective. However, contracting authorities should recognise that it is often more helpful to give a forward view of procurement and indicate a high level of uncertainty than not publish at all. Visibility of demand will make government a more attractive client for suppliers, including SMEs in the DDaT sector.

“ Effectively signalling upcoming demand across government will drive better innovation and enable the market to respond effectively”

Procurement Reform

The current intention under the Procurement Bill is that the requirement to publish information on Governmental procurement pipelines will be expanded to all Government bodies who expect to spend over £100 million in a financial year for all contracts (exemptions apply, such private utilities and national security contracts) over £2 million within 56 days of the start of the relevant financial year. It is envisaged that this information will be provided on a pipeline notice and be available on the single, central platform.

Market management

Healthy, competitive markets matter because they support our ability to achieve value for money for taxpayers, level-up the UK economy and drive innovation in delivering public services.

Good market management is about looking beyond individual contracts and suppliers. It is about designing commercial strategies and contracts that promote healthy markets over the short, medium and long term.

How government delivers DDaT services can have a profound effect on market development. For example, those winning early contracts may acquire first mover incumbency advantages, accepting that

they also take on increased risk. We should adopt models that promote competition and contestability over time, so that those that win the initial contracts know that they must deliver value for money and perform to the standards required for the delivery of the service.

Mixed economies represent one way of broadening competition in a market and can therefore help drive value for money. However, where mixed economies are used, care is required to create a level playing field between public, private and third sector providers. The expectation of commercial practitioners for managing markets is set out in section 5.1.3 of the government commercial functional standard.



Market health and capability assessments

All DDaT procurements should include an assessment of the market early on during the preparation and planning stage. There is no one-size-fits-all for how we assess the market and this should be appropriate for the size, scope and complexity of the procurement.

Market health and capability assessments should include a consideration of the available skills, capabilities, size and capacity of the market, and an assessment of barriers to entry and market concentration.

These assessments should then be used to:

- identify potential opportunities and limitations in the market
- take advantage of effective new technologies and innovation
- consider what actions would increase competition and improve market health, including strengthening skills and capability

Contracting authorities should also consider what the market could look like when the product or service is next procured. Any review of the market should be based on the intended outcomes and it is important not to confuse the description of the requirement with the definition of the market.

Market health assessments for individual projects and programmes should form part of a wider ongoing market strategy. Contracting authorities can request access to supplementary market intelligence collected by commercial teams in the Cabinet Office and Crown Commercial Service (CCS). The Cabinet Office also offers ‘on the shoulder support’ where appropriate. Advice can also be sought from the Competition and Markets Authority (CMA) in relation to more complex or substantial competition issues.

The role of SMEs

SMEs and VCSEs make a considerable contribution to the DDaT industry and have been key contributors to much of the innovation and product development that has emerged in recent years. Although SMEs have a wealth of experience to contribute, they may not always have the capacity and/or commercial capability to engage to the extent and scale that larger suppliers can.

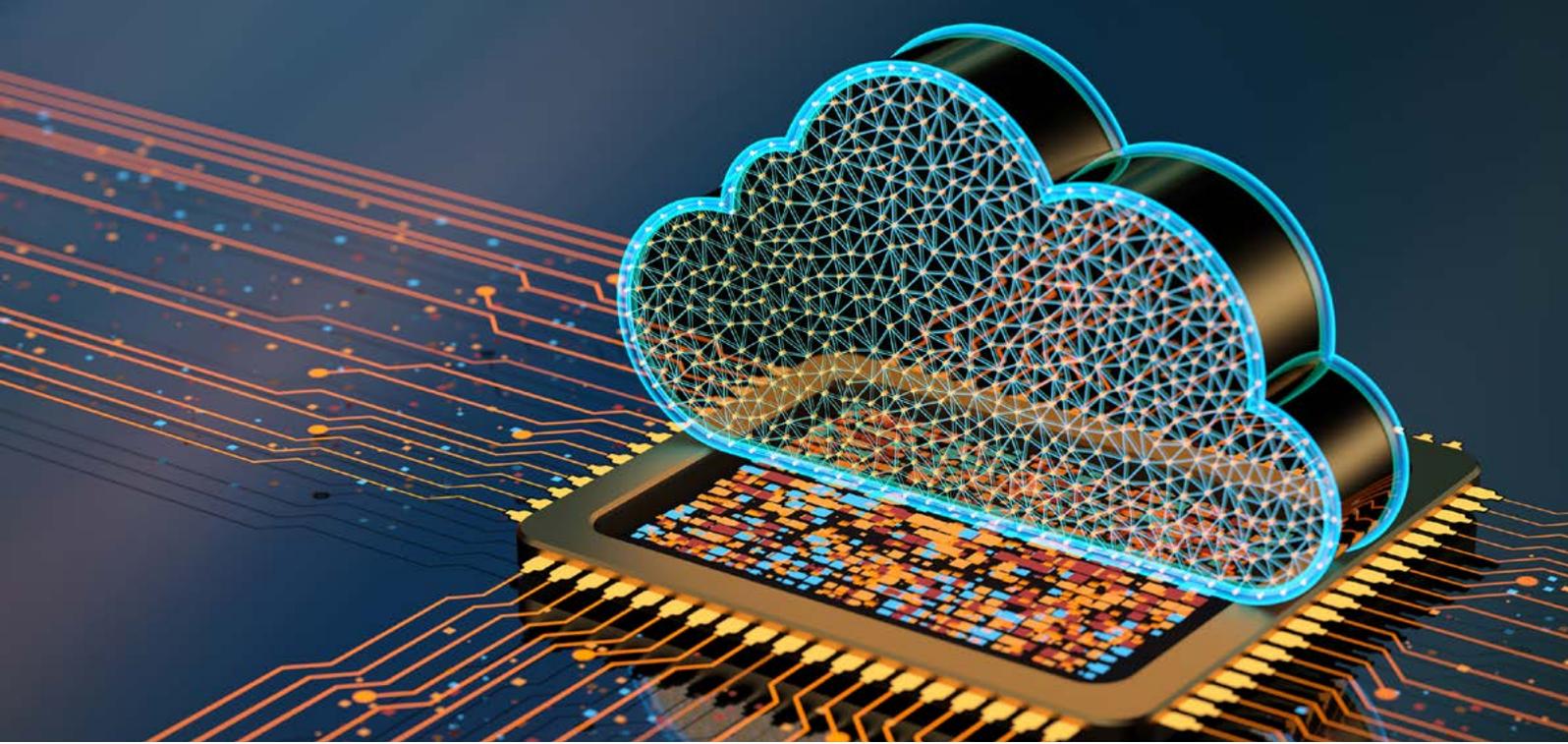
It is important during the initial phase of the project or programme, that we acknowledge this and adjust what we ask of them accordingly.

The government is committed to supporting SMEs and VCSEs through government procurement and we expect suppliers to follow the principles and policies set out in this Playbook and the Supplier Code of Conduct, particularly where SMEs and VCSEs are engaged through the supply chain.

Contracting authorities should consider how they can evaluate this in practice and whether the use of a key performance indicator linked to feedback from the supply chain is appropriate (see **Chapter 8**).

Procurement Reform

The Procurement Bill intends to introduce new measures to make it easier for SMEs to bid for public sector contracts. In addition to a duty placed upon contracting authorities to consider whether there are any such barriers in place, contracting authorities will not be able to request the submission of audited annual accounts as part of a selection/award process, except from suppliers who are required to have their accounts audited by the Companies Act. In addition, suppliers will not be expected to have contract-specific insurance policies in place before the award of a contract. This reduces nugatory costs that may prohibit smaller suppliers from bidding.



Using cloud to enable SME involvement

As a greater proportion of our DDaT services become cloud-based, we need to ensure that we are maintaining a level playing field for SMEs where possible. This will be enabled through various levels of cloud-based working as set out in Figure 2.

Software as a service (SaaS)

Unlike in a hosted model, where contracting authorities buy software which they install on their own platforms and infrastructure, in a SaaS model the provider makes the software available via the internet and manages the underlying platform and infrastructure stack. For SaaS components, contracting authorities will not need to consider hosting directly and the cloud provider is responsible for providing the service to you, usually within an agreed service level agreement (SLA).

Many UK based SMEs have developed the capability to develop custom applications or provide SaaS services by building on top of industry standard/hyperscale cloud platforms. By using these platforms as appropriate, we can create opportunities for SMEs to work with government using cloud as an important enabler of a diverse and competitive market.

Platform as a service (PaaS)

Most elements of the technical stack are managed by the cloud provider. The cloud provider may also offer additional managed services such as operating systems or logging infrastructure.

Most PaaS suppliers will expect contracting authorities' architecture to meet specific requirements and will offer limited flexibility for software environments, languages or interfaces, so check the details before you sign an agreement. This sector has a highly active SME base.

Infrastructure as a service (IaaS)

Some elements of the technical stack, for example networks, storage and servers, are owned by a cloud provider and provided to you as a hosted service. This typically means contracting authorities are no longer responsible for operating a data centre.

The benefit of IaaS is that contracting authorities can quickly add or remove capacity and the supplier only bills you for what you use. However, teams will need to have the technical infrastructure skills and time to manage it what is deployed on the infrastructure.

Public cloud infrastructure deployments are predominantly available from large multinationals and via partners/resellers including a large SME base. Private cloud deployments are available from local Large and SME vendors. Mainstream technologies from multinationals are available to support this, mostly via partners, including SMEs.

Artificial Intelligence (AI) and Machine Learning

Artificial Intelligence (AI) is an evolving area which comprises a set of technologies that have the potential to greatly improve public services by reducing costs, enhancing quality, and freeing up valuable time for frontline staff. We are in the early days of deploying AI systems in the public sector and are continuously discovering new benefits for using AI systems to drive decision making, as well as challenges and risks that need to be addressed.

AI can be defined as the use of digital technology to create systems capable of performing tasks commonly thought to require human intelligence. Machine learning is a subset of AI, and refers to the development of digital systems that improve their performance on a given task over time through experience. Machine learning is the most widely-used form of AI, and has contributed to innovations like self-driving cars, speech recognition and machine translation.

The Cabinet Office and the Office for AI have published Guidelines for AI Procurement. These can be found [here](#). They help inform and empower contracting authorities, helping them to evaluate suppliers, then confidently and responsibly procure AI technologies for the benefit of citizens.

When applied efficiently, AI and Machine Learning have the potential to transform how public services are delivered. They can ensure that we are managing and using data better, improving diagnostics in healthcare and helping the public sector communicate better with customers and suppliers through the likes of online chatbots, which allow customers to ask questions and chat through an online messaging application. While AI and Machine Learning can bring many benefits, it should not be assumed that these technologies are the default solution to the challenges facing the public sector, and the country more widely. CDDO and the Office for AI have produced guidance on assessing if AI is the right solution for your challenge.

When procuring AI and Machine Learning technologies, products or solutions, contracting authorities should be clear on what they intend to buy. Broadly, these can be broken down into three categories: the model, the algorithm and the data set. In most cases, a contracting authority will procure the pre-trained model (for example when it is part of a wider application). However, that model could be static and not update when the characteristics of the training data change over time (some cloud-based applications may include dynamic models).

Alternatively, contracting authorities could procure (or acquire if it is open-source) the algorithm and use it to train on procured data or, if relevant, their own data. With this alternative approach, the contracting authority could either use their own data science capability or procure contract resources to train the model. Some suppliers sell access to pre-trained models on a per-use basis, in which contracting authorities use APIs (application programming interfaces) to apply them to their own data.

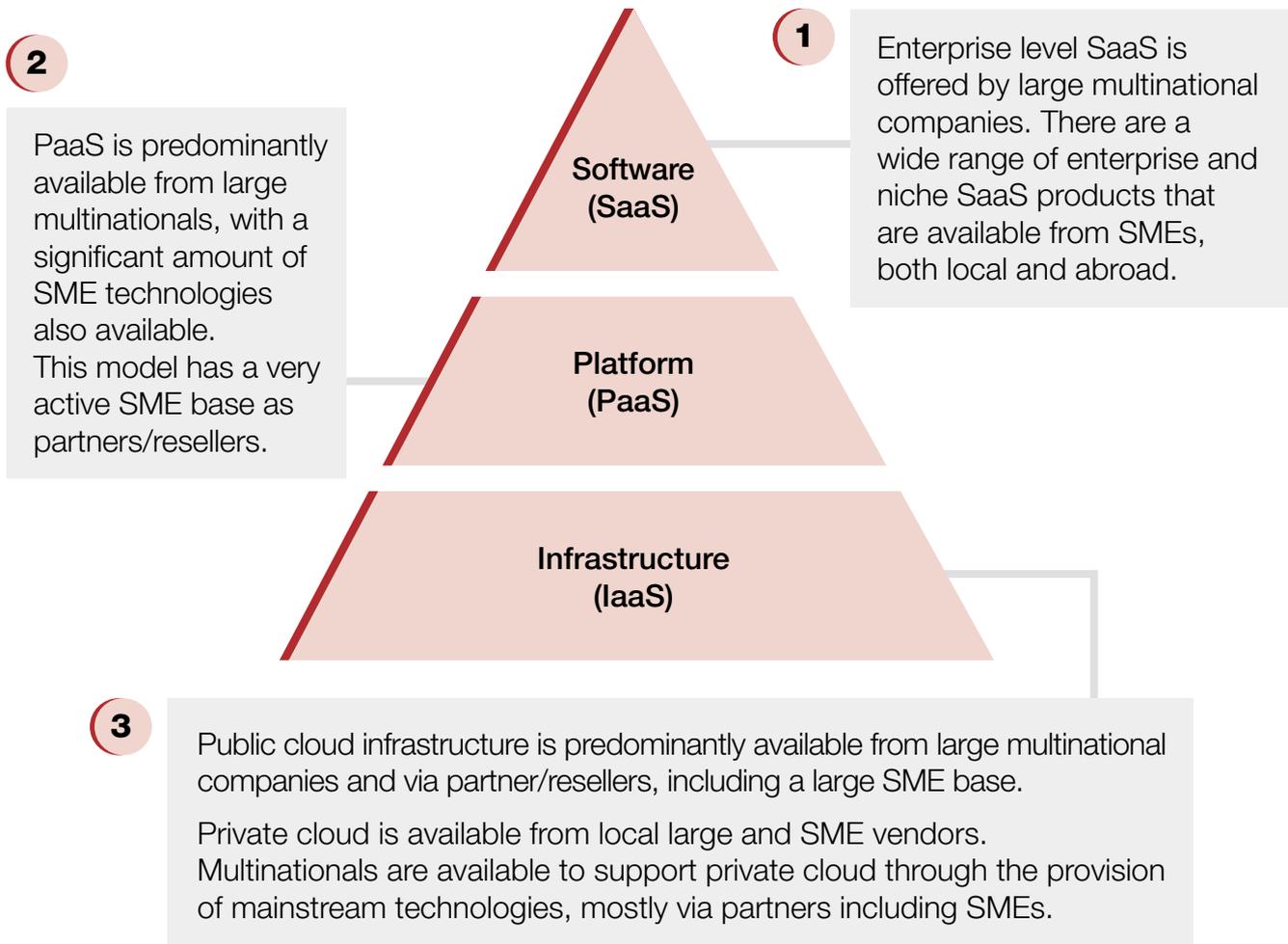
Contracting authorities may also wish to procure the data set the model has been trained on. In this case, contracting authorities should be aware of specific considerations on data usage. Further details of this can be found in **Chapter 3**.

Understanding what you are procuring will be central to defining and assessing its value, and managing it post-award. For example, different Intellectual Property Rights (IP) considerations may need to be made depending on if you are procuring the model, algorithm and/or the data set. Further detail on IP can be found in **Chapter 7**.

AI technologies are increasingly being used in services that are not exclusively AI and contracting authorities should be aware that this may be the case with many of the services they are procuring. Market and bidder engagement should be used to determine if AI is being used as part of the service or within the supply chain. If AI technologies are being used in the background, contracting authorities should consider the additional risks this may bring. Further details can be found in **Chapter 3**.

Whenever we apply AI within the public sector, we need to be aware of its weaknesses. AI and Machine Learning, including Generative AI (which creates text and images) can create very plausible and believable content. However, these systems are driven through probability and are subject to bias based on their learning. CDDO can be contacted for additional support and guidance on the use of this technology, and the risk and opportunities it creates.

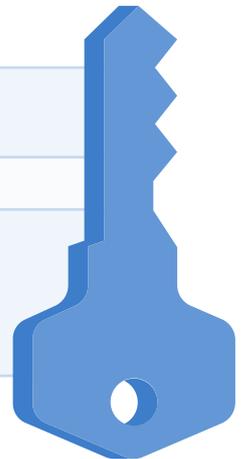
Figure 2. Levels of cloud-based working





Key points

1. Publish commercial pipelines so suppliers understand likely future demand for services across government.
2. Contracting authorities should have a documented commercial strategy.
3. Assess the health and capability of the market you will be dealing with for all projects and programmes regularly – consider how you can take advantage of innovative approaches, encourage new or potential market entrants and take action to address any concerns.



Want to know more?

1. **GovS008 Commercial Functional Standard.**
2. The standard for central government is set out in the **Commercial Pipeline Guidance** under the Government Commercial Organisation Standards.
3. **Market Management Guidance Note** – This was designed for public services; however, it provides useful guidance for any market.
4. Supplier factsheets and market reports for common goods and services can be requested from **ci@crownccommercial.gov.uk.**
5. Advice from the CMA can be sought via **advocacy@cma.gov.uk.**



2 Successful relationships

We need to consider how we will work with suppliers throughout the lifecycle of projects and programmes to achieve contractual outcomes including effectively managing contracts.

Contracting authorities should place significant importance on the relationships they create with their supply chains at an organisational and portfolio-level, especially given the often high-value and complicated nature of many digital and/or data products and services. Building and maintaining successful relationships starts long before the manage stage of the contract and is a continuous process.

Within a strategic framework, the nature of the relationship between an organisation and supplier should be tailored to individual projects and programmes. This means thinking about the specific type of relationship and engaging early with the market whilst following the principle of using standard contracts (see **Chapter 8**). Delivery teams, designers and contract managers should be involved early in the process to support commercial and contract design and the transition from procurement to delivery, ensuring adequate time is allocated for each stage.



Effective contract and portfolio management

Projects and programmes should be built on a robust contractual relationship overseen by an appropriately qualified contract manager with a clear operational understanding of the contract.

How a contract will be managed is a key strategic decision which needs adequate consideration early in the procurement process and should be reflected in the contractual agreement. A proportionate and consistent open book approach to contract management should be applied to a broad range of different contracts, in line with government guidance. In line with the expectation to adopt a portfolio approach to procuring products and services, contracting authorities should consider a strategic portfolio approach to the management of contracts.

Good contract management involves a wide range of activities and government's most important contracts should be managed by an expert or practitioner accredited contract manager, as set out in the Contract Management Professional Standards framework.

Building and maintaining supply chain relationships

As outlined in the Supplier Code of Conduct, acting together with suppliers drives mutual understanding, improves delivery and helps to solve problems more effectively. Relationships are formed by behaviours, specifically collaborative behaviours and these should be exhibited to build and maintain successful relationships.

“ Within a strategic framework, the nature of the relationship between an organisation and supplier should be tailored to individual projects and programmes”

The process of contracting should look to codify the relationship that has already been established between the contracting authority and supplier. This should include all the best practice and good behaviours already extant in the relationship and will act as a starting point for future relationships.

For all types of relationships, clear and agreed reporting, change management and dispute resolution mechanisms are a critical success factor, including, where appropriate, how allowable costs will be managed. These are included in standard forms of contracts (see **Chapter 8**).

For more complex projects and programmes, experience has demonstrated that a partnership model with the principles of collaboration, openness, transparency, and flexibility based on contractual delivery, can be beneficial in driving successful outcomes and innovation. Critical success factors of a partnership model include a focus on delivery by both partners, clear roles and responsibilities, a shared understanding of how to resolve disputes and a collaborative culture.

Projects and programmes should start with an initial workshop, bringing together the delivery team, leadership, and key stakeholders to set expectations on standards, behaviours and ways of working, align success measures and objectives,

and outline how the individual project is supporting an organisation's goals. These workshops should be proportional in length and complexity to the size of the project and existing relationships, and should be followed up with regular engagement throughout the delivery phase.

Flow down of contractual terms and conditions

It is not recommended that all terms and conditions set out in contracts with prime suppliers automatically flow down through the supply chain unamended. This should be tailored and proportionate to the size of the product or service being delivered by the supplier in the supply chain. However, fundamental contractual terms, such as prompt payment (see **Chapter 9**), should flow throughout the supply chain, no matter the size of the project.

On critical DDaT contracts authorities should consider the requirement for resolution planning clauses to flow down into the supply chain. In many cases, this may be an appropriate way to help mitigate risks.

