



National Audit Office



REPORT

The Digital Strategy for Defence: A review of early implementation

Ministry of Defence

SESSION 2022-23
19 OCTOBER 2022
HC 797



We are the UK's independent public spending watchdog.

We support Parliament in holding government to account and we help improve public services through our high-quality audits.

The National Audit Office (NAO) scrutinises public spending for Parliament and is independent of government and the civil service. We help Parliament hold government to account and we use our insights to help people who manage and govern public bodies improve public services.

The Comptroller and Auditor General (C&AG), Gareth Davies, is an Officer of the House of Commons and leads the NAO. We audit the financial accounts of departments and other public bodies. We also examine and report on the value for money of how public money has been spent.

In 2021, the NAO's work led to a positive financial impact through reduced costs, improved service delivery, or other benefits to citizens, of £874 million.



National Audit Office

The Digital Strategy for Defence: A review of early implementation

Ministry of Defence

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 17 October 2022

This report has been prepared under Section 6 of the
National Audit Act 1983 for presentation to the House of
Commons in accordance with Section 9 of the Act

Gareth Davies
Comptroller and Auditor General
National Audit Office

13 October 2022

Value for money reports

Our value for money reports examine government expenditure in order to form a judgement on whether value for money has been achieved. We also make recommendations to public bodies on how to improve public services.

The material featured in this document is subject to National Audit Office (NAO) copyright. The material may be copied or reproduced for non-commercial purposes only, namely reproduction for research, private study or for limited internal circulation within an organisation for the purpose of review.

Copying for non-commercial purposes is subject to the material being accompanied by a sufficient acknowledgement, reproduced accurately, and not being used in a misleading context. To reproduce NAO copyright material for any other use, you must contact copyright@nao.org.uk. Please tell us who you are, the organisation you represent (if any) and how and why you wish to use our material. Please include your full contact details: name, address, telephone number and email.

Please note that the material featured in this document may not be reproduced for commercial gain without the NAO's express and direct permission and that the NAO reserves its right to pursue copyright infringement proceedings against individuals or companies who reproduce material for commercial gain without our permission.

Links to external websites were valid at the time of publication of this report. The National Audit Office is not responsible for the future validity of the links.



Contents

Key facts 4

Summary 5

Part One

The Digital Strategy for Defence 13

Part Two

Progress with implementing the
Digital Strategy for Defence 21

Part Three

Strategic challenges 29

Appendix One

Our evidence base 36

This report can be found on the National Audit Office website at www.nao.org.uk


If you need a version of this report in an alternative format for accessibility reasons, or any of the figures in a different format, contact the NAO at enquiries@nao.org.uk


The National Audit Office study team consisted of:


Kristian Barrett,
Kaye Dunnett, Daniel Kintoff,
Abdullah Mohamed and
Jenna White, under the
direction of Tom McDonald.

For further information about the National Audit Office please contact:

National Audit Office
Press Office
157-197 Buckingham Palace Road
Victoria
London
SW1W 9SP

 020 7798 7400

 www.nao.org.uk

 @NAOorguk

Key facts

£4.4bn

estimated spend on digital in 2021-22 by the Ministry of Defence (the Department)

£11.7bn

how much Defence Digital estimated in 2019 it will spend updating or replacing legacy technology over the following decade

£2bn

total cash-releasing efficiencies Defence Digital intends to find for the Department by 2032-33

£1.7 billion

the estimated amount of the Department's £4.4 billion 2021-22 digital spend that is outside the direct control of the chief information officer

200,000

users in the Department and the Armed Forces

66%

percentage of Top-Level Budgets' 2022-23 digital alignment tasks which are on track for completion or face only minor issues

**55 to
2 minutes**

the change in call waiting time for the IT service desk between October 2021 and May 2022

78%

the proportion of significant project delivery milestones Defence Digital completed successfully in 2021-22

151

people with high-priority technical skills that Defence Digital is currently aiming to recruit

Summary

1 The nature of modern warfare is changing, with access to and exploitation of information becoming vital to securing military advantage. The government's Integrated Review placed greater priority on identifying and deploying new technologies faster than potential adversaries to enable operations across all arenas of warfare and collaborate better with partners. Cyberspace is itself also becoming an increasingly important arena of warfare, with external threats increasing and constantly evolving as access to offensive cyber capabilities becomes easier.

