Office for Environmental Protection

Board Paper

Date
8 December 2022

Title
Digital Data and Technology (DDAT) Strategy

Report Author

Rich Marsh, Head of Digital and IT

Responsible Executive Director
Richard Greenhous, Chief of Staff

Paper for decision

Issue

1. The OEP's Digital, Data and Technology (DDAT) Strategy has been developed over the last few months of operation. We are now seeking Board approval of the proposed strategy.

Recommendation

2. We recommend that the Board agree the following:
    a. Four design principles - cloud first, security by design, common standards, web accessibility - to drive future decision making.
    b. Agree to exploit the full length of contracts if SLAs are met and we are satisfied with the service, performance, user experience and functionality.
    c. The proposed DDAT operating model of a small inhouse team managing supplier performance and procurement; supporting staff through training, guidance and IT expertise; expanding the team when required for project work through outsourced talent.
    d. The further development of the Intelligence Management System with a view to be able to start work next financial year, subject to Business Plan approval.
    e. To initiate a project to develop an evidence led plan of website improvements and to subsequently deliver in an iterative manner, subject to Business Plan approval.

f. *This section has been redacted as its publication would be prejudicial to the effective conduct of public affairs.*

Background

3. Our IT estate is the result of a DDAT strategy developed to support the founding and establishment of the OEP. The strategy was developed by DDTS, a Defra digital and IT team. It sought to reflect known and emerging needs of the organisation and our operating context, most notably our small size. The task this year has been to operationalise the service and build beyond the Minimum Viable Product at launch.

Overarching IT Design Principles

4. There are four overarching Design Principles that underpin the development and delivery of our IT estate. They are a sound set of design principles to guide our work in the future and ensure we don't become an organisation constrained by Legacy IT.

5. These are:

a) **Cloud First:** The OEP will look to procure commercial 'cloud' offerings first, rather than dedicated software and hardware, as this will avoid the need for on premise IT infrastructure and lead to more cost-effective and flexible solutions. On premise IT and bespoke solutions invariably results in legacy IT and technical debt.

b) **Security and Data Protection:** Security must be designed into all solutions to provide the level of protection that is appropriate for an arm's length body and conform to both GDS and Defra security standards.

c) **Portability and interoperability:** By selecting off-the-shelf products, the OEP is looking to purchase commodity components that will integrate, reduce the need for bespoke elements and minimise future impact to the organisation.

d) **Accessibility:** All OEP's services should be designed or procured to be easily accessible to all users, including users who require reasonable adjustment for both physical and user interfaces.

Architecture, standards and security

6. Our IT estate can be conceptualised as a set of cloud services. The network enables safe, filtered and monitored access to the public internet with a set of supporting services to protect our staff and enable secure log in to our other business applications like Jira, iTrent and Travel Planet.

7. The IT estate consists of modern, cloud-based technology, provided by a set of suppliers working to documented Service Level Agreements. Our IT estate does not contain any proprietary software or working practices.

8. The operating model is dependent on a small, in-house team managing suppliers and facing into the business to develop and deliver change, most ordinarily through our existing supplier network.

9. Cyber and information security has been properly considered, with Data Protection Impact Assessments in place for IT that manages personal data. We have an operational Security Operations Centre managed by our supplier. Each of our services has undertaken an IT Health Check, a critical and yearly independent assessment of its security.

Analysis

Design principles

10. We propose the adoption of the four design principles. They serve to eliminate the emergence of legacy IT by adopting commercial 'cloud' offerings, procured from established frameworks, rather than building dedicated software and hardware, and for these to be bound by government standards for data security, interoperability and accessibility.

Exploitation of contracts

11. For the purposes of this strategy, we have included six blocks of technology: end-user computing; complaints management system; website; HR system; travel system and finance system. We have assessed each based on their current performance, quality and strategic fit and recommended a course of action for each. In general, where the service provided is performing to the Service Level Agreement (SLA) and meets our needs, we recommend exploiting the full length of our contracts. This is driven partly by a desire to exploit value and to recognise that changing suppliers can be costly, especially in terms of consuming staff time and attention which given our organisational roadmap is a critical factor.

Operating model

12. Given our size and remit, the operating model we propose is designed to provide value to the entire organisation by focusing on four areas of most importance:

13. **Partnering:** we will be an effective partner to the wider organisation by being open and accessible to provide expert support where needed. For day-to-day queries and problems relating to our IT, we design and encourage self-serve, but we will proactively and reactively support staff when we see support is required. We will also continue to support teams, such as Insights who require specialist software for their work and more widely in the case of the Intelligence Management System.

14. **Securing:** the security of our IT is a key focus. We look to the National Cyber Security Centre for guidance on best practice and will continue to commission independent assessment of our platforms and hold our suppliers to account. We will ensure our staff are periodically reminded and trained in the importance of cyber security and our legal obligations for the secure and compliant use of data.

15. **Supporting:** as a small organisation, we have a supporting role to play in ensuring we use our IT in a safe and appropriate way. We are both our strongest and weakest line of defence. The service model we have, and recommend for continuance, seeks to efficiently manage the interface between the OEP and our supplier led IT and Digital estate to ensure our staff can use their IT in a safe and appropriate way. We will employ automated monitoring to actively manage the software we have in operation, ensuring we get value for money and can target support. We will engage with our risk management framework to mitigate IT risks and issues.