Successful relationships and legacy IT³

Contracting authorities should work with suppliers to devise reporting requirements on the status of current and potential legacy IT including suppliers' compliance with the contractual provisions in relation to 'evergreen' clauses. Contracting authorities should ensure legacy IT risks are actively managed by the supplier for all parts of the authority's IT estate under the supplier's management. This should be undertaken by at least one member of the supplier's management team with digital, data and cyber expertise.

Strategic supplier relationship management

Where a significant contract has been placed or a contracting authority has several important contracts with a single supplier, they should consider if the supplier now qualifies as strategic at an organisational level. If so, a strategic supplier relationship management approach should be utilised. Contracting authorities should consider how they can adopt a strategic supplier relationship management approach in their organisation to drive win-win benefits. In practice, this means:

- value creation beyond that originally contracted
- managed engagement at an executive level
- joint strategy development, objectives and planning
- collaborative behaviours and working

- relationship measurement and monitoring
- management of aggregated performance and risk

In addition to an organisation's own management of its suppliers, the Markets and Suppliers team in the Cabinet Office is responsible for maintaining relationships with the Government's Strategic Suppliers, many of whom operate in the digital and data environment, to improve supplier relationships and add value. If you have contracts with any of the Government Strategic Suppliers, you should engage with the Markets and Suppliers team regularly to ensure that you are aligned with government's overall objectives and strategies for working with these suppliers.

SME relationship management

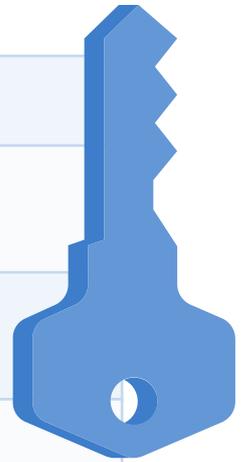
Contracting authorities should ensure that ongoing contract management and reporting requirements are necessary and proportional to the size and complexity of the contract. These can be resource intensive, and excessive reporting requirements may be burdensome, potentially disincentivising SMEs from bidding for further contracts with the government.

The SME Advisory Panel works with the government to support start-ups and small businesses via government procurement. This panel is hosted by the Small Business Policy Team in the Cabinet Office who can be contacted for further advice and guidance at smallbusinesssteam@cabinetoffice.gov.uk

³ Legacy IT Guidance Note: Guideline 8

Key points

1. Effective contract management is essential to drive value for money and deliver successful contractual outcomes.
2. Government's most important contracts should be managed by an expert or practitioner accredited contract manager as set out in the Contract Management Professional Standards framework.
3. Engage with the market and senior stakeholders to consider what type of relationship is most appropriate for the project and use this to inform the choice of procurement procedure and contractual model.
4. A strategic supplier relationship management approach can improve the delivery of objectives and increase mutual value beyond that originally contracted.



Want to know more?

1. [List of the government's strategic suppliers.](#)
2. [Model Services Contract.](#)
3. [Supplier Code of Conduct.](#)
4. [Contract Management Standards.](#)
5. [Access to the foundation level Contract Management Training and Accreditation is available for public sector contracting authorities.](#)
6. [PPN 05/16 Open Book Contract Management.](#)
7. [Strategic Supplier Relationship Management Guide](#) (Khub).
8. [ISO 44001:201](#) specifies requirements for the effective identification, development and management of collaborative business relationships.



3 Governance and approvals

In order to deliver better DDaT products and services, we need to focus on people, processes and systems, and getting the governance and ethos right at the start of a project or programme will shape how outcomes are developed and delivered.

Culture which manages risk and good governance

Government is often overly risk averse in considering new ways of doing things. While it may be thought that an aversion to risk may be the best way to achieve value for money for the public, this can actually prevent us from taking advantage of new opportunities that represent better value in the long-term, and has historically resulted in us procuring solutions which may not meet user needs and risk becoming legacy IT.

Our approach to this has to change. In order to deliver real value over the long term, we must take a more considered approach to risk, utilising established ways of testing and learning to enable us to effectively manage risks and explore new innovations to maximise value. This should be proportionate to the criticality of service delivery and the key will be to ensure whole-life value for money through clearly demonstrating how any 'failures' are steps in the right direction. This is a core part of an iterative approach to testing and learning (see **Chapter 6**).

Outcome-based Approach

Contracting authorities should have consistent, transparent, proportional and streamlined processes to enable effective decision making. Approvals and governance should be shaped in a way that is focused on user needs and conducive to innovation and testing and learning. The Green Book is consistent with this and can enable an agile approach to development, but we are not always successful at doing this in practice, particularly where the detailed requirements are unclear, but the desired outcome is known. To understand these needs, public bodies may need to invest in internal user research capacity before they are well-positioned to go to market for technology solutions.

Project/Programme Outcome Profile

The Project/Programme Outcome Profile (POP) is a method and a tool developed by the Infrastructure and Projects Authority (IPA) to support projects and programmes to set out in a consistent way how they will contribute to government's priority outcomes, and measure progress against them in order to develop stronger business cases in line with Green Book guidance.

“ Once the right people have been identified, ensuring all stakeholders are working from the same information and towards the same outcome is key”

This will support teams to understand the specific contribution of their work to the delivery of relevant priorities. Whether the proposal is for a programme within a strategic portfolio or a project within a programme, its objectives need to be understood in terms of its individual contribution to the wider group of interventions of which it is a part. This includes cross-governmental priorities such as social value, and DDaT priorities such as remediating legacy IT.

Cross-functional teams

Successful delivery of a project and programme is built on ensuring we have the right teams of people with the necessary mix of functional expertise and experience. Early cross-functional working enables innovation and the appropriate and ethical use of data, is essential to an effective cyber security and agile delivery strategy, forming a key element of DDaT service assessments. A number of key roles can be found in the Government Service Manual and will form part of DDaT service assessments against the Government Service Standard (linked later in this chapter). Key roles to think about early in the preparation and planning stages include the senior responsible owner (SRO), service manager, product manager and product owner, in addition to project management. It is essential that these are allocated to suitably qualified individuals.

It is essential that Commercial/Procurement and Technical teams are integrated at an early stage with good communication between the two. This supports the management of risk and the successful delivery of projects.

Additionally, as there is generally a greater prevalence of temporary external contractors in DDaT contracts, there is a greater risk of knowledge loss throughout the procurement process. It is essential that measures are taken to mitigate this risk including, but not limited to, using a RACI (Responsible, Accountable, Consulted, Informed) matrix to define roles and responsibilities, having audit trails for key decisions, and creating knowledge banks.

Once the right people have been identified, ensuring all stakeholders are working from the same information and towards the same outcome is key. Communication is at the heart of any successful project and programme, and this is especially the case for DDaT where technical language, whether legal, commercial, DDaT, or other, can be a barrier to effective communication. Getting this right enables us to make good decisions right from the start. The expectation of commercial practitioners is set out in s.3.4 of the government commercial functional standard.

Senior leadership buy-in

Effective governance is critical for all projects, including DDaT where the breadth of the work is vast and spend is often high, meaning that value for money and accountability are key day-to-day considerations. This process can be somewhat challenging when projects are agile or when trying to do something different, for example innovating. Therefore, senior leadership engagement and buy-in is critical to the delivery of projects which are moving at pace.

The benefit of senior leaders with the right skills being involved is active engagement with the risk profile of the project or programme. Where a project is identified as being agile or innovative, dedicated sponsorship will enable decision making at pace.

Appropriately qualified SROs

Senior Responsible Owners (SROs) will own the business case and be accountable for delivery of the project or programme and its benefits and outcomes. SROs must fully understand the governance and approvals process, both commercial and digital, and commit sufficient time to lead the project or programme through approvals and delivery.

SROs for DDaT projects should sufficiently understand how to frame intended outcomes and potential innovation and capture these in the business case (see **Chapter 3**). The individuals will also need to understand the relevant processes, in line with this Playbook, to get things right from the start, prevent unnecessary delays through approvals and inform decisions through the best available information and expertise.

Project Validation Reviews

Any new initiative likely to result in a major project should go through a Project Validation Review (PVR). This may also apply if the value of a standard project is greater than the delegated spend limit or it is considered to be strategically significant. Contracting authorities should consult the Cabinet Office Strategy, Assurance and Standards (SAS) team, HM Treasury and the CDDO as needed.

The PVR should occur during the early stages of preparation and planning, and before any public commitment is made. It consists of a short independent peer assessment that takes place ahead of the transition from policy to delivery and further information can be found in the major project approval and assurance guidance.

Government Major Contracts Portfolio

Central government's most complex and strategically significant contracts will form the Government Major Contracts Portfolio (GMCP).

Complex outsourcing refers to any of the following: first generation outsourcing; significant transformation of service delivery; obtaining services from markets with limited competition or where government is the only customer; and any service obtained by contract that is considered novel or contentious.

This will be overseen by the Cabinet Office with departments providing data on a quarterly basis. The GMCP enables tracking of major contracts throughout their lifecycle, including assessing impact, complexity and performance.

Commercial assurance

The Commercial Spend Control assures cases against the Commercial Functional Standard and other functional policies and best practice including Playbooks and Procurement Policy Notes. Departments can engage with the commercial spend controls through two channels:

- Submission of a Commercial Pipeline enabling approval through 'Pipeline Assurance'.
- Submission of a controls approval request through the online Commercial Assurance Management System.

For all projects over £20 million (total contract value), additional controls are applied by the Cabinet Office and departments are encouraged to engage with SAS (controls) as early as possible. If an externally sourced project is considered to be complex, a member of the Complex Transactions Team, or another Cabinet Office commercial team, will also be embedded.

DDaT assurance

Technology Code of Practice (TCoP)⁴

TCoP is a cross-government standard setting out the key considerations for how the government should design, build and buy technology. The principles of TCoP focus on avoiding vendor lock-in and on creating interoperable and standards-based procured services, through using common standards across government. Compliance with this code is assured through the Cabinet Office spend control process and services will also need to meet the Government

Service Standard (see below). Departments are expected to maintain a pipeline of current and upcoming DDaT programmes, and this pipeline will be assessed against the TCoP and other standards by central or departmental teams. Many of the practices set out in the TCoP can be considered best practice for the wider public sector also.

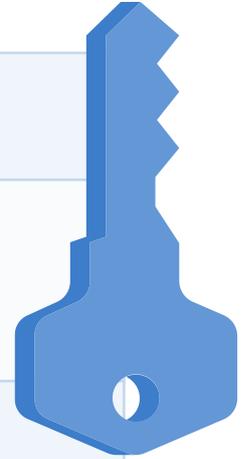
Service assessments

The Government Service Standard helps teams create and operate good public services and sets out best practice for how problems are defined and solutions iterated and delivered for DDaT services. Compliance with the Government Service Standard is assured through service assessments conducted by the Central Digital and Data Office (CDDO) or departmental assessment teams as required. The Government Service Manual provides more information on this, including on when a service assessment is needed.

4 Legacy IT Guidance Note: Guideline 11

Key points

1. Good approval processes should be consistent, transparent and streamlined to enable effective decision making across an organisation and improve value for money.
2. Project or programme Senior Responsible Owners (SROs) should be appropriately experienced and qualified, fully understand the governance and approvals process, the scope of their responsibility and commit sufficient time to guide projects and programmes through approvals and delivery.
3. Early cross-functional discourse enables innovation and is essential to an effective cyber security and agile delivery strategy.



Want to know more?

1. The Cabinet Office Sourcing Programme is leading on implementation of the Digital, Data and Technology Playbook, including working with the Local Government Association and Local Partnerships – contact sourcing.programme@cabinetoffice.gov.uk.
2. For further information on the GMCP contact sourcing.programme@cabinetoffice.gov.uk.
3. **GovS 002: Project Delivery Functional Standard**.
4. For advice on engaging the HMT Spending Teams, contact your departmental approval and scrutiny lead.
5. For further information regarding Cabinet Office commercial spend controls, see: www.gov.uk/guidance/commercial-spend-controls-version-5 or contact commercialassurance@cabinetoffice.gov.uk.
6. **Service Manual – Service Standard** for digital services.
7. **Service Manual – Set up a team**. Outlining the skills that you will need to build good digital services.
8. **Digital and Technology Spend Controls**, including the criteria for evaluating departmental DDaT programme pipelines.





4

Early engagement and enabling innovation

Engaging early with the market is critical to developing potential solutions which meet user needs and inform clear, outcome-based specifications which will enable innovation.

Early engagement

We aren't afraid to talk to the market. We do it regularly and recognise the benefits to both departments and suppliers. It can help to signal our demand and prime the market for opportunity, promote upcoming procurements and provide a forum to discuss delivery challenges and risks associated with the project. Through this process, we are able to understand the viability of our policy aims, outcomes or requirements, the feasibility of alternative options and whether there is appetite (within the market and government) to consider innovative solutions that could help us deliver better public DDaT services. Early engagement should inform the design of the assessment of economic and financial standing of bidders (see **Chapter 10**).

Preliminary market engagement should actively seek out suppliers that can help to improve service delivery, including start-ups, SMEs and VCSEs who may be experts in the needs of service users and widely involved in the delivery of DDaT services across the country.

To enable inclusive economic growth that works for all, assessments of the market and pre-market engagement should consider opportunities for wider social, economic and environmental 'social value' benefits to staff, supply chains and

communities that can be achieved through the performance of the contract.

Contracting authorities should encourage suppliers to share their experience, including past performance and best practice and use that expertise to shape our requirements and inform our approach to:

- overall project timetable
- delivery model assessment
- potential solutions
- testing and learning
- procurement procedure
- bid evaluation criteria
- contractual terms and conditions including intellectual property ownership and exit arrangements

Where contracting authorities are considering the use of Artificial Intelligence, or other work with a significant data element, this market engagement can also help us to understand the capability and limitations of the AI, the provenance of the data and the ethical considerations around the proposed usage.

Good early market engagement is iterative and should involve all tiers of the supply chain, including SMEs.

“ We aren’t afraid to talk to the market. We do it regularly and recognise the benefits to both departments and suppliers”

All preliminary market consultation should observe the principles of public procurement – equal treatment, non-discrimination, proportionality and transparency – and be handled in such a way that no supplier gains an unfair advantage.

In practice, this means not setting the technical specification to suit a particular bidder and making sure any information shared is also available during the tender procedure. Preliminary market consultation should be announced by publishing a Prior Information Notice (PIN) on Find a Tender Service (FTS) and an Early Market Engagement Notice or Future Opportunity Notice on Contracts Finder.

Projects and programmes are tested at the first business case stage (Strategic Outline Case for departments and ALBs) to ensure that engagement has been sufficiently early for suppliers to understand the requirement and for the contracting authority to reflect on any feedback received.

Procurement Reform

The principles around early engagement with the market - to improve understanding of suppliers’ capabilities and risk appetite, and to identify new potential suppliers - remain the same under the Procurement Bill. However, the introduction of the Preliminary Market Engagement Notice makes it clear

that the assumption is that this market engagement will take place, with contracting authorities required to note any decision not to publish a PME notice within their Tender Notice. Contracting authorities will also be required to actively consider whether there are any barriers to small and medium sized enterprises bidding for a particular contract and assess how these can be overcome.

Enabling innovation

We need to create an environment which enables innovative and creative solutions, and effective early market engagement will be key to how we improve our approach to this. Contracting authorities should use early engagement with the market to start thinking about innovation and enable the market to suggest novel solutions to problems to ensure we meet the user needs. By using early market engagement in this way, we can make active decisions on how we set our evaluation criteria to be proportionate to our risk profile (see **Chapter 8**).

Innovation is the successful implementation of a new solution or idea which has the intent to create value for stakeholders and customers. It can occur within a plan for a new service, product, in methods for running operations or within new business models.

Before innovation can occur the first step is to 'frame the challenge'. This allows Contracting Authorities to identify the specific problem they want to solve or improve. 'Framing the challenge' creates a starting point for the entire process, and puts Contracting Authorities on the path to innovative solutions.

It is important to keep in mind that innovation doesn't have to necessarily result in a procurement exercise, but instead can be a way for the public sector to stimulate innovation in the market or demonstrate and test new concepts.

Innovation brings about benefits such as increased productivity, value for money, adding value to products or services and developing creativity. However, it can also bring risk, and therefore it is important to ensure that it is used in a proportionate and relevant manner. Contracting Authorities should consult widely, establish clearly what is trying to be achieved, make sure they are not reinventing the wheel or pre-empting solutions.

Working across the public sector more widely will support the development and implementation of innovative solutions. It will reduce costs by preventing the duplication of effort and may lead to even more innovative solutions to the complex challenges facing the public sector.

Decision making is critical to innovation. Slow decision loops can have negative and costly effects for a project, especially if it is trying to innovate or is employing agile delivery methods. Some ways to ensure smooth and successful decision making include:

1. Create the fastest decision loop possible
2. Run experiments in parallel – and celebrate their outcome

3. Turn things off - identify when something isn't working, stop, and learn from it
4. Engage users at every decision point possible
5. Create an audit trail of decision making
6. Remember that there is no need to break the rules - don't reinvent the wheel
7. Invest in communication
8. Empower people to make decisions as this can create faster decision loops

Innovation starts with being open to new ways of thinking and this corresponds to our appetite for risk. Innovation ranges from what the market can provide us as a public sector buyer to how we contract and engage with the market. Contracting authorities should consider how they can continuously improve their approach to innovation, from seeking to improve processes and products already in place, to applying existing technology to new markets to developing new products and processes which lead to transformational change.

These levels of innovation do not form a hierarchy with an expectation of progress upwards, but should be considered in context. Early engagement can be used to understand how the market is innovating and what suppliers are looking or willing to invest in and build. Contracting authorities should also take into account organisational culture, the capability of the workforce and commercial professionals, the current situation and risk appetite in order to understand and improve their approach to innovation and work with the market.

TRL Scale

Contracting Authorities should consider using the TRL (technology readiness level) scale. It is a useful tool that can help assess the availability and maturity level of a particular technology within a market.

This can help to form a clearer picture of how far solutions are from commercial readiness and operational use. In turn this can inform approaches to offering support, interventions and can inform the strategy for risk management. A TRL is based on a technology readiness assessment (TRA) which examines numerous factors such as demonstrated technology capabilities and technology requirements. The technology is then rated on a scale from 1-9 with 9 being the most mature technology.

As a technology moves along the scale, the more mature it becomes and as a result the less incentivisation is required, whereas the beginning of the scale is where we see examples of more radical innovation which will demand more incentivisation if it is to move along the scale.

From stage 6-9 of the TRL scale, technologies are at a point where they are not yet proven and therefore may require significant investment. The solution needs to be capable of moving from a prototype to an end product which can be procured (which may include testing, iterating and scaling up). This can be a risky stage within the TRL scale, and is an area where innovation commonly fails (you may also see it referred to as the 'valley of death'). At this stage Contracting Authorities should build into their budget and timetables the necessary support for suppliers to scale up and market their solution commercially.