2 The Ministry of Defence's (the Department's) assessment is that it needs to keep pace with adversaries in adapting to this shifting technology landscape, but that it is not set up to implement digital technology at speed and scale. Like many government departments, its digital estate contains many aged ('legacy') systems, with resulting operational and cyber security vulnerabilities.¹ The Department holds vast amounts of data, but those data are not easily accessible across its different component bodies. It also has gaps in critical skills and its organisational processes are not always suited to best delivering digital technology.

3 To address these challenges, the Department has developed the Digital Strategy for Defence (the strategy), which describes how it intends to transform its use of technology and data. The Department aims to achieve three strategic outcomes by 2025, which are:

- a digital 'backbone' – this is how the Department describes the technology, people, and organisational processes that will allow it to share data seamlessly and securely with decision-makers across all the military and civilian domains.
- a digital 'foundry' – a software and data analytics development centre. This will use the capability and access to data provided by the 'backbone' to rapidly develop digital solutions in response to emerging needs; and
- an empowered digital function – a skilled and agile community of digital specialists who will help deliver digital transformation and closer integration across Defence.

4 The Department hopes that, collectively, these will help realise its vision for 2030 of allowing users across all Armed Forces and Defence organisations to access and use the data they need without barriers, and better support more joined-up decision-making.

¹ Legacy refers to systems and applications that have been operationally embedded within a business function but have been overtaken by newer technologies or no longer meet changed business needs.

5 The Department's chief information officer (CIO) leads Defence Digital, an organisation within Strategic Command. The CIO sits on the Department's Executive Committee and reports jointly to the commander of Strategic Command and the second permanent secretary, who holds senior accountability for digital across Defence. The CIO and Defence Digital lead the digital function, which ensures that digital activity is coordinated across the Department and its Top-Level Budget (TLB) organisations. The CIO and Defence Digital are responsible for leading the implementation of the strategy, with support from TLBs, through a portfolio of organisational change and technology upgrades.

Our report

6 Our report examines whether the Department is on track to achieve value for money in its implementation of its digital strategy. To do this, we would expect the Department to:

- have put in place an appropriate strategy, considering its strategic context and existing digital estate, drawing on good practice;
- have made initial progress implementing the strategy in line with a delivery plan, which allows it to measure and coordinate progress; and
- be working to address the biggest barriers to success and know how it will prioritise its resources and people.

7 Our report is in three parts:

- Part One looks at the Department's strategic context, digital estate and the Digital Strategy for Defence.
- Part Two examines the Department's progress with implementing the strategy.
- Part Three considers key challenges to the Department's implementation of the strategy.

Scope of our work

8 Our report focuses on the May 2021 *Digital Strategy for Defence* and the Department's implementation of it. We, therefore, considered performance information between its publication and our cut-off point for reporting of 30 June 2022 (except where otherwise stated). We have not performed a detailed review of the Department's performance on previous digital strategies or programmes, except to the extent it continues to deliver them as part of the current strategy.

9 Our scope includes the whole Department because, although Defence Digital is responsible for leading implementation, the strategy is intended for all of Defence. We do not draw a distinction in our scope between core IT infrastructure and deployed military technologies, as modern warfare requires the seamless movement of data and applications between these spaces. The Department's ambition is to create the infrastructure and organisational capability to do this.

Key findings

The Digital Strategy for Defence

10 Implementation of the strategy will help the Department to operate more effectively in an era of disruptive technology and evolving security threats.