16. **Delivering:** given our supplier led estate and well-defined contractual endpoints, we will approach the end of these contracts in such a way that we can develop an evidence led plan and to fully engage with our governance framework to ensure controlled, professional delivery.

17. These four pillars of our DDAT operating model; Partnering, Securing, Supporting and Delivering are encapsulated in our proposed Roadmap that plots a course through the next three years, looking at how we deliver and how we might resource our plans.

18. The four pillars and design principles serve to deliver a high-quality IT offer for our staff and the organisation. Measuring and tracking performance and user experience is a critical way to assess the health of our IT. We commit to six monthly staff feedback surveys, assessing staff satisfaction with our IT. We will use this to inform how we can improve our service and better support staff. An example of responding to survey feedback is the recent SharePoint and OneDrive training provided to staff.

19. In totality this strategy demonstrates a critical area of our independence; to manage and operate an IT estate that is architecturally separate from Defra, but which is operated in a way that Defra, and wider government, recognise as meeting public sector standards.

Intelligence Management System

20. Being mindful of our capacity to deliver additional change, we are proposing to reuse technology already procured for our Complaints and Investigation team to build a proof-of-concept Intelligence Management System. While this needs further definition and scoping, we are optimistic the combination of Jira and Confluence, two widely used and highly configurable cloud software packages, will provide the necessary functionality to better exploit the various forms of intelligence we gather by centralising, categorising, linking and making searchable. We propose to invest in further scoping and development to be ready to progress next financial year, pending Business Plan approval.

Ongoing resource requirements

21. It is clear from embedding IT operations this year and assessing our future roadmap that a G6 Head of IT and Digital is a long-term requirement for the OEP. Our IT estate has the breadth of a larger organisation, requiring broad knowledge and experience to manage it. In addition, it is supplier led and experience of managing multiple suppliers is essential. With the general operating climate uncertain, we recommend that this role is converted to a permanent role at its current grade.

22. Fundamentally, this DDAT strategy exists to support our overall strategy by providing a modern, secure and user-friendly technology platform on which we work and operate.

For further detail on this strategy, please refer to annex A: DDAT Strategy document.

Finance and Resource

23. When assessing the proposed operating model considering the experience gained this year, it's clear that an increase in our in-house capacity is required to ensure we have the operational resilience to support the overall service. This is especially the case with end-user computing where single points of failure are emerging which could impact operational

performance during staff absence. *This section has been redacted as its publication would be prejudicial to the effective conduct of public affairs.*

24. *This section has been redacted as its publication would be prejudicial to the effective conduct of public affairs.*

25. The Head of IT and Digital role was envisaged as an 18-month secondment to complete the establishment build and embed an IT operation. What is clear from the nine months of operation is that while we are a small organisation, we have a broad IT estate with many suppliers and strong demand for continued enhancement to existing products as well as support for new IT propositions, such as an Intelligence Management System. Our supplier led estate means that we will regularly be procuring IT and delivering it into the business, which requires an appropriate level of seniority to manage the work effectively.

26. *This section has been redacted as its publication would be prejudicial to the effective conduct of public affairs.*

27. When larger projects emerge that require additional capacity and specialist skills, we will assess each project on merit and consider a range of options, including:

    a. **Contingent labour**: When one or two roles are required, for instance a Business Analyst or User Researcher, using the Public Sector Resourcing contingent labour framework may be the most appropriate channel.
    b. **Open procurement**: When a larger piece of work emerges with a clearly defined outcome, it is often desirable to contract with a specialist provider. A good example is where we outsourced User Experience Design work to Hippo Digital and as a result dealt with a co-ordinated and coherent team.
    c. **Existing supplier**: When delivering changes on an existing platform, such as the website or complaints management system, it will often be most economical and efficient to use the supplier's inhouse team.

28. *This section has been redacted as its publication would be prejudicial to commercial interests.*

Impact Assessments

Risk Assessment

29. There is an inherent risk of cyber-attack to the OEP, given the geo-political situation and our position in the public sector. *This section has been redacted as its publication would be prejudicial to the effective conduct of public affairs.*

Equality Analysis

30. No material equalities impacts have been identified.

Environmental Analysis

31. By utilising cloud technology, we are minimising our environmental impact as we can benefit from economies of scale and not having to run our own infrastructure. Architecturally, our IT is based on scalable architecture that increases and decreases capacity based on usage.

Implementation Timescale

32. The roadmap section outlines our plans for the next three years.

Communications

33. Outside of Cascade update, no specific communications are identified.

External Stakeholders

34. We will communicate our DDAT strategy to Defra DDAT as part of our ongoing engagement regarding our forthcoming GDS Assessment.

Paper to be published	In part, with commercially sensitive information redacted.
Publication date (if relevant)	With minutes
If it is proposed not to publish the paper or to not publish in full please outline the reasons why with reference to the exemptions available under the Freedom of Information Act (FOIA) or Environmental Information Regulations (EIR). Please include references to specific paragraphs in your paper	We aim to be as transparent as we reasonably can. We seek to be clear and open about what we are doing and why. We should have clear reasons where we propose not to publish. Publication would harm the OEP's commercial interests (s.43).

ANNEXES LIST

ANNEX A

This section has been redacted as its publication would be prejudicial to the effective conduct of public affairs.

ANNEX B

This section has been redacted as its publication would be prejudicial to the effective conduct of public affairs.