Figure 3

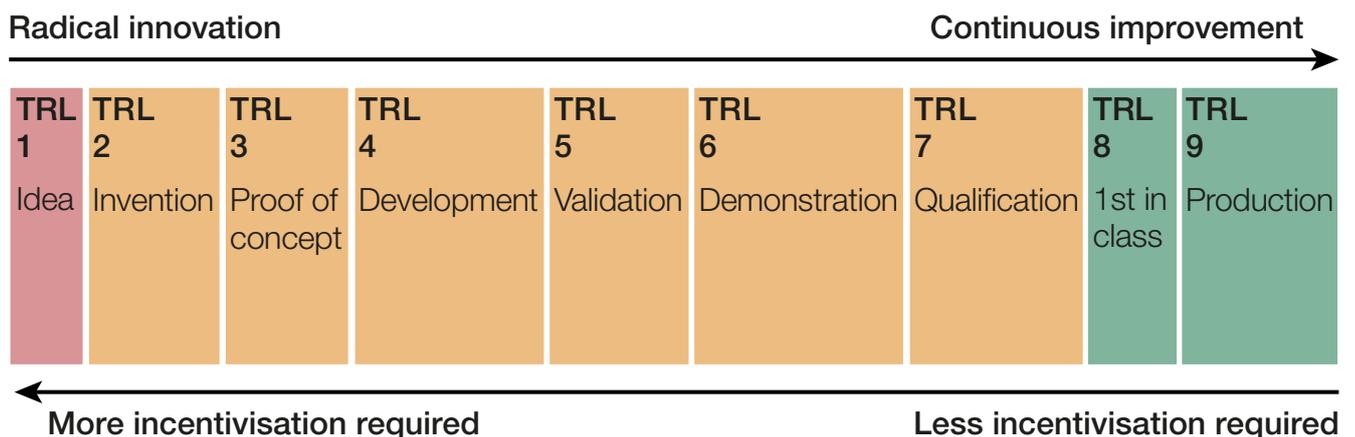
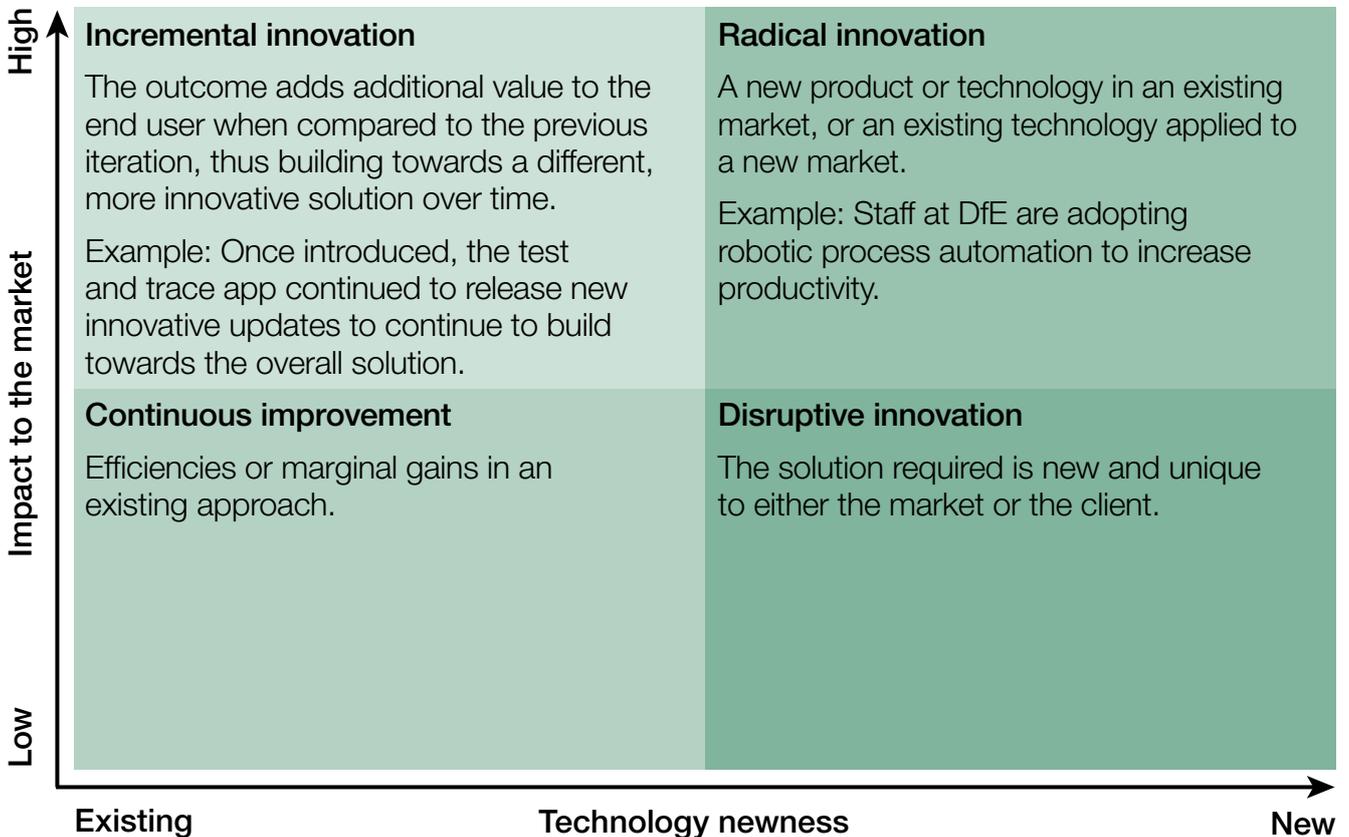


Figure 4



Incentivisation

In order to meet the growing demand for better outcomes which can be achieved through innovation, and to help suppliers move along the TRL scale, it is necessary to ask ourselves how we can incentivise our suppliers to do so. There are some financial and non-financial considerations that can be made:

- Are there any funds/grants that suppliers can access?
- Can you provide greater certainty of future business by better articulating or coordinating demand?
- How can you manage barriers to innovation incentivisation?

(For example, intellectual property ownership or costly compliance testing)

- Can you provide access to resources which are not readily available to support the progression of innovation?
- How could you support suppliers to scale up and commercialise their innovation through mentoring, training, access to subject matter experts, signposting to further funding opportunities and identification of market opportunities?
- Contracting Authorities should be aware of the risk of supplier lock-in, particularly IPR considerations. Further details on this can be found in Section 7 and in the Guidance Note on Intellectual Property Rights.

SMEs

SMEs play a vital role within innovation and driving changes in technologies and markets. However, it can be more difficult for SMEs to invest in innovation. Considerations contracting authorities should make include:

When scoping competition, make sure room for a wide range of potential solutions is allowed for:

- Try to avoid overcomplication of the competition process when publicising.
- Removal of restrictive requirements for applicants.
- Ensure any funding opportunities are articulated early to the SME networks.

Understanding user needs

When specifying products and services, it is essential that we focus on the user and the problem we're trying to solve, rather than a particular solution. By enabling suppliers to propose innovative solutions instead of meeting specific technical requirements, we are more likely to meet users' needs in the most effective way and provide the best value for money.

This requires an outcome-based approach to contracting (see below) and involves:

- doing user research to understand what users need
- undertaking an agile approach in line with the guidance provided in the Service Manual, and testing hypotheses to enable progress towards an appropriate outcome (see **Chapter 6**)
- using web analytics and other data that's available across government and the private sector

- considering the needs of data users, particularly for services that share data and hold key data sets

Public Sector Equality Duty

To ensure the best possible outcomes for users, we should ensure compliance with the Equality Act 2010 and its associated Public Sector Equality Duty. This should include consideration of the end user early in the preparation and planning stage of procurement to ensure the service being specified is fit for purpose and promotes equality of opportunity in a way that is consistent with the government's value for money policy and relevant public procurement law. The Government Data Ethics Framework can help authorities work through these and other questions.

Accessibility

We need to think about accessibility from the start, and testing and piloting should include the use of assistive technologies and users with other accessibility requirements (see **Chapter 6**). This will help us identify and fix issues early and avoid costly fixes further down the line. The Public Sector Accessibility Regulations 2018 require that user interfaces be 'perceivable, operable, understandable and robust' for users with a variety of physical and cognitive impairments.⁵ Meeting this requirement often requires specialist testing to identify problems, and contracting authorities should include this in programme costs.

The DDaT function has collated a number of guidance documents and tools for digital accessibility including accessibility user profiles which may be useful to help contracting authorities test for common accessibility problems.

5 **The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018**

Clear, outcome-based specifications

Early engagement with the market should be used to inform clear specifications. These should be outcome-based and use the Project/Programme Outcome Profile tool (see **Chapter 3**) as a framework through which to demonstrate the ambitions of the project or programme. Clear specifications does not mean having a fixed idea of what the solution is. By leaving no room for iteration or innovation, over-specification is the approach least likely to lead to success in a constantly evolving sector, and is unlikely to produce the best value for money.

Product roadmaps⁶

We should ensure specifications are informed by supplier product and service roadmaps including plans for obsolescence, maintenance and support considerations, to proactively address risks of future legacy IT. We should use early market engagement to communicate DDaT blueprints and commercial plans to suppliers to enable the market to consider and respond to these effectively.

Specifying cyber security requirements

Specifications should include an appropriate level of cyber security to safeguard public data and the delivery of public projects.

Requirements will be informed by an assessment of a contracting authority's own cyber security risk profile and any impact of the procurement on the contracting authority's ability to meet the appropriate government profiles under

the CAF. This should be undertaken in collaboration with the security function and risk colleagues to determine an acceptable level of risk appropriate for the contracting authority. Guidance on minimum outcomes and assessments for suppliers is provided in **Chapter 9**.

Procurement professionals should be aware that security standards such as various Cyber Essentials certifications do not necessarily assure the specific products or services that are to be supplied. Where specific assurance of the service is required, additional, more relevant standards may be applied where appropriate and proportionate to do so.

Some procurements may need a greater level of consideration and risk assessment in terms of cyber security. Consequently, commercial professionals should, where possible, seek specialist advice from suitably qualified personnel as early as possible and adopt a collaborative approach to ensure appropriate measures are taken. In the first instance, organisational security specialists should be contacted. The NCSC provides certifications that cover a range of products, services and organisations.

A supplier managing the right cyber risks will ensure that its own organisational cyber security good practice is in place and that the security of the goods or services it is providing will endure in practice. Confidence that the supplier takes cyber security seriously can be gained through the supplier providing evidence that they adhere to standards such as ISO 27000 or Cyber Essentials. These can be used as indicators of general good practice.

⁶ Legacy IT Guidance Note: Guidelines 1 & 2



Cyber security standards can also be used to help gain confidence that the supplier will manage a specific risk. For example, if a contracting authority wants independent assurance that a supplier will manage the risk to any information, or data, provided by the contracting authority (in relation to the contract), they should ask for independent evidence, which could take the form of a Cyber Essentials certificate for the system that holds it.

Contracting authorities may also want confidence the goods or services being bought won't introduce vulnerabilities that can be exploited by an attacker. In this case they will need to levy security requirements that are relevant and appropriate. For example, if cloud storage is being procured then the security requirements should be derived from NCSC's Cloud Principles and the supplier asked to provide independent evidence they are being met. Defining the security requirements for specific goods and services, as well as assessing evidence provided, can be complex and will likely require the support of the organisation's security team or suitably qualified external cyber security specialist.

Transparency

Transparency and accountability of public service data and information builds public trust and confidence in public DDaT services. It enables citizens to see how money is being spent and allows the performance of public services to be independently scrutinised. It also supports the functioning of competitive, innovative and open markets by providing all businesses with information about public sector purchasing and service providers' performance.

Contracting authorities should explain transparency requirements to potential suppliers as early as possible in the procurement process, and set out clearly in tender documentation the types of information to be disclosed on contract award and thereafter.

The use of data in AI and Machine Learning

Data is an essential part of AI and Machine Learning technologies. Buyers should consider the following factors in relation to the use of data within AI and Machine Learning technologies.

Factor	Key considerations
 Sensitivity	<p>The more sensitive the data that you are using within the AI system is, the more checks you should be building in. You need to closely consider if the data could be re-identified or give away any personal information, including if it were combined with other data. You should also be aware of where the AI is storing data, and how it is using input data, especially when it may contain personal identifiable information, or reveal any unpublished intent of the Government.</p>
 Quality	<p>A fundamental consideration is that poor quality data inputs will lead to poor quality outputs, affecting the reliability and usefulness of the model. This should be assessed early in the project as the less sure you are about the quality of your data, the better it is to build in additional assurances to avoid bias and de-risk the project. Ensuring the representativeness of the data set might be difficult to achieve and qualitative measures might need to be taken. It is important to consider specific societal bias that could be reflected in the data for public sector use cases.</p>
 Consent	<p>If meaningful personal data consent in the context that you are planning to use an AI-driven solution is not clear, the project is considered riskier. Also ensure that you are not inferring consent to a certain use of the data that does not comply with the original use case.</p>
 Provenance	<p>Data provenance includes where the data originates from and what happens to it over time. Contracting authorities need to assess data provenance, understand where the data is coming from and any copyright issues. For example, some algorithms are trained on the entire internet.</p>
 Privacy	<p>The Technology Code of Practice Point 7 details how citizens' rights are protected by integrating privacy as an essential part of your system. The importance of privacy has been further embedded through the restrictions GDPR places on data; for example, where it must be processed. ICO has published standards for this in the context of AI and Machine Learning. These can be found here.</p>

Factor	Key considerations
 Value	<p>The UK Government has a responsibility to its citizens regarding the appropriate and ethical use of their data. Data, particularly when combined in a large-scale data set, has value and may enable state or corporate entities to derive significant conclusions and outputs. We need to recognise the monetary and non-monetary value of this data and the use cases to which it may be applied. This includes considering the possible sensitivities stemming from third-party use of models trained on public sector-held data.</p>
 Jurisdiction	<p>Data jurisdiction is the country or region where the server on which the data is stored is located. In most cases, data offshoring is not a recommended policy. However it is the responsibility of each government department or contracting authority to take risk-based decisions on the offshoring of data.</p>
 Ethics	<p>The increasing use of AI and Machine learning, both explicitly and within other products/services we may procure, raises new ethical considerations which contracting authorities need to think about. The ethical use of AI and Machine Learning and of data should be at the centre of your tender design. Contracting authorities should consider asking bidders for their policies on the ethical use of AI and any testing conducted to reveal bias. This may form part of the tender process and could be a scored element of the quality section. For example, bidders could be asked to provide evidence of how the government's Data Ethics Framework principles have been followed during the development and implementation of the technology, product or service, or provide regular updates on ongoing bias testing.</p>

The list below provides an example for contracting authorities to consider assessing bidders on. It is not exhaustive, and may need to be adapted to align to the particular buying organisation and/or the product/service being procured. The ethics of the specific context and use case, as well as any higher standards stemming from this, should be considered when adapting and finalising such an assessment.

Transparency and explainable AI

- The supplier should describe the capabilities in the business to ensure the outputs of the AI technology are explainable, and that this explanation is widely available and understandable to a non-expert audience.

The supplier should assure the contracting authority of how and where input data will be stored, and used.

Ethical considerations relation to data limitations, fairness and bias

- The supplier should identify data limitations (and possible evolving limitations) and implement strategies to address these data limitations now and in the future use of the AI.
- The supplier should be able to describe the approach to eliminate (or minimise) bias, ethical issues, or other safety risks as a result of using the service. This should include how ongoing testing for bias will be conducted.
- The supplier should be able to describe how they have ensured that the data used to power the AI solution is sufficient in quantity, accuracy and relevance to the data available, and what measures have been taken to mitigate bias in the model.

The supplier should be able to demonstrate how they consider the skills, qualifications and diversity of the team developing and deploying AI systems.

Consent and Control

- The supplier should adopt legally sound and ethical consent for processing and capturing data throughout the full lifecycle of the solution and be able to describe the level of human decision-making at critical points.

Privacy and cybersecurity

- The supplier should be able to describe their privacy and cyber security approach for the proposed solution, in particular how the data will be protected. Contracting authorities should consider this in the context of the Machine Learning Security Principles and the risks of Generative AI created by the National Cyber Security Centre.

Alongside their Artificial Intelligence Framework (RM6200), CCS have published a list of screening questions that could be asked of bidders in relation to the ethical use of AI. These can be found [here](#).

Risks to consider when using AI and Data

While AI and Machine Learning can bring many benefits as detailed in **Chapter 1**, ethical considerations are part of a range of the risks that need to be considered when using AI and data. The contracting authority needs to thoroughly consider and identify the potential risks for a given project early in the planning process, and to consider its risk appetite in relation to these.



This is likely to differ depending on the organisation, the use case and potential impacts, and the stage of development that is being considered. The risks considered in this section are illustrative and non-exhaustive, it is recommended that commercial/procurement professionals should consult digital and data colleagues when seeking to identify and analyse risks pre-procurement.

Generally speaking, an organisation is likely to be less risk averse when in the R&D stage, and progressively more risk averse as it moves through Alpha and Beta until it reaches readiness for deployment. This is because an organisation may be far more likely to take a risk when a solution is still being developed and does not yet affect users. Conversely where an existing or established product contains AI, an organisation is likely to have a lower risk appetite and may expect to see relevant mitigations already in place from a supplier.

Alongside their risk appetite, contracting authorities should be aware that broader considerations may vary in relation to experimental/R&D type projects and those based on well-established technologies, such as chatbots. For example, the bar for AI ethics may be higher for delivery of an established product, ready to move to production, compared to an experimental project where the operationalisation may be many years in the future. Similarly, our expectations on performance against KPIs may differ when comparing an established solution ready to deliver benefits to a research project. These areas must be considered proportionately in the context of the specific project and its stage of development.

Risk	Explanation and further considerations
 Biased data inputs	<p>Where a model is trained or further developed based on biased data inputs it can perpetuate that bias in terms of its outputs. One example of this would be the potential to perpetuate any unconscious bias in recruitment if it sifted applications based on historic data which skewed against a particular group's characteristics. Additionally if a data set is limited such that it is biased to a particular group (e.g. exclusively male) then there may be limitations in its reusability for a wider group of which it was not representative. This needs to be considered when selecting data sets, and in our reliance on any outputs.</p>
 Survivor bias if the data set is incomplete	<p>If a model is trained to look for patterns in data but has an incomplete or partial selection of the data set, it may bias the decision, action or conclusion that is taken as a result. A common example to illustrate this point is planes that return from a war with bullet holes in the wings. If we concluded that this meant additional plating or protection was required on the wings, it might weigh down the plane unnecessarily, whilst at the same time neglecting the areas where planes that did not return were hit, leading to their loss. Considering all data and what may be missing can lead to the opposite conclusion to that provided by a partial picture.</p> <p>This could occur in a range of scenarios and needs to be considered in our selection of data sets, and the controls and safeguards that we may apply before relying on the decisions or outputs from a given model.</p>
 False negatives and false positives	<p>A false positive is an outcome where the model incorrectly predicts the result as positive, while a false negative is an outcome where the model incorrectly predicts a negative result. This occurs because AI works on the basis of probabilities, and may be exacerbated by limitations in its training data.</p>

The severity of impact could differ by use case from, for example, a missed sale opportunity to an incorrect medical diagnosis. Therefore it is crucial to recognise this possibility early and to consider mitigations such as:

- not relying on a model where its confidence in the prediction is below a certain threshold;
- introducing additional controls or human checks.

The exact approach taken is likely to depend on the potential impact and the relative costs and benefits.

Risk	Explanation and Further Considerations
 Lack of explainability of algorithms	If an algorithm cannot be explained, or acts as a black box, it may lead to vendor lock-in because you may struggle to build on or to move away from the existing system with a decent level of confidence in the outputs. This should be considered in your procurement documentation and you may wish to include open standards, royalty-free licensing agreements, and public domain publication terms. See the Guidelines for AI Procurement for further detail. This may also lead to poorer outcomes if the model cannot be adjusted in instances of concept drift (see below).
 Potential liabilities	We need to consider what liabilities may arise if the outcome from the AI is wrong, and where this liability may sit, particularly given any split in the ownership and use of the data, the algorithm and the training of the model itself. This needs to be considered in advance and may involve wider consultation and legal advice when allocating risk and drafting the contract.
 Safety	Depending on the use case, the application of AI can have safety implications. For example if AI were being used to automate the operation of a level crossing. Risks to safety need to be considered and this may mean greater testing or use of technology for which this is an established or closely analogous use case.
 Using AI for decisions	When we use AI in a decision making capacity, for example approval of an application, we need to consider the other risks detailed in this section more broadly and to look at the role of additional checks or appeal processes incorporating human judgement as a mitigation.
 Model Drift	Model drift describes the gradual degradation in the performance of a predictive model over time. Crucially, the relationship between the target variable (what we are trying to predict) and the independent variables (the data we use to train and score the model) changes with time.

There are two types of model drift:

Concept drift: where the properties of the target variable change. If the very meaning of the variable that is being predicted changes, the model is unlikely to work well for the updated definition. For example, the definition of what is a spam email has evolved over time, or, more suddenly, changes in buying behaviours due to the pandemic.

Data drift: where the underlying distribution of the features (which were used to train the model) changes over time.

For example, the gradual ageing of the population, seasonality, or a change in the way something is measured, such as unemployment rates.

Model drift can lead to inaccurate predictions, which can go undetected because the changes may only happen slowly over time. Although concept drift is less common than data drift, it can be more impactful as it could eventually make the model completely obsolete.

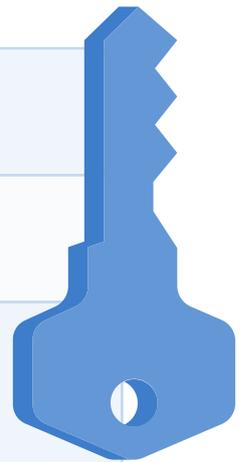
To address model drift, it is necessary to monitor the performance of the model over time (using multiple indicators) and make necessary adjustments (for example, refitting the model on updated data) to ensure its continued accuracy. Also, it is important to ensure that the training data reflects as much as possible the data that the model will experience in the real-world.

The use of data and AI offers significant opportunities, allowing us to obtain efficiencies and sometimes achieve insights which would not otherwise be possible, thereby benefiting our citizens. In securing

these benefits, we need to be mindful of the risks outlined here and to consider their management throughout the project and commercial lifecycle. It is best to identify risks early, to consider if and when they may materialise and ensure that mitigations are put in place ahead of time, including for risks such as model drift which may materialise well after go-live. Organisations should consider the model's longevity, the review of risks and how this fits into any product roadmap. By following these steps we can ensure that we reap the benefits of innovation in an appropriate and informed manner.

Key points

1. Engage early with the market and be ready to demonstrate in the business case that your proposals have been informed by both your market health and capability assessment and feedback from potential suppliers including SMEs.
2. Create an environment which enables innovative and creative solutions. Use early engagement with the market to start thinking about innovation and enable the market to suggest novel solutions to problems.
3. Appropriate, clear and efficient specifications are a critical factor in the overall timely and cost-effective delivery of projects. Specifications should focus on a whole-life value perspective, and align with the government's wider economic, social and environmental priorities and commitments.