The government and Department have set out in several strategy and policy documents that the nature of warfare is changing. In response, the Department aims to join up military operations across land, air, sea, space and cyber and work closely with the rest of government, academia, industry and international partners. The Department has recognised that data are fundamental to achieving this integration and that it needs to transform its digital capabilities to be secure and easy to use so that it can share information seamlessly and make decisions based on data (paragraphs 1.2 to 1.4 and Figure 1).

11 The Department's assessment is that to keep pace with the increasing capabilities of adversaries requires a fundamental reset of its digital capability.

The Department's diagnosis is that its data are hard to access and share, it has gaps in critical skills, its core technology needs updating and its organisational processes are out of date. This is consistent with our wider work on the reasons government finds digital change challenging. The Department has a large legacy IT estate and upgrading to modern replacements is complex. Defence Digital estimated in 2019 that it would spend £11.7 billion over a decade updating or replacing systems, although this figure does not encompass all of the Department's legacy estate (paragraphs 1.5 to 1.7 and Figure 2).

12 The nature of the Department's business adds additional challenges to implementation of the strategy. The Department works across three security classifications (Official, Secret and Above Secret), which sometimes requires it to develop separate systems for each. The Department uses its technology in hostile environments with limited connectivity, such as at sea. This adds to the challenge of modernising and integrating technology. Adversaries also may be actively looking to degrade its digital and military capabilities. The Department shares data with international partners and must be able to work with their technical solutions and security policies (paragraphs 1.8 and 1.9).

13 The Department's digital strategy is consistent with good practice.

The strategy states the Department will focus on technology, people, processes and cyber security so that it can securely and seamlessly share and exploit data. Importantly, the strategy recognises that data are a strategic asset and that people and processes are as vital as technology to successful digital change. Both wider government and the Department have been slow to implement digital strategies previously. However, there is strong support for the current strategy from the most senior leaders of the Department (paragraphs 1.10 to 1.14 and Figure 3).

Progress implementing the Digital Strategy for Defence

14 The Department does not have a complete plan to implement the strategy or a clear way of measuring whether its implementation of the strategy is on track.

Although the Department has individual plans supporting each of the individual workstreams and programmes, it has not brought these together to provide a complete picture of progress across the strategy. In our work on implementing digital change across government, we have stressed the need for an overall plan for how an organisation can transform itself that clearly sets out the associated ambition and risk. Such a plan would also allow the Department to prioritise its activity effectively when delivery challenges emerge (paragraphs 2.2 to 2.4).

15 The Department has substantially improved the governance of its digital function, which has begun to align Defence organisations to common digital standards and approaches. To create the coherence of digital activity needed to realise the strategy, the Department has developed common approaches and standards for aspects such as data, technology architecture and cyber security. For example, a new Chief Data Office has developed a Data Strategy and rules for formatting and managing data to make them more accessible and usable across Defence. The Department has also established governance to oversee the adoption of these standards across its business, which for 2021-22 it assessed as working effectively with only minor weaknesses. However, the changes required to comply with these standards are substantial, and currently at an early stage. For example, the Department has not yet fully mapped its legacy estate, and not all technology teams have adopted the new standards. Defence Digital sets TLBs annual tasks to improve digital coherence across the Department. For 2022-23, TLBs reported at the end of June that they are on track, or face only minor issues, with completing 66% of them. However, they face moderate issues with, or are at risk of not completing, 29% of them (paragraphs 2.5 to 2.11 and Figures 4 and 5).

16 The Department has improved its core IT services and has plans to improve services further. In 2015, the Department assessed that its users' experience was unacceptable: its operating system was out of date; users had limited storage and collaboration tools; and its devices largely did not allow mobile working. As a result, the Department amended its core IT service contract to progressively roll out upgrades, such as an improved core IT system (MODNet), new software and mobile devices. While the Department judges that its core IT is now fit for purpose, it concluded that the contract was too large, insufficiently transparent to understand user experience, and lacking in levers to improve services further. It is now breaking the contract up and procuring its constituent services separately, which it will integrate itself. The new user service desk introduced in October 2021 supports this effort, by gathering information to spot common problems and address them faster. Following the introduction of the new service desk there was a fall in service performance, but it has recently begun to show improvement in service call waiting times and incident resolution times (paragraphs 2.12 to 2.14).

17 Defence Digital's historically poor reputation for project and programme delivery has been a barrier to integrating digital activity across Defence.

Defence Digital has a portfolio of more than 90 digital projects and programmes, including larger and more complex major programmes, many of which it needs to replace fragmented legacy systems and older software with newer capabilities. Defence Digital's project delivery has suffered from a lack of skilled and experienced personnel, immature project controls, and a culture focused on the approvals process rather than outcomes. TLB CIOs told us that this undermined trust in Defence Digital's delivery of the strategy and incentivised them to maintain or produce their own separate capabilities for certain requirements, rather than rely on shared ones delivered by the Department (paragraphs 2.15 and 2.16, and Figure 6).

18 Defence Digital has recognised the weaknesses in its project and programme delivery and is taking action to begin improving them. Defence Digital is resetting its project delivery organisation with improvements including better management information and reporting. The effects are not yet clear in its performance, which the COVID-19 pandemic has also affected. In 2019-20, Defence Digital completed 76% of its most important project delivery milestones, but this fell to 57% in 2020-21 before recovering to 78% in 2021-22, with the Department aiming to increase this to 90%. As of June 2022, two-thirds of projects across its total portfolio reported delivery confidence ratings of green or amber-green, a level it has broadly maintained since the end of 2020-21. The delivery of its major programmes has remained challenging; the Infrastructure and Projects Authority (IPA) publicly rated five programmes for 2021-22, of which three programmes were rated amber, and two red.² Defence Digital has further plans to improve delivery, including through additional technical training for its delivery staff (paragraphs 2.17 to 2.19 and Figure 6).

² The IPA produces an annual report that assesses the likelihood of government major programmes achieving their aims and objectives on time and on budget. A 'red' rating means successful delivery appears unachievable; 'amber' that successful delivery appears feasible but that significant issues exist requiring management attention; and 'green' that successful delivery appears highly likely with no outstanding issues that appear to threaten delivery. Across its portfolio of programmes, Defence Digital internally uses a similar rating system that adds amber-green and amber-red as two further possible ratings.

Strategic challenges

19 To make the strategy affordable Defence Digital increased its efficiency targets and reviewed its costs, which it found to be lower than it originally forecast.

The Department had not fully funded the strategy when it published it in May 2021. There was a short-term funding gap for digital transformation of £248 million and an additional £260 million needed for the Digital Foundry. During 2021-22 Defence Digital and Strategic Command worked together to identify funding for the strategy and address wider financial pressures on Strategic Command. Defence Digital considers the strategy affordable following the Department's annual budget cycle in March 2022, which prioritised allocating funding to the Digital Foundry. As part of the annual budget cycle Defence Digital found funding for the following few years by reviewing and refining cost forecasts which decreased by £190 million; increasing efficiency targets by £160 million; capitalising £110 million of resource expenditure; and stopping £60 million of lower-priority work. The Department is likely to continue to experience funding challenges for digital transformation: it may need to fund new capabilities; it may underperform against efficiency targets; and it may experience future cost increases (paragraphs 3.2 to 3.4, 3.9 and 3.10).

20 Defence Digital is on track to exceed its efficiency targets for this Spending Review period and aims to identify up to £790 million more by 2032-33.