Want to know more?

1. [Guidance and Tools for Digital Accessibility.](#)
2. [Service Manual – Testing for Accessibility.](#)
3. [GOV.UK – Understanding Disabilities and Impairments.](#)
4. [NCSC – Certified Cyber Security Consultancy.](#)
5. [CCS – Cyber Security Services 3.](#)
6. [Public sector equality duty.](#)
7. [Government Data Ethics Framework.](#)
8. [Ethics, Transparency and Accountability Framework for Automated Decision-Making.](#)
9. NCSC Certification.





5 Delivery model assessments

The right delivery model approach enables clients and industry to work together to deliver the best possible outcomes by determining the optimal split of roles and responsibilities.



Delivery model assessments

Contracting authorities should follow an evidence-based process to decide the most appropriate delivery model and structure for a specific project or programme. This process is known as the delivery model assessment (DMA) and it should be conducted proportionately on all public sector projects and programmes. For DDaT projects, this is a decision on who, through insourcing, outsourcing, or mixed-model delivery (see Figure 6), will develop and deliver and take responsibility for the various stages of a project or programme (see **Chapter 6** on agile development and testing).

Delivery model assessments are expected to be iterated over time in-line with the business case development process set out in the Green Book. The department should then reassess the delivery model assessment ahead of the Outline Business Case and ensure that any assumptions have been validated and factored into the Full Business Case. Delivery model assessments are expected to be iterated over time in-line with the business case development process set out in the Green Book.

The department should then reassess the delivery model assessment ahead of the Outline Business Case and ensure that any assumptions have been validated and factored into the Full Business Case.

The DMA is a strategic decision that should be given consideration with an appropriate level of analysis and attention applied. It should usually take place early enough to inform the first business case stage and be proportional to the size and complexity of the project or programme. For central government departments and their ALBs, this is the Strategic Outline Case (SOC) and where this stage is too early to elicit sufficient objective data to support the full DMA, the principles should be applied to get to a shortlist of options.

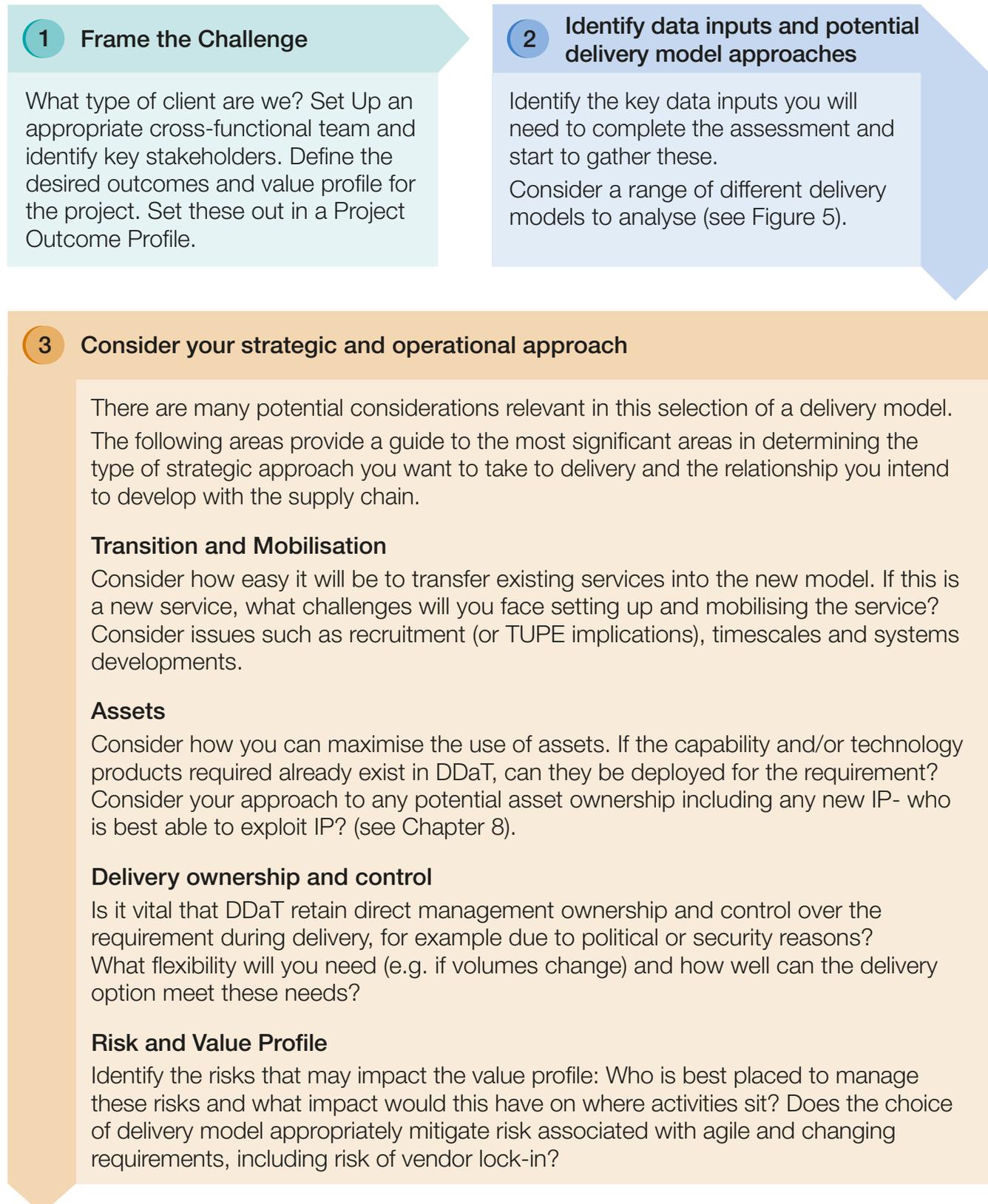
The right delivery model enables contracting authorities and industry to work together to deliver the best possible outcomes. When designing the appropriate delivery model, contracting authorities will need to consider a number of factors including wider strategy on cloud, risk and capability and an analysis of the value profile, strategic risks, client and market factors is required and should inform the split of roles and responsibilities across the client and market.

Undertaking a DMA

The structured approach, set out in Figure 5, provides a high-level framework consistent with the options appraisal approach prescribed in the Green Book. Contracting authorities should consider a wide range of potential delivery models and how each model would support a value-based approach across the whole lifecycle.

The DDaT sourcing delivery models (set out in Figure 6), set out the four broad approaches by which DDaT projects will usually be delivered. Once we understand our strategic approach to the delivery model, we need to reflect that in our commercial approach – the way we procure, contractualise and manage projects and programmes (see **Chapter 7**). Guidance on DMAs is provided by the Cabinet Office and will be updated in 2022.

Figure 5: Delivery model assessment approach



The Market

Assess the capability and capacity of the market, including whether there is a viable solution in the market that will deliver better overall value for the public than in-house delivery. Can the expertise and capability of internal delivery sufficiently match or better the supply available in the market?

Internal Capability

Consider the capabilities and skill sets needed and existing capacity. Will it be possible to find or obtain the required skills and capabilities in-house in a permissible timeframe for the requirement? What will the training and recruitment impact be?

Strategy and Supplier Interaction

What is the strategic significance of the requirement? Consider how well the delivery model aligns with departmental and government strategies and policies. How will it ensure delivery of strategic objectives, such as SME engagement, equalities or social value? Consider nature of relationship desired with potential suppliers i.e. collaborative, transactional etc.

Cyber security

What is the level of cyber-security risk inherent in the requirement and how is this impacted by possible delivery models? Consider your own risk appetite and conduct a documented risk assessment of the contracting authority's requirements.

4 Assess the whole life cost of the project

Use your strategic approach and specification to identify potential cost drivers for the build phase and a period of running. All projects should undertake benchmarking and develop a Should Cost Model.

5 Align the analysis, reach a recommendation and sense check your findings

Combine the whole life cost evaluations of different solutions with the non-cost criteria. Learn from evidence, past-projects and colleagues across the public and private sector to test and sense-check your findings. Consider a Red Team review to validate your recommendation. Complete further market engagement where necessary.

6 Design an appropriate commercial strategy

Align commercial considerations including form of contract, payment approach, and performance management with the delivery model. These are set out in more detail in Chapter 7.

Figure 6: DDaT sourcing delivery models

DDaT Delivery Models



Insource	Bridge	Borrow	Outsource
<p>Deliver internally, using existing capability (such as the DDaT Profession) and products.</p>	<p>Deliver with a hybrid approach, utilising capabilities/products both internally and from the market.</p> <p>Uses supplier capability to bridge organisational capability gaps to augment delivery until internal capability is sufficiently developed to own and run the requirement.</p>	<p>Deliver requirement in entirety by borrowing capability on fixed term from the market. Uses supplier capability to fulfil a requirement that would ideally be delivered internally (Insource or Bridge), but cannot be due to lack of capability or the nature of the delivery requirements.</p>	<p>Deliver requirement through buying capability/product from the market</p>

Programme leadership



Delivery Team



Supplier Internal



Agile delivery models

Agile delivery models and approaches to service development are required as part of the DDaT Service assessment (see **Chapter 3**) and are most suitable when:

- dealing with situations with complex problem(s), unknown solutions and/or scope that is not clearly defined
- customer preferences and solution options change frequently
- customer and/or end users are available for close collaboration and to provide rapid feedback
- requirements can be broken down into priorities and dealt with in iterative cycles

There is value in incremental developments with an outcome(s) that can be utilised by the customer at the end of each cycle.

Benchmarking

Contracting authorities should undertake benchmarking of key project deliverables including cost, schedule, GHG emissions and agreed outcomes at each stage of business case development. This will be supported by a new data IPA benchmarking hub in 2022.

The use of benchmarking data will drive consistency and the overall robustness of cost estimates. Benchmarking is the analysis of information and good practice from past projects and programmes to create data reference points. It can generate the inputs required for Should Cost Models, provide the building blocks for whole-life cost evaluation, and provide a comparator for project and programme performance.

Using Should Cost Models to understand whole life value

A Should Cost Model (SCM) helps to provide a clear understanding of the whole-life value of a contract, ensuring that opportunities and benefits are considered alongside the costs and risks of delivering a project or programme. A SCM should be undertaken as part of the delivery model assessment (DMA) to drive a better understanding of the whole-life costs and risks associated with including the set-up, operation and decommissioning of different options and scenarios, such as emergency migration. The identified costs should be agreed and reflected in the pricing model of a contract.

All contracting authorities should carefully consider end-of-life costs as part of the SCM, allowing a better understanding of the costs associated with decommissioning the project, programme or service. SCMs should also factor in the cost of continuous improvement, preventing and/or remediating legacy IT concerns, whilst ensuring that the appropriate knowledge transfer takes place at contract end.

All procurements should produce a proportional SCM during the planning and preparation stage to support the DMA. The level of investment in producing an SCM will vary with the complexity and significance of the procurement, and the purpose for which the SCM is produced – an SCM that is required to support a Full Business Case (FBC) should be more detailed and accurate than one needed just for DMA purposes.

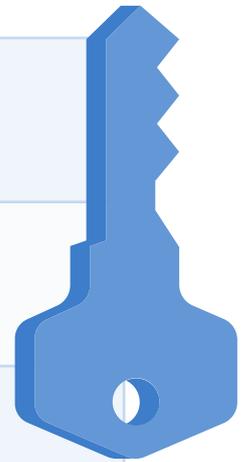
Using public sector demand strategically

One of the core things which will inform the options assessed through the DMA, is whether there may be any benefits achieved through aggregating or disaggregating demand.

By splitting up the project into smaller parts and understanding the scope of innovation within those parts, we can increase start-up, SME and VCSE participation through appropriately-sized procurements. Alternatively, where shared requirements, whether for a complete solution or one component of a solution, exist in projects across contracting authorities or programmes owned by a single contracting authority, we should consider harmonising our demand to enable cost benefits and increased start-up, SME and VCSE participation in developing innovation as part of larger supply chains.

Key points

1. The delivery model assessment should take place early in the preparation and planning stage of a project or programme and may be revisited at later stages of the Business Case process as assumptions and market engagement are clarified.
2. To complete a delivery model assessment, start by thinking about the outcomes you want to achieve, your strategic approach, and a robust understanding of value before determining the appropriate commercial approaches for the delivery model.
3. Projects and programmes should undertake benchmarking of key project deliverables including cost, schedule, emissions, and agreed outcomes at each stage of business case development.
4. Should Cost Models should be produced as part of the planning and preparation stage to inform the delivery model assessment and pricing model.



Want to know more?

1. Project Initiation and Project Development Routemap, in particular the Governance Module.
2. **Delivery Model Assessments Guidance Note.**
3. **Should Cost Modelling Guidance Note.**
4. **Should Cost Modelling – Tools and Templates.**
5. **HM Treasury Guidance – Producing quality analysis for government.**
6. **IPA Guidance – Best Practice in Benchmarking.**
7. **IPA Guidance – Benchmarking Capability Tool.**
8. **CDDO Spend Controls.**
9. **Minimum Cyber Security Standard.**
10. **UK Government Security Information.**



6 Agile development – testing and learning

Testing a DDaT product or service is the best way to understand the environment, constraints, requirements, risks and opportunities.

Iterative approaches to development

An agile approach to the development of new DDaT data services is required as part of the DDaT service assessment (see **Chapter 3**), and iteration is one of the cornerstones of agile delivery.

In an agile project, the detailed requirements are not clear at the outset, but the problem statement is known. This evolves through an ongoing series of short ‘sprints’, with the conclusion of each sprint being to test the outcomes, validate whether these are in line with expectations and consequently determine the requirements for the next sprint.

Rapid iteration enables new ideas and innovations to be delivered with speed and productivity and developed through fast cycles of building, field testing and learning.

This includes progress from ‘discovery’ stages, where an understanding of user needs is sought and multiple potential solutions, or even an understanding that the problem does not need solving, may emerge. These recommendations should then be tested and eliminated as necessary through ‘alpha’ and ‘beta’ stages of development, as set out in the DDaT Service Manual (see also Figure 7) allowing just

barely-good-enough prototypes to be tested for feedback in order to spot problems early and resolve them quickly. As potential solutions are improved and/or eliminated, this allows the quality of the final product or service to improve as the scope of it expands. The **Contracting for Agile Guidance Note** provides further information on what agile is, and the associated appropriate procurement approaches and commercial models, as well as how to manage these projects post-award including how to act as an Intelligent Client Function and performance management.

Iterating against outcomes

Measuring and reporting progress should be built into agile projects to ensure each iteration is progressing towards the outcomes set out in the Project/Programme Outcome Profile (POP). The POP tool developed by the Infrastructure and Projects Authority (IPA) will enable contracting authorities to clearly link the contribution of an individual project to the delivery of priority outcomes, whether directly related to the project, departmental aims or cross-governmental priorities (see **Chapter 3**). This will help suppliers understand contracting authorities’ ambitions without being prescriptive about how to deliver outcomes. A shared focus on outcomes, rather than scope, will unlock innovation and drive continuous improvement.

“ As potential solutions are improved and/or eliminated, this allows the quality of the final product or service to improve as the scope of it expands”

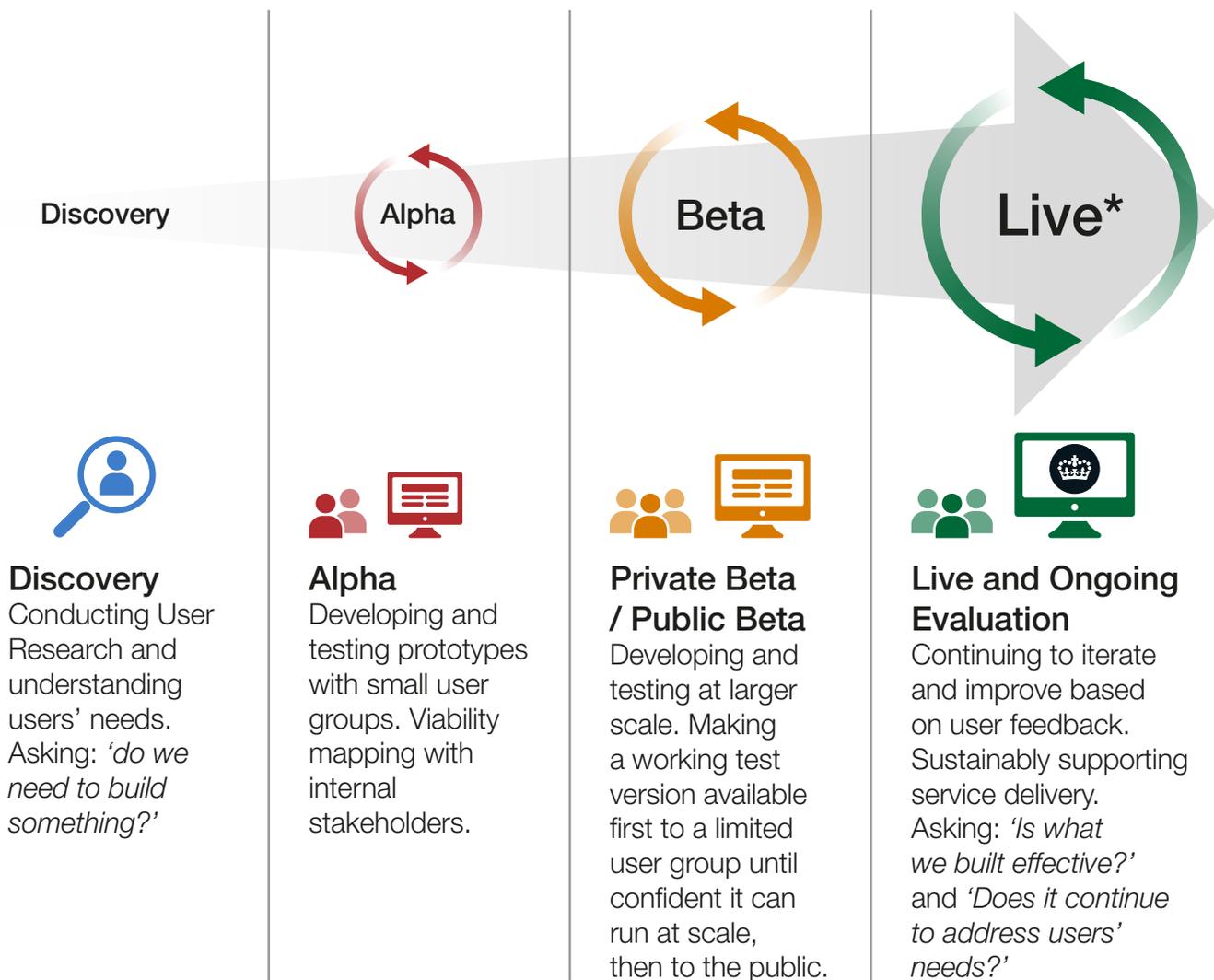
These clear and measurable outcomes should be set at the outset of a project or programme and tested through approvals stages to enable agile ways of working and iterative development, allowing us to measure progress towards an appropriate solution, ensuring value for money.

Contracting authorities should work with the market to set out a roadmap of milestones, stages or product iterations, each with a set objective which moves towards the intended outcome. Progress against this roadmap should be continually monitored and this outcome-based approach forms a crucial part of business cases to enable an understanding of how the agile project will deliver value for money.

Agile programmes depend on using lessons learned from one release to the next. Contracting authorities should consider that flexible resource allocation may be required to enable fast, simple processes to evaluate the progress of work and the decision to either ramp it up, put it on hold, or shut it down entirely will be required.

Figure 7: Agile methodology

Agile methodology



*See the [Contracting for Agile Guidance Note](#) for further information on agile in a Commercial context.

The 'Digital by Default' process. *First published 2013 by GDS.*



Testing and piloting solutions

When to test or pilot

Iteration and a focus on continuous improvement for agile projects should take place across the commercial lifecycle. However, an agile approach may not be appropriate for every project. Testing approaches should be proportionate to the size, complexity and level of uncertainty in delivering a service. Piloting should also be proportionate to the existing market capability. Where there is limited capability, piloting may be appropriate to build up that capability whilst collecting data or evidence to inform any future process.

Planning which testing approaches to include and whether to include a pilot should begin at the earliest strategic stages of a project, before the start of any procurement process, and should be incorporated into the delivery model assessment, sourcing strategy, bid documents and evaluation processes. Ensure you communicate the likelihood that a pilot phase will be used through early market engagement to seek feedback from the market to inform the procurement.

The testing programme should align to key project milestones throughout the lifecycle of the project up to full implementation.

Options for testing

- Trial programmes and proofs of concept.
- Scoping phases, agile approach and innovation partnerships.
- Test and learns.
- Pilots.

In many instances it will be appropriate for departments to use one or more testing approaches at earlier stages of project development, with the pilot being the final testing stage prior to a full-scale rollout of services. The testing and piloting services guidance note sets out when certain tests may be more appropriate in a project lifecycle.