Defence Digital has formal targets for £1,370 million of cash-releasing efficiencies by 2032-33 but has ambitions to go beyond this and make £2 billion. In June 2022 Defence Digital forecast making £1,215 million of cash-releasing efficiencies between 2023-24 and 2032-33. In the first two years it expects to overachieve against the formal target. However, over the 10-year period it still needs to find £160 million to meet its formal target and £790 million to match its full ambition, and is continuing to work on doing so. It plans for efficiencies to come from workforce transformation, supplier management, automation and data centre rationalisation. Defence Digital's performance in increasing efficiency will affect the funding available for the Department to invest in its priorities, including the strategy, and to address future financial pressures (paragraphs 3.5 to 3.10 and Figure 7).

21 The Department does not have enough people with the right digital skills, which is affecting delivery of the strategy. There is a digital skills shortage across UK industry and the public sector, and the Department finds it hard to recruit and retain talent. This is because the Department cannot match private sector pay, and not all TLBs have the authority from the Department to apply pay uplifts for digital specialists, which is creating internal competition. Technologists see the Department as bureaucratic and the hiring process, including getting security clearance, takes too long. The Department also finds it increasingly difficult to recruit digital specialists to work in Defence Digital's main location in Corsham – it intends to make working flexibly the default to help with this issue. The shortfall of technical skills is affecting the delivery of both individual programmes and the strategy as a whole (paragraphs 3.11 to 3.15 and Figure 8).

22 Defence Digital is trying several initiatives to fix its skills gaps, but its progress has not been fast enough to match the problem and a different approach is required. Our wider work across government suggests that, based on its current plans, the Department will find it difficult to make progress on this issue at the pace it wants. Defence Digital's 'Digital Skills for Defence' programme aims to enhance digital skills across the Department for its digital professionals, leaders and the remaining workforce. Defence Digital is tackling its own workforce challenge by recruiting for technical skills, investing in training, removing legacy roles and reducing the contractor workforce. This activity has taken it longer than anticipated, due to the complexity of developing a workforce plan, and it has begun implementing key elements while it finalises this plan. By June 2022, it had hired 42 of the 151 people with critical skills that it wanted and was in the process of bringing in 39 more. Defence Digital has 3,090 workers, of whom 570 are contractors (18%). It intends to reduce workforce costs further, through organisational restructuring and by reducing the cost of contractors. Defence Digital has started extending its approach to TLBs, who are largely on track to align with it, but still face their own issues acquiring skilled people (paragraphs 3.15 to 3.19).

23 The Department's CIO and Defence Digital are accountable for leading the implementation of the strategy, but they do not have all the organisational levers needed to do so. The CIO is accountable for the whole Department's use of technology and data but only has direct control of £2.7 billion of Defence's estimated £4.4 billion digital spend. There are business changes needed to realise the strategy, which the wider Department will need to deliver. For example, the Department's lengthy approvals and acquisition processes do not suit the more iterative approach favoured in technological change. The Department's senior leadership has recognised that trying to influence the wider Department through the digital function is not enough. The Department is now addressing this as part of its agenda to exploit digital for wider Defence objectives (paragraphs 3.20 to 3.23).

Conclusion on value for money

24 The nature of modern conflict is rapidly digitising, affecting the Department's business and how the Armed Forces operate in the battlefield. The Department has put in place a digital strategy to respond to this challenge, which is consistent with good practice, has provided clear direction across the Department and has support from the most senior Defence officials. The Department has made good progress with bringing together and aligning digital practitioners across Defence. However, its performance in delivering major digital technology programmes needs to improve and is a risk to achieving this alignment.

25 The Department does not have a complete picture of its progress against the strategy and so cannot readily demonstrate whether it is on track to deliver it or not. To meet the needs of the modern battlefield, and enhance its business efficiency, the Department must transform a large and complex organisation with an extensive legacy estate, using scarce specialist skills. Given the scale of the challenge and the persistent barriers to change, achieving the strategy's objectives by 2025 is ambitious. As future delivery challenges emerge, it will be important for the Department to prioritise its funding and specialist skills to where it needs them most urgently. The Department will be able to do this more effectively if it can articulate better how it will achieve the strategy's vision in practice and how it will measure success along the way, not least in supporting its wider departmental objectives. This will allow it to achieve greater value for money with its £4.4 billion of annual digital expenditure.