Early testing enables departments to understand the viability of a project or outcome at its various stages of development. This allows the department the opportunity to change the course of action, limiting cost and time where it becomes apparent that the project will not deliver the required outcome. Tests can also be used to explore new technologies and delivery innovations for services that are already outsourced.

Designing effective tests and pilots

DDaT products and services can be more susceptible to change than other sectors and a firm foundation is essential for scaling and sustaining agility – tests, including pilots, should be developed to ensure success and the most value is obtained to mitigate potential risks prior to scaled implementation.

This includes using resilience testing to understand the impact of change on the delivery of the product or service and to ensure our systems are sustainable and future-proofed.

Key considerations when designing effective tests:

- Set clear, measurable objectives and success criteria.
- Identify the scope and scale of what will be tested, and where they will be run.

- Put in place the right resources.
- Establish clear timescales and embed these in the overall project plan.
- Ensure the right commercial mechanisms are in place.
- Allow sufficient time at the end of tests for due consideration of the results.

Where the new requirement is to replace a product or service, including legacy IT, testing should consider options including dual running and a focus on timely decommissioning and migration of data and services.

Testing data-based projects

On data-based projects one of the key issues can be testing with realistic or production data early enough. Complex data projects may require the merging of data from multiple sources and applications. To minimise risk, therefore, real data should be used as early as possible and the team should create processes so that they can report and respond to data failures and complexity. Until real data is used, we can never be certain an application is working correctly and this should be raised as a risk particularly in complex data integration projects.

Procurement Reform

The Bill does not change the policy on testing and piloting but the new Competitive Flexible Procedure will provide greater flexibility for contracting authorities to design procedures which use testing and piloting as formal parts of the procurement and to set out clear rules in advance about how the results of any pilots will be used and down-select decisions made.

Meeting the challenges of scaling

Scaling after testing

Scaling from a pilot to full production is a project like any other and faces the same challenges – lack of senior support, funding, focus and time. It is therefore important to ask the same questions as you would of any other large-scale project:

- How feasible is the requirement at the necessary volume?
- Can the requirement be defined and will its delivery meet the user's needs? (See **Chapter 7** on outcome-based approach).
- Does the organisation have the capability to deliver or manage an organisation that can deliver at scale? This includes both the ability to deliver the system or programme but also the ability to support the system or service at scale, taking into account value for money and wider stakeholders.

Design considerations

Pilot

Consider your end goal at the design stage as the business develops an understanding of the key challenges that need to be addressed and the project objectives. The business should also have a shared definition of scale. The pilot should be designed with a control for comparison and be representative of the community or users it is intended to serve. This makes it easier to replicate without relying on specific requirements or capabilities.

Standardisation

This should apply to ways of working, process and documentation to ensure, where possible, results can be replicated.

Monitoring and success criteria

Be clear about what success looks like and the data the pilot will need to collect to know:

- how well the pilot has addressed the challenges or met the objectives
- whether the pilot can be scaled to full production; or
- which areas need to be optimised or possibly reassessed

There should be a clear and approved approach for data gathering including the documentation and sharing of lessons learned. The central review of pilot information is crucial, particularly in instances where it can be linked back to success or failures as an ongoing approach to testing and learning.

Planning

Revisit the definition of scale – does it still stand or does it need to be assessed in light of the results from the pilot? What is the plan for scaling? The output from the monitoring and evaluation stage should drive these discussions:

- Agreeing the rate of scaling or expansion.
- Assessing the organisational capacity to scale to full production.
- Resources – increasing capacity of existing resource or recruiting additional resource.
- Timescales.
- Commercial arrangements – see commercial considerations.
- Communications.
- Governance.

Commercial considerations

Using separate suppliers for each element of the pilot. This can have a number of advantages – it allows SMEs to bid for services that require specialist technical expertise, and ensures we can choose from a competitive field when the future service is procured. The use of suppliers, for example, for independent monitoring and evaluation, can also provide an objective assessment of the services and scaling preparedness.

Contracting authorities should recognize that running multiple procurements may introduce additional cost and complexity, with repetition of work being a key risk without effective knowledge transfer or a single, consistent integrator. Projects and programmes must allow sufficient time for the procurement of the products or services, and where appropriate and lawful, use frameworks or direct award procedures. This may not always be appropriate where agile projects are not suited to pausing between phases to allow for re-procurement.

Avoid being ‘locked into’ a supplier’s solution

This is especially the case if the supplier(s) is involved at the design or concept stage. Requirements should be drafted to be supplier or technology agnostic and intellectual property implications should be fully assessed.

Many suppliers provide guidance on how to build systems with their tools which avoid lock in. This should be considered and referred to and there should also be an obligation on the supplier to maintain clear (and current) documentation during the pilot and as part of the handover/knowledge transfer process.

This can include, but is not limited to, design documents, system architecture, sprint planning/story boarding, transition plans, risk management plan, process flows, training guidance, evaluation reports and benefits assessment.

Beware of 'pilot creep'

There should also be clear processes and the use of breakpoints at the end of each stage within the contract to allow for (i) pilot assessment to determine the status of the pilot e.g. to assess its suitability for scaling; (ii) limited pilot extension or expansion e.g. to facilitate independent monitoring, evaluation or to test an incremental roll out; and (iii) onboarding of new delivery partners. The contract should be time-limited to reflect the nature of the pilot and should be clear on the:

- problem statement or goal – what issue does the supplier need to solve and how does the product or service relate to the project or business objective(s)?
- supplier obligations – this can also include 'scaling assistance' although suppliers may wish to agree a rate card for these services
- performance objectives and evaluation criteria
- deliverables - supported by clear acceptance criteria, Q&A methodology and processes and a robust sign off process
- governance and reporting – this should include a regular feedback mechanism to facilitate course correction in light of any issues
- resourcing - with the appropriate level of experience (this should extend to the knowledge transfer stage)
- funding model

Pilots should be able to be tested in the market as these are developed into fuller solutions. Contracting authorities must maintain the in-house knowledge and capacity to enable management of solutions and a home for knowledge transfer. There should be appropriate governance and sign off to ensure oversight and separation of suppliers from future commercial decisions and practice.

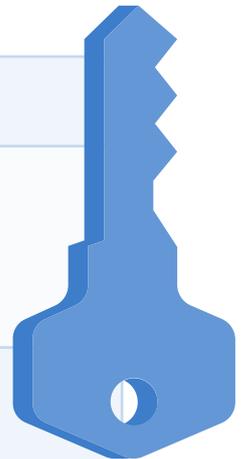
Knowledge transfer

Contracting authorities must plan for effective knowledge transfer back to the business and/or other suppliers. The project should ensure that it retains appropriate ownership of the outputs and deliverables, including any intellectual property rights (see **Chapter 8**), and is able to distribute or disseminate information. The project may wish to hold industry days or workshops to allow other suppliers to access key learnings from the pilot.



Key points

1. Iteration is a cornerstone of agile delivery, and is required as part of the digital, data and technology service assessment.
2. Build measuring and reporting progress into agile projects to ensure each iteration is progressing towards the outcomes set out in the Project/ Programme Outcome Profile. Work with the market to set out a roadmap of milestones, stages or product iterations which move towards the intended outcome.
3. Testing approaches should be proportionate to the size, complexity and level of uncertainty in delivering a service, as well as to the existing market capability.
4. Carefully consider the design and commercial considerations when scaling from a pilot to full production of a requirement.



Want to know more?

1. [Service Manual – Agile Delivery.](#)
2. [Service Manual – Agile Delivery: Developing a Roadmap.](#)
3. [Service Manual – Agile Delivery: Measuring Reporting Progress.](#)
4. [Service Manual – Testing for Accessibility.](#)
5. [18F Accessibility Guide Checklist.](#)
6. [GOV.UK – Understanding Disabilities and Impairments.](#)



7 Preparing to go to market

Preparation is the key to achieving flexible and efficient procurement processes that encourage broad participation and are open and accessible to all.

Commercial approach

Deciding on the correct commercial approach is critical to achieving the intended benefits and wider value. The commercial approach should be based on how much delivery responsibility we are willing, able or need to take on, versus outsource. This may change at each stage we go to market and should be linked to the delivery model and the desired outcomes (see Figure 6 for DDaT delivery models). Depending on the commercial approach and nature of the project, this will impact the procurement procedure and contracting strategy.

Contracting authorities should seek specialist advice to establish the most appropriate commercial approach and procurement strategy which optimises whole-life value and involves all relevant team members early enough for them to contribute to this value. We then need to select or design an appropriate form of contract for the complexity and criticality of the project or programme which reflects how we intend to manage the contract based on the appropriate level of resource capability and capacity.

Developing the commercial model

- Traditional pricing models such as fixed price or time and materials for the whole project are not optimal for agile ways of working, or where contracting authorities are uncertain of the detailed solution and are procuring capability from suppliers.
- In order to incentivise delivery productivity and efficiency, an outcome-based contract based on collaboration and which reflects a shared vision is likely to be more appropriate and will enable scope, priority and sequencing decisions to be made without re-working commercial arrangements.
- Similarly, outcome-based and gain share contracts will enable shared risk and reward for remediating legacy IT.⁷
- For legacy remediation contracts 'locked-in' to a specific supplier, contracting authorities should consider whether direct awards to incumbents may be necessary. Legal advice should be taken before any direct award. These situations should be avoided as far as possible when deciding on the contracting strategy for a procurement. The Guidance Note on Dealing with Legacy IT provides further information on this topic.

“ A successful framework contract should be based around principles that align objectives, success measures, targets and incentives so as to enable joint work on improving value and reducing risk”

- Innovation focused contracting routes such as Innovation Partnerships or SBRI procurements may be particularly attractive to SMEs.

It is necessary to develop the commercial approach and the procurement strategy before making the decisions needed for the contracting strategy. Digital teams should be included in the design of the commercial and contracting model at every stage.



Outcome-based approach

Instead of deciding on a solution upfront, contracting authorities should focus on outcomes to enable agile working and innovative solutions.

These outcomes may be project specific and/or those linked to wider departmental or cross-government priorities such as:

- fewer non-emergency calls to an emergency service number
- enabling staff that work remotely to access and store documents securely
- reducing or offsetting environmental impacts

This will support agile working, and while it is possible to undertake an outcome-based approach on a project which is not agile, any effective agile project will be outcome and user focussed and optimised for continuous development and learning. More information on testing and learning can be found in **Chapter 6**.

Contracting strategy

This is where we define acceptable contract parameters informed by the commercial model. This includes:

- ensuring the outcomes and/or technical specifications are integrated into the contract
- defining critical risk allocation, and ensuring it is properly reflected in the contract
- documenting the decisions made earlier on the contractual roles and responsibilities
- defining clearly the rights and obligations of each party and the associated contractual processes required to implement the commercial model, manage the contract and deliver the project

The contract is where all the key elements of the project are drawn together and should be a fully integrated, consistent suite of documents. It will define what you want to buy (specification), the method and timeframe for delivery, risk allocation and other key commercial terms (e.g. the payment mechanism and KPIs) and what happens if things go wrong.

Proportionality

The complexity of contracts should match the scale, complexity, criticality and lifecycle of the goods/services they are attached to, and teams should be sufficiently resourced to actively manage contracts once they are live.

Remedies for poor or non-performance should be proportionate to the overall strategic value of the contract.

Procurement procedure

Once we have considered the commercial approach and contracting strategy, we need to select the most appropriate procurement procedure. Cabinet Office policy on the choice of procurement procedure can be found in PPN 12/15. The business case should justify the chosen procedure and there are a number of key considerations, which include:

- the contract award method we would want to follow (e.g. negotiation, direct award, frameworks, competitions etc.)
- who is responsible for developing the solution
- who would take on the responsibility for maintenance and updates

Use of frameworks

Frameworks are an efficient method for the government to procure common products and services and can provide an opportunity for contracting authorities to access economies of scale. They can also lead to an overall reduction in bid costs and duplication of effort on behalf of suppliers, as certain information is requested and tested at framework award level.

As such, where we are using a 'borrow' or 'outsource' delivery model (see **Chapter 5**), we should look first to available frameworks to see whether the need we are procuring for is already met by existing contracts and contracting mechanisms. However, using frameworks inappropriately can have negative consequences for contracting authorities, markets and suppliers and can unintentionally inflate prices.

A successful framework contract should be based around principles that align objectives, success measures, targets and incentives so as to enable joint work on improving value and reducing risk. This should then be combined with transparent and meaningful performance measurement and work allocation procedures.

Procurement Reform

Dynamic Purchasing Systems will be replaced by Dynamic Markets in the new regime. Their use will be expanded beyond common goods and services. The operation of frameworks will also be different, with changes to notices, duration and the ability to bring new suppliers onto the framework during its term.

CCS Frameworks

The Crown Commercial Service (CCS) offers a number of framework options through which DDaT products and services can be procured. CCS frameworks offer a full set of standard contract schedules and terms & conditions, and publishing the appropriate contract, tailored to the particular project as part of the tender process can significantly reduce the amount of time needed to finalise contracts post-competition.

Contracting authorities should take into account a number of factors to evaluate which framework is most appropriate for the project or programme including:

- impact on procurement timetable
- the assurance criteria for suppliers under the framework and whether these are sufficient for the needs of the project and programme
- The market health and capacity, including range of suppliers
- suitability of contract terms

Contracting authorities must use frameworks appropriately, and only procure products and services that are within scope of any particular agreement. Framework providers can provide support for this decision-making and further guidance on sourcing general services and capability is provided in the Sourcing and Consultancy Playbooks respectively.

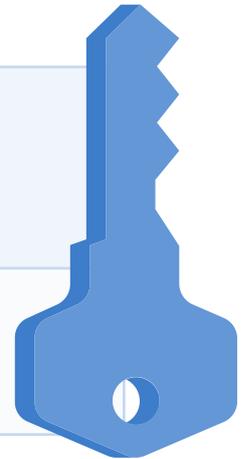
To ensure a framework is appropriate for your requirements, contracting authorities should read all the framework documents before selecting it as the route to market. Contracting authorities should check with the framework provider that it meets their requirements, provides the necessary, relevant and proportionate protections and is suitable for the criticality and value of the product or service. Keeping up to date pipelines will avoid the time pressures that can lead to inappropriate framework selection.

Procurement Reform

Under the future regime, contracting authorities will be able to publicise new opportunities and engage with the market through a Planned Procurement Notice or a Preliminary Market Engagement Notice (or both).

Key points

1. Effective, sustainable contracts should support project and programme outcomes, be designed to implement and align with the selected delivery model, be consistent with the best practices and policies set out in this Playbook, drive continuous improvement and be structured to enable an exchange of data using open standards.
2. Procurement processes should be of proportionate duration and effort to the size and complexity of the contract opportunity so as not to create barriers to entry for start-ups, SMEs and VCSEs. The business case should justify the chosen procedure.



Want to know more?

1. Availability of Procurement Procedures (Decision Tree): [PPN 12/15](#).
2. [Model Services Contract](#).
3. [Public Sector Contract](#).
4. [CCS Technology Frameworks](#).
5. [The Technology Code of Practice: Define your purchasing strategy](#).
6. [Cyber Resilience in Local Government Supply Chains](#).

Preparation and planning

Publication

Selection, evaluation and award

Contract implementation

Contract end



8 Designing effective contracts with common data standards

Contracts should deliver a sustainable, resilient and effective relationship, focused on outcomes, and that creates long-term value for all.



Effective contracting

Public sector contracts should be designed to support an exchange of appropriate and meaningful data, drive collaboration, improve value and manage risk. This will allow roles, responsibilities and scope to evolve during the life of the contract and adapt to changing user needs and technologies.

Core Commercial Priorities

Risk allocation

We recognise that risks exist as a normal part of every project and programme. Ensuring that risks sit with the party best able to manage them is key to delivering value for money and successful outcomes. Suppliers should not be asked to take on unlimited liabilities, other than the small number of circumstances where this would not be lawful or where a commercial cross-government policy has been agreed.

Complex situations commonly require risk trade-offs which may include tolerated and accepted risks to achieve the intended outcomes and risk allocation defines which party or parties will assume (or remain) responsible for which risks and to what extent. It should be informed by market engagement and take into account both the practical capability and the financial capacity

of suppliers to manage those risks. Where the requirement involves AI or the usage of data, the risks referenced in section 3 should be considered as part of the overall allocation and management of risk.

This should be supported by good risk management aligned to the project and programme strategic outcomes set out in the Project/Programme Outcome Profile.

Managing commercial risk

Managing commercial risk is complex and there is no one-size-fits-all model. Contractual provisions for risk management should be proportional to the size and complexity of the contract, informed by engagement with the market and reviewed throughout the life of the contract. This should include any requirements for ongoing financial monitoring and resolution planning information (see **Chapters 10 and 11**) and any risk mitigation strategies put in place. The Cabinet Office Markets and Suppliers Team can provide advice on appropriate risk mitigations on specific contracts.

Key performance indicators

Contractual KPIs are used to measure progress and performance of suppliers in the delivery phases of a project (e.g. during set-up, testing and operation).

“ Ensuring that risks sit with the party best able to manage them is key to delivering value for money and successful outcomes ”

These should be relevant and proportionate to the size and complexity of the project or programme and drive both a focus on outcomes, aligning with the Project/ Programme Outcome Profile, and continuous improvement. However, contracting authorities should have regard to any risks outside the suppliers’ control and care should be given to how outcomes are linked to supplier KPIs and payment.

As per the Service Manual, DDaT contracts must publish performance against four specified mandatory KPIs. These are:

- cost per transaction
- user satisfaction
- completion rate
- digital take-up

Further information on the four mandatory KPIs for DDaT contracts can be found [here](#).

There is also a wider requirement, in line with the Government’s transparency agenda, for performance against four KPIs from each of the Government’s most important contracts to be made publicly available. These four should be the three most relevant to demonstrating whether the contract is delivering its objectives and one social value KPI, and they should be measured regularly.

If the four mandated digital KPIs are also the most relevant for an individual contract then publication can be limited to performance against those four and one social value KPI. However, the programme may determine that only one or two of those mandated four are among the most critical three for their service and may select additional KPIs for publication. In this way, DDaT contracts may require the publication of anywhere between five (four mandated and one social value) to eight (four mandated, three most relevant and one social value) KPIs. KPI performance that is published in one place does not need to re-published in another.

Procurement Reform

The Bill states that all contracting authorities (i.e. including local authorities) will be required to publish three KPIs and associated performance annually on all contracts with a value, or expected value, over £5 million. (This will not apply to overarching frameworks, private utilities, concession contracts and those covered by Light Touch rules.) The plan is that this will be published on the single, central platform. The focus on setting appropriate KPIs and properly monitoring and recording performance will intensify because the performance data could grant contracting authorities discretionary rights to exclude suppliers who are perennial poor performers and have not responded to calls to improve.

Payment mechanism and pricing approach

The aim of the payment mechanism is to reflect an optimum balance between risk and return in the contract. As a general principle, the approach should be to link payment to the delivery of outputs and/or value of the work and supplier performance, and the approach to pricing should reflect the level of certainty or risk around the scope and requirement.

Where the scope of a project is certain, then fixed pricing may be appropriate and where there is increased uncertainty in scope, a variable approach may be more suitable to achieve best value for money. For agile projects, contracting authorities should select payment milestones to ensure that the delivery of non-functional requirements are included, avoiding milestones based on the delivery of the agile process itself, (e.g. completion of a specific number of sprints). Similarly, 'pay as you go' mechanisms may be the most appropriate for cloud or software as a service (SaaS). Where there are a number of linked procurements, it is important to consider a holistic approach and ensure that the individual payment mechanisms support the overall intended outcomes.

Contracting authorities should ensure sufficient rationale for the selected pricing approach in tender documents. The final pricing model under a contract should include all recognised charges and lifecycle costs in line with the Should Cost Model assumptions to ensure transparency of costs and reduce risks of cost increases. This should include costs of migration at contract end or in the event of emergency. Additionally, transparency on payment practices throughout the supply chain is essential to ensure we are compliant with our prompt payment obligations (see **Chapter 9**).

Onerous contracts

A possible consequence of getting risk allocation and the approach to pricing wrong is that contracts can become loss making for a supplier.

When a contract is publicly designated by a supplier as onerous, this should prompt a root cause analysis and a conversation with the supplier about the reasons the contract has become onerous and the options available to address this.

Fair returns

Short-term thinking can reduce the value for money that the public sector as a whole is able to derive from markets. Supplier reports examples where public sector Contracting Authorities have mandated unreasonable payment mechanisms, applied unreasonable terms and conditions and/or sought unsustainable cost reductions. This can create a bias towards low quality and can increase the probability of contract failures. In addition, suppliers may exit the market to the point where competition is severely weakened.

The fundamental principle is that contracts should be profitable with fair returns and expectations need to be reasonable for suppliers to remain interested and for the market to be sustainable.

Digital, data and technology considerations



Legacy IT and up-to-date products

Legacy IT refers to systems and their component software and hardware that are outside of vendor support, on extended support and/or on bespoke support arrangements. Legacy IT can have a significant negative impact on the UK and the government, including on cyber and national security and the operational resilience of critical systems, transformation of services and value for money.

Managing IT obsolescence is essential for better outcomes and to achieve that, contracts should include provisions to ensure software and technology is kept up-to-date and in mainstream support by the appropriate party for the duration of the contract and any extension. Key contractual considerations include:

- what is meant by ‘up-to-date’ – contracting authorities should consider value for money to decide whether it is necessary to have the latest version of any software, or if an older, but supported version may be appropriate
- a robust lifecycle management process including:
 - the patching schedule and the frequency at which bugs are addressed and features changed and updated over time
 - the suppliers’ intended roadmap for their product and any planned obsolescence

- the allocation of risk and reward for legacy IT remediation, supplier risk management and reporting must include the status and risk mitigation for current software and end of life software (see above)
- asset management to include all DDaT assets
- the ability for data extract and sharing capabilities
- KPIs relating to legacy mitigation and remediation
- switch off/switch over plans

Where contracting authorities are aware of services which may become legacy, risk should be allocated so as to incentivise suppliers to address this and, where appropriate, transform rather than maintain the service. Contractual provisions should be put in place to ensure suppliers review, report and act on the status of any current and potentially future legacy IT risks with appropriate regularity. This reporting should include the supplier’s compliance with ‘evergreen’ clauses and be overseen by a member of the supplier’s management team with DDaT and cyber experience.

Getting this right at the start and throughout will ensure that legacy IT is prevented from building up and enables steps to be taken to mitigate risks as they occur. This will help to safeguard against risks including cyber-attack and threats to national security, enables operational resilience, allows for digital transformation and provides better value for money.

Intellectual Property (IP)

Intellectual Property developed in the course of the contract should be owned by the party or parties best able to exploit it. Government needs to move away from binary interpretations of IP ownership and instead consider this on a case-by-case basis to maximise long-term value which can bring benefits to both contracting authorities and suppliers. Strategies for IP should consider possibly contradictory commercial benefits, risks and unintended consequences. A number of these factors are noted below and Figure 8 sets out possible options for IP and when they may be appropriate.

A separate **Guidance Note on Intellectual Property Rights** has also been published alongside the Playbook. Please refer to this for further guidance and information. The Guidance Note covers what IP is, how it relates to Commercial/procurement, commercial actions to take, as well as providing additional guidance on the ownership options available to contracting authorities and when they are most suitable.

Maximising the benefits of IP for the UK

If a supplier owns and can exploit IP, they are able to realise a benefit over and beyond individual contracts. This benefit would be removed or reduced if contracting authorities impose contractual provisions such as the Crown ownership of any new IP and contracting authorities should expect that increased control over IP will result in a proportionally greater cost. When considering IP and ownership structures, contracting authorities should consider how best to avoid supplier lock-in. Further information on how to do this can be found in the Legacy IT Guidance.

However, the government is the custodian of data about or for all of our citizens. Maintaining the integrity and security of this data is at the core of the government's approach, but we also need to protect the intellectual value of this data as an asset used for the benefit of the UK overall. The value of this data as an asset must be recognised and protected from hostile use, misuse or other commercial exploitation which does not confer appropriate benefit back to the UK.

Maintaining a competitive market

If the proposed contractual position does not grant adequate ownership or licence rights to the Crown, consideration should be given to the impact when re-competing the contract or otherwise using that IP to avoid being placed in an ongoing single supplier position. Open sourcing is the default ownership option across the public sector. Buyers should be aware of ownership or licence rights and how these impact the ability to publish as open source. Please see points 3 and 4 of the Technology Code of Practice and Service Standard 12 for further information, and the Guidance Note on Intellectual Property Rights for further guidance on ownership options.

Encouraging innovative solutions

Contracting authorities should also consider whether Crown ownership of any new IP or retention of exclusive rights may discourage suppliers from providing the Government with their best ideas and solutions if they are unable to gain wider market benefit. This is particularly the case where contracting authorities may sub-license suppliers' innovation to a competitor at a later date. Please see the Guidance Note on Intellectual Property Rights for further guidance and information.

Figure 8: Option for Intellectual Property ownership

Level of public sector investment

<p>Supplier ownership with Crown licence to use</p> 	<p>Options include:</p> <ul style="list-style-type: none"> • A licence for the contracted service only (and its future competition). • A licence for wider access across other HMG services. 	<p>This is likely to be appropriate when</p> <ul style="list-style-type: none"> • There is no clear benefit in the Crown owning the IP. This is because, in the absence of Crown interest in using the outcomes, the supplier is normally best placed to use and exploit the innovation. • New IP created cannot easily be separated from the supplier's existing IP. For instance, where suppliers provide Software as a Service solutions (SaaS). • New IP (principally code) cannot be separated from the supplier's existing IP because it all resides as a single entity on a remote server.
<p>Supplier ownership with profit sharing option for Crown</p> 	<p>Options include:</p> <ul style="list-style-type: none"> • An exclusive licence (or sole licence) (to allow the Supplier only (or the Supplier and the Crown only) to fully exploit the IP). • A non-exclusive licence (to allow Supplier to exploit the IP but retain the right for the Crown to exploit the IP or to authorise others to also exploit the IP). 	<p>This is likely to be appropriate when</p> <ul style="list-style-type: none"> • The contracting authority has invested significant resource or funding in the development of the project and intends to seek a return on that investment. • Where we want to maximise innovation and exploitation potential. • As means of avoiding subsidy control issues by removing the means by which a supplier gains exclusive benefit from that funding.

Crown ownership with supplier licence



Options include:

- An exclusive licence (or sole licence) (to allow the Supplier only (or the Supplier and the Crown only) to fully exploit the IP).
- A non-exclusive licence (to allow Supplier to exploit the IP but retain the right for the Crown to exploit the IP or to authorise others to also exploit the IP).

This is likely to be appropriate when

- The IP produced is likely to be high risk or business critical to the contracting authority its use and deployment should be closely managed.
- The contracting authority wants to retain use of IP for a wider benefit (for instance standardisation leading to enhanced value for money).
- The Crown provides a lot of existing IP – this can create a muddled position if further developments of that IP are owned by the supplier. It is usually better to leave the ownership of all the IP in one place so that it can be exploited or licensed as a whole.
- The IP services more than one contract – for instance if contracting authorities want to use it across other solutions for other contracts which have yet to be awarded.
- The control of certain IP is in the public interest, for example where ownership of detailed drawings could pose a terrorist threat.

Further details on ownership structures can be found in Section 3 of the Intellectual Property Rights Guidance Note.

IP Ownership in Cases Commercial Of-The-Shelf (COTS) Services

In cases of COTS/standard packaged services being provided (e.g. standard OEM software support), the expectation is that the standard OEM licence terms for the product/services will apply.

These cases will likely involve an End User Licence Agreement (EULA)/standard service terms that will, among other things, set out what happens should there be issues with the product/service. Buyers should be familiar with the details of EULA/service terms and understand what they cover before contract award. The EULA/service terms apply directly between OEM and the contracting authority.



Cyber security risk

Cyber security risk management is an ongoing process and vulnerabilities anywhere in the supply chain can be exploited by cyber threat actors. This includes our own vulnerability and contracting authorities will need to have regard to their own risk profile, as well as their suppliers, in order to effectively manage cyber security risk. Applying the principles of the Government Cyber Security Strategy will help public sector organisations stay resilient to cyber threats.

Contracting authorities should complete an assessment to determine the cyber security risks associated with the contract, which can then be used to derive relevant cyber security requirements. The assessment should consider both the risks associated with any data and information (e.g. the contract and related communications) provided to the supplier, as well as the risks associated with the delivered goods or services. There are a variety of approaches to cyber risk management the contracting authority could adopt, but ultimately it needs to align with their organisation's overall approach to cyber risks. Further guidance on approaches to cyber risk management is published by the National Cyber Security Centre (NCSC).

Contracting authorities should consider how cyber resilience will be managed and contractual provisions should require that any minimum standards set as part of the evaluation (see **Chapter 9**) be maintained and any reporting requirements which may be needed. Contracting authorities should also complete a documented risk assessment to identify their cyber security requirements. Further guidance on cyber risk management can be found in the Cyber Essentials Scheme guidance, PPN 09/14, or published by the National Cyber Security Centre (NCSC).

Physical and personnel security

Assessing the risk of a contract should include an appreciation of the physical and personnel security risks associated with the provision of the goods and services required. Contracting authorities should consider the vetting required to fulfil the contract as well as the access rights that suppliers will be given to government estates. In these cases, the mobilisation period for hiring and vetting resources must be realistic to enable new skills, ideas and experience into the security cleared environment. The security clauses in the contract should accurately reflect the risk associated with the supply of those services or goods.

Where contracting authorities are responsible for Critical National Infrastructure (CNI) assets, consideration should be given to how the contract safeguards these assets. This may require advice from departmental security teams or the National Technical Authorities (CPNI and NCSC).



Open and interoperable data and software⁸

Open standards have long been a priority for government; however, the COVID-19 crisis has demonstrated the criticality of enabling data sharing across suppliers and government. There is also an important consideration in how open standards relate to IP and contracting authorities should take into account that IP will need to be owned by the Crown (or licensed under an appropriate model) if it is intended to be published by Government as open-source material. The National Data Strategy sets out the government ambition to transform government's use of data to drive efficiency and improve public services.

Open software

There is an expectation that government software and code is open-source by default. This means it should be developed in the open and published using an Open Source Initiative (OSI) approved licence. Open and interoperable software will enable:

- transparent and clear documentation, making it easier for teams to maintain the code, understand the data, track changes to the code and data and for other people to use the Application and data
- reuse of software components built by others

- reduction of overall cost of digital services or technology programmes

Open data

Open data is information which is available to the public. This supports the government's transparency agenda and where possible, contracting authorities should ensure data is provided in open, machine-readable formats while maintaining compliance with data privacy laws.

Data held by the government can often concern the most sensitive areas of citizens' lives, and therefore may be unsuitable for open access. In these cases, contracting authorities should consider whether it may be appropriate to be open about the categories of data which are held.

Data interoperability

Government's information assets, including data, should be able to be easily exchanged across platforms to make efficient use of the data we own. Contracting authorities should ensure that all contracts, including for commercial off-the-shelf (COTS) software, enable data extraction in a common format and IP and licencing requirements should be considered to ensure accessibility and transparency.



API technical and data standards

All contracts should ensure that both performance and operational data is made available via APIs which meet Central Digital and Data Office (CDDO) API technical and data standards.

⁸ Legacy IT Guidance Note: Guideline 10

Organisations and services will have specific technical needs around the data that needs to be shared, and their institutional approaches to these should be standardised as specific design guidelines for APIs - which are then applied alongside CDDO guidance during development to ensure consistent API production. This means that external users will be able to rely on a standard interface to data across the organisation, to save time and enable reuse of methods. APIs should also be managed over their life cycles according to the CDDO guidelines, to ensure adherence to security and usage best practices. Access to data via API should be strictly controlled to ensure both transport and access is managed and audited.

Interoperable data is also important for a healthy and competitive market. Data which is not interoperable can give incumbent suppliers a competitive advantage when re-procuring and may result in vendor-lock into a specific piece of technology, or supplier software. By allowing equal access to government IT contracts for open source and proprietary software providers, we will create a level playing field, drive competition and incentivise suppliers to co-operate and innovate.

Repair and reuse

The UK generates around 1.5 million tonnes of electrical waste every year and the impact on our environment both in the production and disposal of these products is manifold. The Ecodesign and Energy Labelling Regulations 2021 enshrine a new legal right to repair for consumers and set higher energy-efficiency standards for electrical products.

Extending the life of hardware across government, where appropriate, could have significant value for money and environmental benefits. Where possible, contracting authorities should ensure the hardware is designed for long-term resilience, and the ability to repair and/or reuse components should be incorporated into new contracts. The ability to undertake repair should also be considered as part of any testing and learning process.



Contractual terms and conditions for cloud

Contracting for cloud and SaaS can differ from how we contract for other products and services due to the one-to-many data model. There are a number of considerations often included in supplier terms and conditions for cloud contracts which contracting authorities will need to consider:

- **Cloud and cyber security:** Cloud service providers often require customers to contractually recognise their particular 'shared responsibility models' which set out predefined responsibilities around managing cyber security risk for both the customer and supplier.
- **Data protection:** Due to the multinational nature of supply chains, data may, in some instances, temporarily cross international borders. This will not constitute a breach of data protection requirements where data is only "in transit" (e.g. data is being transmitted over the Internet and certain packets transit through a network in a particular jurisdiction). The transfer of data to another jurisdiction will, however, always constitute a restricted transfer.

- GDPR: EU Standard Contractual Clauses (SCCs) are often incorporated into suppliers' proprietary 'data processing agreements' by default to ensure the contract covers all eventualities. Post EU Exit, contracting authorities should use the approved UK SCCs. These are currently the same as the old EU SCCs but remember to check current requirements on this as the ICO is consulting on a refresh of UK SCCs.
- Cloud Subprocessors: Cloud service providers often require customers to provide an upfront "general written authorisation" for them to use new subprocessors, or third-party affiliates to undertake certain tasks. This should operate on a "notice and veto" basis. Existing subprocessors are more typically agreed expressly by consent.
- URL terms and conditions: Cloud and SaaS providers almost universally ask customers to include reference to service specific terms and conditions by way of URLs to their websites.
- As detailed in PPN 05/16 open book contract management should be used.

For all of these factors, it is essential that the effect of critical government terms and conditions is maintained and contracting authorities should have a strategy in place for how supplier terms and conditions and any variations are managed. This should include transparency and financial monitoring requirements of the main supplier and critical subcontractors.

Issue logs should be kept of any unacceptable terms and conditions and/or variances, and legal advice sought as appropriate. Guidance will be developed by Cabinet Office and Crown Commercial Service to support contracting authorities to manage these considerations.

Memorandums of Understanding (MoUs)

Being able to approach cloud providers as a single government customer is an important goal of the One Government Cloud Strategy. If one organisation has successfully negotiated a contract with a cloud service provider, the aim is that every organisation should be able to benefit from that effort.

MoUs look to enable a common cloud procurement process with multiple suppliers, leveraging the combined purchasing power of the government to achieve better commercial results. This can include agreeing greater discounts for smaller departments and reducing negotiation time for government and providers. This enables a baseline of commercial, technical, security and legal principles across government with each cloud service provider.

Standardised contracts and terms

Standardised Government contracts or standardised Government contract terms, including various CCS frameworks (see **Chapter 7**), can be used to help simplify and speed up procurement procedures, especially for common goods and services. By applying a common approach across the public sector, best practice is more easily embedded and suppliers are more likely to experience a consistent application of policies and practice.

Contracting authorities should avoid amending standard clauses where possible and select the appropriate provisions to reflect the specific services being procured. Where standard contract terms are amended, contracting authorities should seek assistance from the Government Legal Department (GLD) or in-house legal teams, to ensure that any risks are assessed and recorded.

The Model Services Contract (MSC)

The MSC comprises a set of model terms and conditions for major services contracts. It is intended for use by commercial specialists and lawyers to aid assurance and reduce administration, legal costs and negotiation time. Where the MSC is not appropriate, contracting authorities should consider including provisions which support the policies set out in this Playbook.

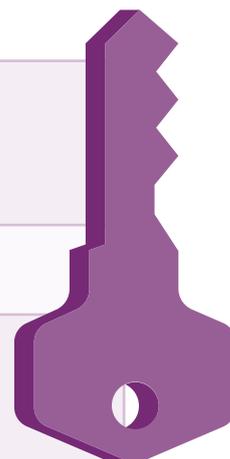
The Public Sector Contract (PSC)

When setting up new frameworks, contracting authorities should use the PSC for common goods and services. This should include:

- the standard core terms (used in every procurement)
- relevant best practice and optional schedules
- adjusted PSC terms for specific markets (SaaS, hosting)

Key points

1. Risks should be allocated to, and managed by, those best able to bear and manage them (this includes the contracting authority). Contractual allocation should reflect the extent to which parties are responsible for risks and their management.
2. When a contract is publicly designated as onerous, this should prompt a root cause analysis and conversation with the supplier.
3. Contracts should be designed to be profitable and offer a fair return for the market to be sustainable. It is good practice to test profitability under different circumstances and make use of the Should Cost Model in developing payment mechanisms.
4. Always factor in digital, data and technology specific considerations when designing contracts, including preventing the build-up of legacy IT, and ensuring that Intellectual Property is owned by the party best able to utilise it and that government software and code is open-source.
5. Use appropriate contractual terms and conditions, including considering supplier specific terms when contracting for cloud and/or for services, including terms which permit redeployment of supplier staff without restrictions after the contract has ended, and making use of standardised contract terms for commercial goods and services.



Want to know more?

1. Guidance on use of open standards.
2. The technology code of practice.
3. Make better use of data.
4. Service Manual – Make new source code open.
5. Describing RESTful APIs with OpenAPI 3.
6. When code should be opened or closed.
7. Be open and use open source.
8. Choosing technology: An introduction.
9. PPN 09/14 – Cyber Essentials Scheme.
10. Cyber security – Risk management guidance.
11. IaaS – Managing your responsibilities.
12. DDaT Service Standard 9 – Protect users' privacy.
13. The Minimum Cyber Security Standard.
14. Cloud specific:
 - CDDO – How to assess a hosting business case (associated with Spend Controls).
 - CDDO – Public Cloud First Policy.
 - CDDO – Cloud guide for the public sector / One Government Cloud Strategy.
 - CCS – provide a wide range of customer guidance. Please see Cloud Compute and G-Cloud 13 in particular.
 - NCSC – 'Cloud Security Principles' and 'IaaS – Managing your responsibilities'.
 - Transfer does not mean the same as transit.



Preparation and planning

Publication

Selection, evaluation and award

Contract implementation

Contract end



9 Developing evaluation criteria

We will drive wider value through our projects and programmes and this starts with how we evaluate our suppliers.

Ethos for evaluation

Cost and quality

Evaluation – and evaluation criteria – should focus on value over cost in order to avoid a ‘race to the bottom’. All of our contracts should seek to achieve the best value for money possible and this is defined as securing the best mix of quality and effectiveness for the least outlay over the life of a project or programme. It is not about minimising initial costs.

When considering ‘outlay’ the key factor is the whole-life cost, not the lowest purchase price. Whole-life cost takes into account the total cost over the life of an asset, including capital, maintenance, management, operation and exit, and can be very different from the initial price.

Affordability will always be a key factor and contracting authorities should determine whether increased benefits justify higher costs to ensure whole-life value for money. The expectation is that quality will be weighted higher than cost, recognising the importance of delivering quality public services and paying more for higher quality may be justified if the whole-life value is advantageous.

Robust evaluation processes

Bid evaluation is not only about the decision to award the contract, it is about the design and execution of the whole process, leading up to that decision, ensuring the process is properly documented, and can stand up to internal and external scrutiny.

Contracting authorities should ensure they are making full use of the most advantageous tender (MAT) methodology to evaluate value and test evaluation criteria and weightings prior to procurement to ensure they produce the desired outcomes. For example, applying minimum quality criteria inappropriately can lead to the competition unintentionally being based on price.

Evidence suggests that, although Complex Outsourcing projects can be inherently difficult to cost, on occasions there has been a bias towards low cost bids rather than the best value for money in terms of cost and quality. One of the reasons for this could be the use of relative evaluation models where the bidders’ scores for pricing are ‘pinned’ against the lowest price bid. This type of scoring can have many unintended consequences and should not be used unless there is a specific business reason. More information can be found in Section 7 of the Bid Evaluation Guidance Note.

“ It is in everyone’s interest for projects and programmes to be sufficiently prepared ahead of going out to tender”

In developing the evaluation model, contracting authorities should draw on a number of criteria including the outcomes set out in the Project/Programme Outcome Profile and wider factors including social value and sustainability as part of the ‘quality’ criteria. Evaluation of bids should also take into account whether the proposal includes the time and cost needed to address the risk of the future accumulation of legacy IT.

Once completed, bid differentials in evaluation which affect scoring and choice of supplier should be captured in the contract and KPIs and suppliers should be assessed on their delivery against these as appropriate.

Procurement Reform

The Bill set out that contracting authorities should assess bids to determine the Most Advantageous Tender (MAT). In practice, there is no change from the current regime, but the removal of the word ‘economic’ emphasises that contracting authorities should be seeking value and not the lowest price. This is particularly relevant where relative scoring mechanism have been used (see above).

Testing evaluation criteria

Contracting authorities should test their evaluation models before publishing them, running different potential bid scenarios to test the outcome. Similarly, Should Cost Modelling will inform the value placed on quality criteria and different levels of cost versus quality, and should be tested to determine the appropriate thresholds of delivery. Contracting authorities should also seek to identify and test potential change scenarios and use this to inform evaluation criteria.



Delivering sustainability

Sustainability goes beyond just the environment to also encompass the economic and social conditions which affect the ability of current and future generations to create healthy and liveable communities. This means evaluating not just short-term outlay, but long-term value to ensure the sustainability and resilience of our digital and data contracts, products, services, supply chains and citizens.