Recommendations

26 Our recommendation aims to support the Department as it attempts to implement the strategy by its target date of 2025. We recommend the Department should immediately create a clear delivery plan for the digital strategy which:

- integrates the strategy with wider efforts to transform the department, deliver efficiencies and exploit technology;
- identifies and prioritises all the activities needed to achieve its strategic outcomes;
- identifies what people, skills and funding it will need to deliver these;
- develops a set of leading indicators to show the prospects for future progress; and
- sets out and agrees a consistent set of performance information for use across the digital function and the wider Department.

Part One

The Digital Strategy for Defence

1.1 This part sets out the background to the Ministry of Defence's (the Department's) Digital Strategy for Defence (the strategy), an overview of the Department's digital estate, the strategic context for the strategy, its aims, and our comparison of this with similar challenges across government.

Strategic context

1.2 The Department operates a large and complex digital estate with more than 2,000 applications and systems, which support 200,000 users in the UK and overseas. This serves diverse needs including managing veterans' welfare and pensions, maintenance of the Department's physical estate such as naval bases, communication satellites in space and the technology used in warfare. The Department estimated it would spend around £4.4 billion on digital in 2021-22, with around £2.7 billion of this within the central Defence Digital organisation and £1.7 billion in its Top-Level Budget (TLB) organisations across the Department.

1.3 Government has set out in several strategy and policy documents that the nature of warfare is changing. The 2021 Integrated Review, *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*, signalled a change in response to an international order characterised by intensifying competition between states.³ The Department's view is that the UK now has a wider range of state and non-state threats, enabled by technology, which are increasingly blurring the distinctions between peace and war, at home and overseas, and virtual and non-virtual. This includes the newer domains of cyber and space, which opponents will increasingly seek to exploit and which have been characteristics of the current conflict in Ukraine.

³ Cabinet Office, *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*, CP 403, March 2021.

1.4 In response, the Department aims to integrate its activities to move to a way of operating more fit for the information age. As we set out in **Figure 1**, the Department calls this its 'integrated operating concept', which aims to join up military operations across land, air, sea, space and cyber, as well as working more closely with the rest of government, academia, industry and international partners. The Department has recognised that data are fundamental to achieving this integration, which it wants to exploit for competitive advantage through better, faster decision-making and improved defence outcomes. To do this the Department intends to transform its digital capabilities to be secure and easy to use, so that it can share information seamlessly across Defence and with partners and make decisions based on data.

Comparison with the challenge across government

1.5 The Department's assessment is that to keep pace with the increasing capabilities of adversaries requires a fundamental reset of its digital capability. Large-scale digital transformation is inherently difficult for government to achieve, and the Department has not set itself up to adopt technology at speed and scale. The Department's diagnosis is that:

- data are in internal and contractual silos and hard to access and share;
- there are gaps in critical skills across the Department;
- its core technology is fragmented, insecure and needs updating; and
- its organisational processes are suited to the industrial age, not the information age.

1.6 **Figure 2** on pages 16 and 17 shows a simplification of the Department's current process for ordering basic goods such as boots, which involves 29 information systems and 23 different people. This is an example of the Department's reliance on legacy systems and complex processes for accessing and sharing data.⁴ The Department's diagnosis of its digital challenge is consistent with what we identified across government in our report on *The challenges in implementing digital change*.⁵

⁴ Legacy refers to systems and applications that have been operationally embedded within a business function but have been overtaken by newer technologies or no longer meet changed business needs.

⁵ Comptroller and Auditor General, *The Challenges in implementing digital change*, Session 2021-22, HC 575, National Audit Office, July 2021.