This is known as value-based procurement and is distinct from Social Value as it goes beyond what we ask of our supply chains to encompass our end-to-end approach to procurement. Value-based procurement should be adopted at an organisational level and driven through projects and programmes to drive sustainability.

This will require a consistent approach running through policy intent, project selection, approval, initiation and into procurement, evaluation criteria, contracts, delivery and operations. Project/Programme Outcome Profiles will help projects to do this by providing a tool to capture clear outcomes at the outset, aligned to government's strategic priorities, that can be referred to throughout the project lifecycle.

When considering how sustainable practices can be integrated into the procurement, close attention should be paid to point 12 of the Technology Code of Practice - Make your technology sustainable. This provides step-by-step instructions of how to increase sustainability throughout the lifecycle of your contracted DDaT product or service.

Setting the tone

Projects and programmes should be run in accordance with the Supplier Code of Conduct. This recognises the joint nature of public sector products and services and sets out how we achieve constructive and collaborative engagement with suppliers. The supplier code of conduct applies across our engagement with the market (see **Chapter 1**) and the Contract Notice and tender documentation should carry a statement to indicate that the procurement will be run in the spirit of the Supplier Code of Conduct.

It is in everyone's interest for projects and programmes to be sufficiently prepared ahead of going out to tender. Before we do, it is good practice to put in place a final sense check to ask: Is this project or programme set up for success?

Procurement timelines and transparency

Suppliers need sufficient time and visibility of tender documentation to develop and price solutions, raise clarifications and get clear and timely answers and respond with high quality responses to tender documentation. Experience tells us that inadequate timescales and lack of transparency can result in a lack of due diligence, rushed solutions, poor quality tenders and may lead to a number of problems downstream in implementation.

Early engagement with the market will help to inform how much time is necessary or appropriate for a specific procurement and this should be reflected in the procurement and project timelines (see **Chapter 1**).

Procurement Reform

Transparency is a stated objective of the new regime and it is embedded by default throughout the Bill. With the new rules, the Government is committed to increasing transparency within public procurement, for suppliers, buyers and the general public alike. This is intended to improve competition, widen the supplier base and to hold contracting authorities and suppliers to account for their actions and performance. As a result, you will notice many changes to the required notices (and their names) as follows. Further detail on what information each notice must contain will be included within the detailed secondary legislation which is yet to be published:

Pipeline Notice - a contracting authority anticipating spending over £100 million in the following financial year is statutorily obliged to publish a notice setting out all of its planned contracts over £2 million within the next 18 months. This must be published within 56 days of the start of the financial year.

Planned Procurement Notice - this provides suppliers with advance notice that a contracting authority intends to run a competition and, like the current PIN, allows timescales to be reduced.

PME Notice - the preliminary market engagement notice is to be published before the Tender Notice and used by contracting authorities to provide information on upcoming or past preliminary market engagement.

Tender Notice - this notice invites suppliers to either submit a tender or a request to participate in a competitive procurement process.

Transparency Notice - a new notice requiring contracting authorities to inform the market and the public of their intention to direct award a contract (this isn't applicable for user choice contracts).

Assessment Summary - this is provided to bidders at the end of a competitive process and will contain information about the winning bid and the assessment of the bid of the supplier who is receiving the summary. This will help suppliers improve their bids in future and increase the quality of the market

Award Notice - the Award Notice is notification that a contract is about to be entered into. It is required for competitive and non-competitive contracts and will usually mark the start of an 8 working day standstill period before which the contract can not be entered into.

Contract Change Notice - a new notice which is to be published advertising the

contracting authority's intention to modify an existing contract.

Contract Details Notice - to be published within 30 days of the contract being entered into.

Mandatory exclusion criteria

Supplier selection is a key stage in public procurement and we must ensure that we are meeting the high standards expected of the UK government. It is mandated that potential suppliers self-assess against Part 2 of the Supplier Selection Questionnaire which asks them justify their status against the exclusion grounds and selection questions. Further guidance on these exclusion criteria can be found below.

Prompt payment processes

The government understands the importance of prompt, fair and effective payment in all businesses. Being paid promptly for work carried out in accordance with the contract, current policy and legislative requirements ensures businesses have a healthy cash flow throughout the supply chain, especially at the lower tiers where delivery occurs.

The principle of paying promptly applies to all public procurement and contracting authorities who also have obligations to demonstrate that terms to pay within 30 days are cascaded throughout the supply chain (in accordance with the Public Contracts Regulations 2015, Regulation 113).

For contracts valued above £5 million per annum, contracting authorities should include an assessment of a supplier's payment systems to demonstrate it has a reliable supply chain as part of the selection process and determine when it would be appropriate to exclude those suppliers that cannot demonstrate this. Further guidance can be found in PPN 07/20.

All public sector suppliers must pay their supply chain promptly and suppliers who use their status as signatories to the Prompt Payment Code (PPC) are expected to be able to demonstrate compliance with the latest PPC requirements.

Procurement Reform

The Bill establishes prompt payment provisions as implied terms in all public contracts, excluding private utility and concession contracts, and those awarded by a school.

Net zero

Government is committed to bringing all greenhouse gas (GHG) emissions to net zero by 2050. Contracting authorities should ensure all new products and services support their GHG Government commitments and take account of suppliers' Net Zero Carbon Reduction Plans as set out in PPN 06/21.

This introduces new criteria at the selection stage of the procurement, and requires bidding suppliers to detail their commitment to achieving net zero through the publication of a Carbon Reduction Plan. Further guidance on selection questions and how to apply them and assess supplier responses can be found in the guidance on adopting and applying the Carbon Exclusion Measure in the procurement of major contracts.

Modern slavery

Where we are procuring products and services, particularly from high-risk sectors including DDaT, we need to take all the necessary steps to mitigate the risks of Modern Slavery within our supply chains in line with the Modern Slavery Act 2015.

A risk-based approach should be applied to combatting modern slavery starting in the planning and preparation stage of procurements. Contracting authorities should ensure their approach to modern slavery is proportionate and does not impose any unnecessary burdens. This means a blanket approach is unlikely to be appropriate and consideration will need to be given to the circumstances of each contract and whether any of the mandatory or discretionary exclusion grounds apply.

This should be regularly monitored throughout the commercial lifecycle to manage and mitigate against any modern slavery risks. Further information can be found in PPN 05/19 and the associated Tackling Modern Slavery in Government Supply Chains guidance.

The Modern Slavery Assessment Tool

(MSAT) is a modern slavery risk identification and management tool. This tool has been designed to help public sector organisations work in partnership with suppliers to improve protections and reduce the risk of exploitation of workers in their supply chains. It also aims to help public sector organisations understand where there may be risks of modern slavery in the supply chains of goods and services they have procured. Public sector organisations are encouraged to use the MSAT with existing suppliers.

Applying minimum standards



Cyber security

Our digital and data products and services must be resilient against cyber security threats and proportionate assessment will better safeguard public data.



The Cyber Essentials Scheme, set out in PPN 09/14, creates a framework which provides organisations with basic protection from the most prevalent forms of cyber-security threat and is mandatory for all new central government contracts which involve handling personal information and providing certain ICT products and services.

Cyber Essentials should be applied as a minimum standard of cyber-security risk evaluation and management. A documented risk assessment should take place to consider whether it may be appropriate to apply more developed standards of cyber security such as Cyber Essentials Plus, ISO 27005 risk assessment software or NIST and whether cyber-security specific terms and conditions need to be flowed-down the supply chain.

The controls outlined in Cyber Essentials should be seen as a minimum set and evidenced where appropriate through the production of a Cyber Essentials or Cyber Essentials Plus certificate. A documented risk assessment should take place to consider whether additional controls (such as those found in ISO27000 or the NIST framework) and ways of evidencing are required. This will also indicate whether cyber security-specific terms and conditions need to be flowed down the supply chain.

Evaluating social value

Taking account of social value in the award of contracts can achieve significant benefits for our communities. This can range from delivering skilled jobs across the country to level-up the economy, enabling start-ups, SMEs and VCSEs to lead or be part of government supply chains to ensuring those in disadvantaged groups have equal opportunity to become part of a diverse and resilient workforce.

Social value outcomes should be applied consistently to make it easier to clearly and systematically understand and evaluate the social value in the award of a contract. Central government, executive agencies and non-departmental bodies should use the Social Value Model to achieve this. Under the model, a minimum overall weighting for social value of 10% of the overall score should be adopted whenever any of the social value policy outcomes are included in a procurement.

Further information on how to evaluate social value can be found in PPN 06/20.

Procurement Reform

The Procurement Bill requires that all contracting authorities have due regard to a set of national strategic priorities set out in a published National Procurement Policy Statement. The first version was published in PPN 05/21 and set out national priority actions for Social Value. It places emphasis on creating new businesses, new jobs and new skills; tackling climate change and reducing waste, and improving supplier diversity, innovation and resilience, all themes within the social value model.

Tailored evaluation

Accessibility

The accessibility of public products and services is a legal requirement under the Equality Act 2010 and is essential to better user experiences and outcomes. As part of any evaluation criteria, contracting authorities should ensure compliance with the Public Sector Bodies Accessibility Regulations and Web Content Accessibility Guidelines (WCAG) for all digital, data and technology products and services.

Legacy IT

In order to be able to future-proof our DDaT products and services, contracting authorities should ensure that suppliers are capable of keeping products and services kept up-to-date and in mainstream support for the duration of the contract and any extension. Contracting authorities should use pre-market engagement to inform any minimum thresholds of support set as part of the evaluation criteria. This need not be the 'latest' version of any product or service as default, and contracting authorities should work with the market to find balance between the need for support against value for money.

Software licence terms

When procuring commercial off-the-shelf (COTS) software, parameters should be set to enable an effective evaluation of the licensing terms and conditions attached to various products, including the frequency of update and any relevant support offer. This will enable the evaluation process to ensure that terms and conditions are acceptable to the contracting authority and meet the requirements specified.

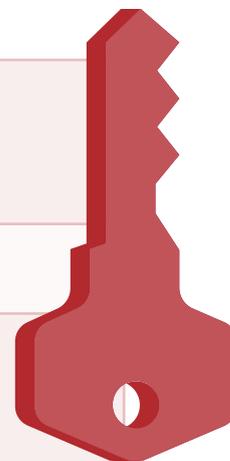
Sustainable working practices

Government contracts with thousands of suppliers for DDaT products and services, and by considering the sustainability of suppliers' organisational practices, we will work towards better outcomes for citizens and support the long-term health of the industry.

In addition to prompt payment information, contracting authorities should consider whether there are wider considerations which may be relevant and proportional to the size and complexity of the contract. Metrics such as gender pay gap and staff retention data may be helpful to consider as part of the tender process and contracting authorities should ask potential suppliers to explain any poor results and consider whether it may be appropriate to put in place contractual measures to remediate these.

Key points

1. Sustainability includes environmental, economic and social sustainability and evaluating not just short-term outlay, but long-term value will ensure the sustainability, resilience and the best possible outcomes for our digital and data products and services, our supply chains and our citizens.
2. Value-based procurement should be adopted at an organisational level and driven through a portfolio approach to projects and programmes.
3. Evaluation should focus on whole-life value rather than simply cost, making use of the social value framework and Project/Programme Outcome Profile to design fair, open and sustainable evaluation criteria. Relative price scoring should be treated with caution and not be used unless there is a specific business reason which has been approved by the Commercial Lead and the project SRO.



Want to know more?

1. **The Green Book**: appraisal and evaluation in central government.
2. **Bid Evaluation Guidance Note**.
3. **PPN 06/20: Taking Account of Social Value in the Award of Central Government Contracts**.
4. **Supplier Code of Conduct**.
5. **Accessibility requirements for public sector bodies**.
6. **Web Content Accessibility Guidelines**.
7. **PPN 06/21: Taking account of Carbon Reduction Plans in the procurement of major government contracts**.
8. **Modern Slavery Guidance**.
9. **PPN 05/19- Tackling Modern Slavery in Government Supply Chains**.
10. **Social Value Act: information and resources**.
11. **The Technology Code of Practice - Make your technology sustainable**.

Preparation and planning

Publication

Selection, evaluation and award

Contract implementation

Contract end



10 Due diligence and contract award

We have a responsibility to assure ourselves of the solvency and competency of suppliers that bid for our contracts. A relevant and proportional selection process is critical to enabling this.

The selection process

The selection process is used, amongst other things, to determine whether bidders are able to demonstrate suitability and meet our requirements to carry out the contract. The standard Selection Questionnaire (SQ) should be used and some standard information may be obtainable via the Supplier Registration Service.

Part 2 of the SQ comprises a self-declaration regarding whether or not any of the Exclusion Grounds set out in the relevant regulations apply.

Part 3 of the SQ relates to financial standing and technical capacity. This will need to be adjusted in line with requirements under the economic and financial assessment of suppliers (EFS). An updated version of the SQ is expected to be launched in 2021 which will align with the standard EFS metrics.

In addition to the SQ, contracting authorities should consider the economic and financial standing of suppliers during the pre-qualification stage as set out below.



Assessing the economic and financial standing of suppliers

What is economic and financial standing (EFS)?

As part of the selection process, DDaT projects should comply with a consistent approach to assessing the risk of a supplier going out of business during the life of a contract. To safeguard the delivery of public sector products and services, it is critical that suppliers' economic and financial standing is considered during the selection process.

As well as informing the selection itself, financial assessments and ongoing monitoring should inform risk-management activity during the life of the project. The key principles of appropriate financial testing are:

- The objective is to determine bidders' financial capacity to perform the specific contract.
- Economic and financial standing forms one part of the overall judgement of suitability during selection.
- The methodology of assessing the ratios and the minimum requirements for procurements should be transparent, objective and non-discriminatory.

“ Investing time into good feedback can be extremely useful to unsuccessful bidders by helping them to understand what they did well, what they could have done better, and points to consider in the future ”

- All bidders, whatever their size or constitution, should be treated fairly and not inadvertently disadvantaged by the tests employed.
- Where bidders' scores against the financial assessment metrics result in anything other than a 'low risk' classification, bidders should be given the opportunity to provide additional acceptable evidence and explain why different risk classifications may be more appropriate.
- Bidders with scores other than 'low risk' may be able to proceed subject to acceptable risk mitigations
- Consistently applying a minimum standard of testing will provide a better understanding of financial risk and leave us better able to safeguard the delivery of DDaT products and services.

How is EFS conducted?

The key to undertaking EFS is that these are tailored to individual projects, and are proportionate, fair and transparent and that financial metrics are used as an indicator of financial health and not as a pass/fail exercise. This will enable contracting authorities to effectively think about the risks to project or programme delivery and any mitigations needed. Guidance on how to do this is included in the Assessing and Monitoring

the Economic and Financial Standing of Suppliers Guidance Note.

The Contract Tiering Tool should be used to determine the stringency to which bidders are tested, with higher thresholds for more critical contracts and framework agreements. Assessment should be proportionate to the size, risk and complexity of the contract, flexible, not overly risk averse, and clearly outlined in the SQ.

It is important to recognise that measures for evaluating economic and financial standing are often backward-looking and that SMEs and other growing entities may often publish limited public accounts or limited financial history. Contracting authorities should ensure that they develop robust market health assessments (see **Chapter 1**), have suitable systems in place for ongoing financial monitoring (see **Chapter 11**) reflecting supplier and sector specific financial risks.

The DDaT context for EFS

It is critical to recognise that the digital market is a dynamic sector with diverse types and sizes of suppliers coupled with a high level of mergers and acquisitions which may change the nature of financial risks quickly.

This is why even on low and medium-risk (bronze and silver) procurements and framework agreements, contracting authorities should still apply proportional financial tests and rely on minimum standard contractual clauses enabling access to financial information of suppliers and the wider group, including ultimate parents, when it may be needed to better understand financial risks in order to protect government systems and data (see **Chapter 11**).

For multi-supplier frameworks agreements, including those for non-critical contracts, there should be minimum but proportional financial tests at call-off stage and warranties from the supplier to the contracting authorities to ensure that the latest financial performance is reflected prior to contract signature.

Procurement Reform

The introduction of a single supplier platform in which suppliers will input standard financial and descriptive information that will be stored on the system and pulled through into multiple procurements will make it easier for contracting authorities to undertake economic and financial standing assessments and for this information to be validated if required before contract award. There are also changes proposed to the rules on excluding suppliers (both mandatory and discretionary) which may change what needs to be taken into account from a qualitative perspective at this point in the procurement process.

Keeping records and providing feedback

Evaluators should keep detailed records of their evaluation of bids, setting out the scores awarded and the rationale for the score. On completion, a robust evaluation report should be produced. This should

demonstrate that the evaluation has been completed in accordance with the stated evaluation model, showing the evidence supporting the scores allocated, providing a clear interrogation of the all costs and demonstrating that the bid is financially sustainable over the life of the contract.

At the end of the evaluation process providing feedback to unsuccessful bidders is required by Regulation 86 of the Public Contracts Regulations 2015. Investing time into good feedback can be extremely useful to unsuccessful bidders by helping them to understand what they did well, what they could have done better, and points to consider in the future. This will support the long-term development of diverse, healthy markets.

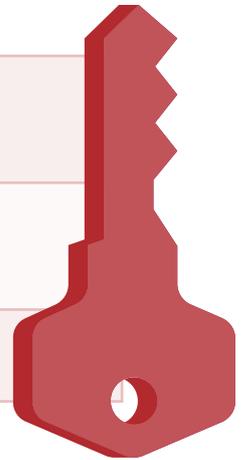
On award, contracting authorities should publish details of the contract on Contracts Finder in line with publishing advice from the Commercial Policy team. Departments should take particular care not to publish unredacted versions of contracts that include information marked as commercially sensitive or confidential.

Low-cost bid referrals

Even when evaluation criteria are designed to balance quality and cost, there is an ongoing risk of low-cost bias. Departments should refer any abnormally low bid that is more than 10% lower than the average of all bids or the Should Cost Model to the Continuous Commercial Improvement Team in the Cabinet Office prior to accepting it. This is to be done in accordance with Regulation 69 of the Public Contracts Regulations 2015.

Key points

1. The selection process is used, amongst other things, to determine whether bidders are able to comply with exclusion grounds and demonstrate suitability to carry out the contract.
2. The payment mechanism and pricing approach including limits of liability should reflect the level of risk and uncertainty in the scope of requirement and will be subject to greater scrutiny.
3. The selection stage is an assessment of the bidders themselves, whereas the evaluation and award stage is an assessment of their bids.



Want to know more?

1. Standard Selection Questionnaire (SQ) [PPN 8/16](#).
2. [Supplier Registration Service for Government](#).
3. [Assessing and Monitoring the Economic and Financial Standing of Suppliers Guidance Note](#). Support is available from the Cabinet Office via supplierfinanalysis@cabinetoffice.gov.uk.
4. [Financial Viability Risk Assessment Tool](#).
5. [Guidance on Corporate Financial Distress](#).



11 Resolution planning

Although major disasters are infrequent, we need to be prepared for the risk to continuity of critical projects and programmes posed by factors ranging from natural disaster to cyber-attack and the insolvency of key suppliers.

Resiliency through early planning

Government is the custodian of critical digital, data and technology products and services which our citizens rely on every day. This means that disasters in our supply chains, ranging from the loss of critical systems due to natural disaster to falling victim to cyber-attack, can potentially have catastrophic consequences on the delivery of critical public sector services and result in the loss of public trust.

As such, we must also plan for instances when things do go wrong. Suppliers of the most important public sector DDaT products and services should have resolution plans in place to ensure the continuity of critical public infrastructure. This will inform our own contingency planning.

Suppliers and contracting authorities should take a collaborative approach to the development of resolution plans to understand risks, vulnerabilities and potential disruptors and their impacts and develop strategies for recovery and remediation. This should be proportional to the size, complexity, criticality and inherent vulnerability of the contract and should include cyber incident response plans and corporate resolution plans.



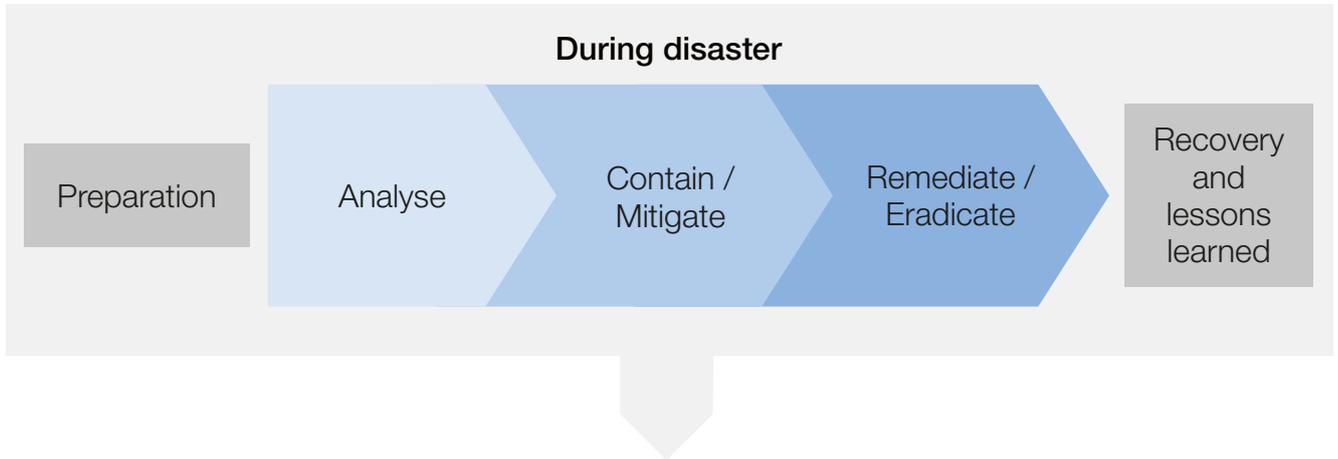
Cyber incident response plan

An initial stage of an effective resolution plan is a robust cyber Incident Response (IR) plan. An IR plan is written with distinct phases (see Figure 9) that helps suppliers and contracting authorities recognise and deal with a cyber-security incident like a data breach or cyber-attack.

Properly creating and managing an incident response plan involves regular updates and training to ensure it is well-documented and understood. The plan and processes should be tested on a regular basis so that the supplier is ready to respond when a cyber-incident or crisis occurs, in order to limit any data loss and then quickly recover.

The cyber incident response plan should be linked to disaster recovery, business continuity and crisis management plans, and supported with the relevant capabilities. If the incident is severe and poses a risk to business operations, customers or supply chain, the supplier should inform the relevant contracting authority. From there the contracting authority is encouraged to contact the NCSC, who can also provide further guidance on incident response planning, and where personal data is at risk, the Information Commissioner's Organisation (ICO).

Figure 9: Cyber Incident Response Plan



Increasing complexity of Disaster Recovery

Low	Medium	High	Critical
<p>Minimal, if any, impact</p> <p>One or two non-sensitive / non-critical machines affected</p> <p><10% of non critical staff affected temporarily (short term)</p>	<p>20% of staff unable to work</p> <p>Possible breach of small amounts of non-sensitive data</p> <p>Low risk to reputation</p> <p>Small number of non-critical systems affected with known resolutions</p>	<p>50% of staff unable to work</p> <p>Risk of breach of personal or sensitive data</p> <p>Non critical systems affected, or critical systems affected with known (quick) resolution</p> <p>Potential for significant financial impact and cost of recovery</p> <p>Potential serious reputational damage</p>	<p>Over 80% of staff (or several critical staff/teams) unable to work</p> <p>Critical systems offline with no known resolution</p> <p>High risk to / definite breach of sensitive client or personal data</p> <p>Significant financial impact and cost of recovery</p> <p>Severe reputational damage - likely to impact business long term</p>

Corporate resolution planning

There is a requirement for suppliers of critical DDaT contracts to provide resolution planning information where appropriate. The contract tiering tool should be used to understand a contracts criticality in the first instance. This requirement should be considered early in the procurement process during the development of contractual documentation. Although major insolvencies are infrequent, this change will help to ensure the government is prepared for the risks to the continuity of critical public DDaT projects posed by the insolvency of critical suppliers. To discuss the inclusion of this clause and the assessment of contract criticality, please contact the Cabinet Office Markets and Suppliers Team.

Potential options to mitigate commercial risk

There are a number of potential contractual options available to contracting authorities where there are concerns about the stability of a supplier, to help mitigate the impact of insolvency.

Treatments should be proportionate to the risk identified and the criticality of the contract, considering the impact on the overall value for money of a contract. Key options include:

- Bonds – typically provided by independent third parties and provide financial payments in the event of supplier failure. Bonds should be used proportionately as they can be burdensome requirements for lower value contracts and add significant costs that are likely to be reflected in bids. Professional advice should be sought when considering the use of bonds.

- Guarantees – under a guarantee, another party (such as a parent company) undertakes to fulfil the terms of the contract (a performance guarantee) and/or provide financial payments to the contracting authority (a financial guarantee) if the supplier does not honour the contract.

Further guidance on how to do this is included in the Assessing and Monitoring the Economic and Financial Standing of Suppliers Guidance Note and the Resolution Planning Guidance Note.

Contractual documentation

The provision of corporate resolution planning information must be a contractual requirement on critical DDaT projects and this requirement should flow down into the supplier chain. Consideration to this requirement must be given early on in the project as it will have an impact on the route to market and the contract documentation.

Contracting authorities may also wish to include the requirement to provide CRP information for contracts where there is the possibility that the successful supplier will be a Public Sector Dependent Supplier. Contracting authorities must have regards to suppliers for whom particular contracts are a disproportionately high percentage of their business and this risk may require additional mitigation strategies to be in place.

Ongoing financial monitoring

Although the financial standing of suppliers should be assessed during procurement, this can subsequently change or deteriorate, either suddenly or over time, particularly in a dynamic market, such as the DDaT sector marked with regular mergers and acquisitions. Early recognition of the risk of supplier financial failure gives us more time to prepare for failure 'should it occur' and mitigate the risk to continuity of critical projects, including in situations of change of ownership where the new parent may not be of the same financial standing or have different business strategies.

We should, therefore, monitor the financial standing of our key suppliers on an ongoing basis as a routine part of risk monitoring and reporting. This should include contractual financial reporting where this was agreed as a mitigation based on the financial assessment at the selection stage.

Considering the dynamic nature of the digital sector, contracting authorities should apply minimum standard contractual clauses enabling access to financial information of suppliers, guarantors and ultimate parents, when it is needed to better understand financial risks in order to protect government systems and data, including on low and medium-risk (bronze and silver) contracts and framework agreements.

Monitoring should normally be performed in the first instance by a function or team that is independent of the day-to-day contract management role. Its frequency should reflect the criticality of the contract, as well as the perceived risk of failure but it should be carried out at least annually, linked to full-year financial results.

More regular reviews (e.g. every six months or less) are recommended for public sector dependent suppliers and suppliers that contracting authorities assess as critical for their services.

Ongoing 'alert' systems should be established to monitor company announcements and other information sources, capturing wider economic and sector trends that may have impacted suppliers. The outcome of financial monitoring should be discussed with contract managers and, where appropriate, reassurance and additional information should be sought from the supplier.

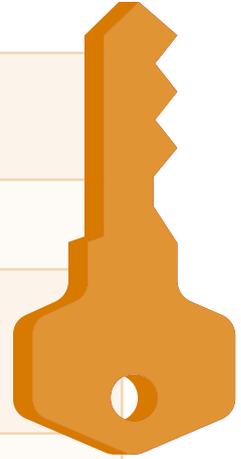
Where monitoring and follow-up suggest a raised level of concern, contract managers should ensure their contingency plans are up-to-date and consider what further action or monitoring is required. Further guidance is included in the Assessing and Monitoring the Economic and Financial Standing of Suppliers Guidance Note.

Terminating contracts with public sector dependent suppliers

Contracting authorities must have regard to contracts which form a large or vital proportion of a supplier's business and consider early the impact termination of a contract may have on that supplier's financial health.

This will enable appropriate remediation to be put in place for the health of the market, supplier and contracting authority. The Cabinet Office Markets and Suppliers team should be notified whenever departments are planning to terminate a DDaT contract with a public sector dependent supplier.

Key points



1. Resolution planning helps to support continuity of critical projects and contain disruption in the event of supplier insolvency. Resolution planning can be at corporate level and/or at service level.
2. Contracting authorities should ensure that they produce contingency plans for critical contracts.
3. When reviewing suppliers' Service Continuity plans for critical contracts, ensure they include a supplier insolvency continuity element. Make sure exit plans and exit information cover emergency exit arising from supplier insolvency.
4. Ongoing financial monitoring enables early identification of possible problems and the opportunity to test contingency plans before they are needed.
5. When considering the mitigation of risk against potential supplier insolvency it is important to consider proportionality and the wider impact on suppliers and competitiveness.

Want to know more?

1. **Cyber incident management.**
2. **Resolution Planning Guidance Note.** Support is available from the Cabinet Office via resolution.planning@cabinetoffice.gov.uk.
3. **Contingency plan template.**
4. **Contract Tiering tool.**
5. **Assessing the Economic and Financial Standing of Suppliers Guidance Note.**
6. **Corporate Financial Distress Guidance Note.**
7. **GovS 008: Commercial Functional Standard.**
8. **The Green Book:** appraisal and evaluation in central government.
9. **Government Soft Landings Revised guidance** for the public sector on applying BS8536 parts 1 and 2.
10. **OGC Gateway Process Review 4: Readiness for service.**
11. **OGC Gateway Process Review 5: Operations review and benefits realisation.**
12. **Reducing the carbon footprint of ICT products through material efficiency strategies.**





12 Exit planning and legacy IT

Planning for and maintaining a view of the end of a contract's life is essential for DDaT contracts. This is key to preventing new legacy IT from developing and early planning puts us in a position to conduct orderly transitions to new contract arrangements.

Preventing future legacy IT

The early part of this Playbook sets the expectation that all projects and programmes should invest time and resources in preparation. This guiding principle equally applies when we are approaching the completion of a contract and planning for this at the earliest stages is essential.

Legacy IT is often the result of a failure to plan for the end of a contract, product or service's life and is one of the biggest issues for the government's DDaT products and services. Technical debt is an estimated cost of future development to make the service or product function optimally again. When we allow our products and services to fall into legacy, this mounts over time as technical debt, with significant impacts on our resilience, security and at a cost of billions of pounds to the public.

To avoid this, contracts should be designed with the right length of time in mind and we have to plan for the expiry, extension, transition and termination of our DDaT products and services in good time and contracting authorities, and suppliers should work together to ensure that there is an agreed and streamlined process to wrap-up

contracts at the end of a project, including any final payments and the timely resolution of any outstanding issues.

Exit planning⁹

Contracting authorities should undertake early planning for contract end including with regards to knowledge transfer, ongoing support needs and plans for e-waste and disposal of hardware and decommissioning of data.

Effective exit planning will be linked to wider strategies and will take into account common pitfalls, including with regard to legacy IT to ensure, under any circumstances, a smooth transition to new arrangements. The contract should have been written to include clear expectations for exit and transition arrangements, including obligations on the supplier to warrant data and information back to the department at the end of the contract.

In practice, contracts should include a requirement to develop an exit plan that joins together the exit strategy of the outgoing supplier with the mobilisation of the incoming supplier (or in-house provision). Contracting authorities should also consider using IT demand management and cost optimisation tools to address (and remove) unused and under-used legacy assets and capacity.

⁹ Legacy IT Guidance Note: Guideline 12

“ Departments should consider how performance and a service may benefit from a phased introduction rather than an abrupt step change”

Preparing for exit takes time. Plans for exit requirements should be regularly reviewed, not just at the end of life of the contract so that adequate time can be allocated for exit management. The exit plan may be separate or included within the contract management plan, and should include:

- a clear outline of activities, milestones and required resources
- roles, responsibilities and accountabilities for each activity
- a joint risk register
- defined timelines, criteria and standards that each activity is required to meet
- relationship and behavioural expectations
- key interfaces and dependencies
- asset registers and transfers including digital, data and knowledge assets and processes

In order to ensure continuity and successful transition, it is key that the right resource remains on a project through to completion and handover and does not move off early due to budget constraints or to deliver other projects.

Contracting authorities should ensure sufficient incentivisation within the contract for incumbent suppliers to maintain resources and performance up to contract end.

Extensions

Some contracts contain an option to extend. Whether to take up this option or not should be considered well in advance notice being served. Extensions above £20 million will require approval under commercial spend controls and contracting authorities should apply the relevant governance and assurance processes as needed. Effective management of our commercial pipelines helps to ensure we are prepared for this decision. See also section 4.3.5 of the government commercial functional standard.

In the past, when we failed to plan early enough, we have been left in the very weak position of having inadequate time to carry out a re-procurement.

During any extensions, the adequate cost and time needed to address the risk of future accumulation of legacy IT will need to be retained and not be traded away for a short-term saving, since this may lead to an accumulation of legacy IT at a later date.¹⁰

We should plan early and set out our requirements for any extension to the contract. Some contracts provide for an extension to be on the same terms and conditions, while others rely on a review clause that, if it is to be relied upon, should set out a clear, precise and unequivocal review process. If we decide not to extend the contract, this decision should be taken far enough in advance to allow for a re-procurement.

Transition

Where delivery of a project or programme is being transitioned, either to another supplier or to in-house delivery, effective mobilisation immediately following contract award and prior to the contract start date is a key phase in setting up a project for success.

Adequate time should be set aside for mobilisation activities in the planning of a procurement to make sure that the right contract management processes and relationship can be developed prior to the contract going live.

Departments should consider how performance and a service may benefit from a phased introduction rather than an abrupt step change. If a phased introduction is required, this should be made clear in the procurement documents.

Plans should include the requirement for dual running of the product or service. IT demand management and cost optimisation tools may identify unused and under used capacity of the legacy system which could be turned off earlier and result in cost savings.¹¹

Data exchange

A critical success factor for an effective project or programme is the sharing of high quality and robust data between parties during the project lifecycle and into operation and contract end.

Contracts should be written to include clear expectations for completion, support, maintenance and transition arrangements, including obligations on the supplier to supply data and information back to the contracting authority at the end of the contract.

If required for a reprocurement, then data and information must be transferred to the contracting authority in time for it to be given to upcoming bidders. This is an essential component of our relationships with suppliers and the provision of the appropriate data at predetermined milestones or intervals should be business as usual for all contracts across government.

Application Programming Interfaces (APIs) should be used to enable effective data sharing across suppliers and departments in interoperable, reusable and open formats. This should conform to the government's API standards and Data Quality Framework and be monitored on an ongoing basis. This is also enabled by the use of open data standards rather than bespoke ones.

¹¹ Legacy IT Guidance Note: Guideline 7



Evaluating and sharing success and lessons learned

To deliver the best possible outcomes for our users, we need to collect systematic and robust data to understand what is going well and where we can improve.

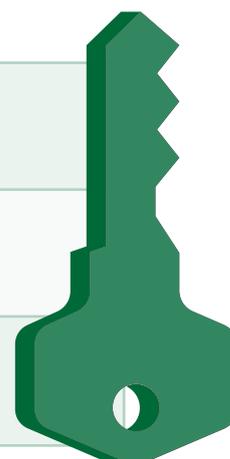
Ongoing scrutiny and transparency with regard to delivery is essential and evaluation should be linked back to the outcomes set out in the Project/Programme Outcome Profile.

This should be used to capture lessons throughout the life of a project or programme and feed these back into delivery throughout the project lifecycle.

Feedback, stories and case studies should be published to share learnings across the public sector. This is particularly important for agile projects to ensure that our iterations are able to demonstrate our progress against outcomes and enable others across government to benefit from existing learning.

Key points

1. Contracts should be designed with the right length of time in mind, and plan for the expiry, extension, transition and termination of our digital, data and technology products and services in good time.
2. Be prepared for the additional burden on operational and commercial staff of simultaneously managing an existing contract, tendering a replacement contract, on-boarding a new provider and off-boarding an incumbent.
3. Engage with the market and senior stakeholders to consider what type of relationship is most appropriate for the project and use this to inform the choice of procurement procedure and contractual model.



Want to know more?

1. **Retiring your service.**

About this Playbook

Key terms

1. Contracting authority' – all public sector bodies procuring DDaT products and services (excludes devolved administrations). The Digital, Data and Technology Playbook is mandatory for central government departments and arm's-length bodies (ALBs) on a 'comply or explain' basis, recognising that there is not a one-size-fits-all approach for all DDaT products and services. It should be considered by the wider public sector. See 'What is the scope of the Digital, Data and Technology Playbook?'.
2. Departments' – used where a point is specific to central government departments and ALBs.
3. 'Shall' – the Digital, Data and Technology Playbook, and all principles and policies contained within it is mandatory guidance for central government departments and ALBs to be implemented on a 'comply or explain' basis (see 'contracting authority'). This will be enforced through spending controls, appropriate governance and approval processes for central government and ALBs.

Who is the Digital, Data and Technology Playbook for?

The Digital, Data and Technology Playbook is aimed at Commercial, Finance, Project Delivery, Policy and any professionals across public sector contracting authorities who are responsible for the planning and delivery of public sector DDaT contracts.

The principles and policies have been co-developed with input from public officials and industry stakeholders. They can be considered good practice for all professionals involved in public digital and data projects and programmes across the public sector. The Playbook will be supported through further guidance and engagement materials in 2022 as part of the implementation programme.

Experience has shown us that successful project delivery requires cross-functional working bringing together different professional areas of expertise. The key is ensuring that we have joined-up teams with input from the right functions early in the process. Pipeline reviews can help to facilitate early planning and identify opportunities for more collaborative working.

Figure 10 provides an analysis for the 11 key policies mapped against functional groups. This should be considered a guide to support contracting authorities in implementing the Digital, Data and Technology Playbook and may vary in different contracting authorities depending on their structure.

Ministers, Permanent Secretaries, Accounting Officers, Commercial Directors, Project Sponsors and Senior Responsible Owners will also find this Playbook useful when acting as decision makers or approvers, or when conducting checks within the capacity of scrutiny and assurance.

Figure 10. Analysis of roles and responsibilities across the 11 key policies.
OKUA stands for:

- **O**wnership: Individuals within the function lead the activity and have overall responsibility for it. '**Joint-O**' is used where ownership is split across a number of functions.
- **K**nowledge: Individuals within the function are the Subject Matter Experts on at least one element of the activity.
- **U**nderstanding: Individuals within the function understand what the activity is and what good looks like.
- **A**wareness: Individuals within the function know what activities are required and who is responsible

Figure 10: Key policy areas mapped against functions

Functions	1 Commercial pipelines	2 Market health and capability assessments	3 Delivery Model Assessments	4 Cyber security assessment	5 Testing and learning	6 Effective contracting	7 Open and interoperable data and code	8 Legacy IT and up-to-date products	9 Assessing the economic and financial standing of suppliers	10 Sustainability	11 Resolution Planning
Commercial	O	O	K	J-O	K	J-O	K	J-O	J-O	J-O	O
Finance	U	U	U	U	A	U	A	J-O	J-O	U	K
Programme and operations including project delivery, digital, property, HR	K	U	J-O	J-O	O	K	K	U	U	K	U
Policy	A	A	U	K	K	U	O	U	A	U	A
Legal	Legal need awareness of the legal obligations throughout the project or programme lifecycle										
Other functions including audit, comms, digital security	Other functions' roles will depend on individual projects										

What is the scope of the Digital, Data and Technology Playbook?

The Digital, Data and Technology Playbook applies to all DDaT projects and programmes including software and hardware. It describes what should be done from policy inception through to transition to operation and sets out a best practice framework to achieve improved delivery and outcomes. This framework should be embedded through the structure of an organisation from governance through to the delivery of individual projects and programmes.

This Playbook is mandatory for central government and arm's-length bodies (ALBs) on a 'comply or explain' basis recognising that there is not a one-size-fits all approach for all DDaT products and services. It should be taken into account by the wider public sector. Figure 9 sets out the actions contracting authorities and suppliers should take in adopting the Digital, Data and Technology Playbook.

Where the planning and preparation of projects and programmes is already underway or there are existing frameworks in place, contracting authorities should adopt a pragmatic approach to embedding the Digital, Data and Technology Playbook by taking all reasonable steps to embed the principles and policies at the appropriate stage of development. There is no expectation to restart in-train projects and programmes or re-let existing frameworks.

The Digital, Data and Technology Playbook is part of a wider portfolio of Sourcing Playbooks developed by the Cabinet Office. Guidance on the delivery of public services is available on [GOV.UK](https://www.gov.uk).

The Markets, Sourcing and Suppliers team can support contracting authorities in deciding which Playbook is most appropriate for their project.

Framework agreements are in-scope of the Digital, Data and Technology Playbook, and should be set up in accordance with the principles and policies set out.

Implementation

Implementing the Playbook has begun but this is a journey the whole of government will walk together to improve the way we deliver projects and programmes. The government has committed to a multi-year implementation period to drive improvement on a 'comply or explain' basis recognising that there is no one-size-fits-all approach.

The Cabinet Office will develop materials to support implementation including a series of e-learning modules which will be available on the [Government Commercial College](https://www.governmentcommercialcollege.gov.uk).

Further information on implementation is available via markets-sourcing-suppliers@cabinetoffice.gov.uk.

Contacts

Contracting authorities and industry are encouraged to reach out where parties are not approaching projects and programmes in the spirit of this Playbook. For further information or to provide feedback on the Digital, Data and Technology Playbook, please contact the Cabinet Office Markets, Sourcing and Suppliers team at markets-sourcing-suppliers@cabinetoffice.gov.uk.

This Playbook will be updated annually to respond to feedback and ensure that it continues to represent best practice.