Figure 1

The Ministry of Defence and the integrated operating concept

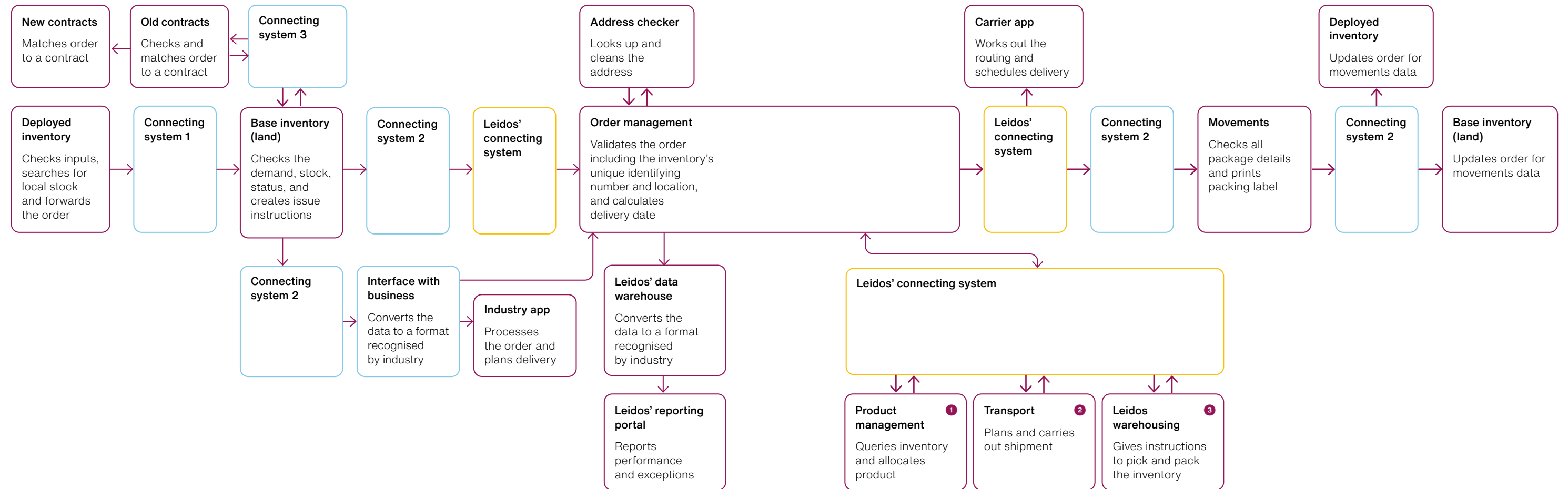
Data are fundamental to connecting the Ministry of Defence internally, across the five military domains, and with external partners and allies



Source: National Audit Office analysis of Ministry of Defence strategy documents

Figure 2
The Ministry of Defence's current process for ordering basic goods

The process for ordering basic goods such as boots is complex and inefficient



- System or application used in the inventory, warehousing and movements process
- Ministry of Defence connecting system that re-routes and formats the data
- Leidos' connecting system that re-routes and formats the data
- Main flow of data

Notes

- 1 This process map shows how the Ministry of Defence (the Department) orders basic goods for the land environment. It does not show how the Department orders other categories of inventory, such as munitions, or inventory for the air and sea deployed environments.
- 2 This is a simplified version of the process, which does not include all systems and steps, but summarises what the Department identifies as some of the most important ones.
- 3 Leidos is a supplier to the Department, providing warehouse management and other services.

1.7 We concluded in that report that government needs to transition from legacy systems to modern replacements, which are cheaper to support and more resilient. However, this takes significant and regular investment over time and upgrading legacy systems can be complex and difficult, especially if they have many dependencies. The Department has a large legacy estate; for example, two of its three main inventory systems have been in place since the 1980s. Defence Digital estimated in 2019 that it would spend £11.7 billion (47% of its planned digital spend) over 10 years updating or replacing legacy systems, although this figure does not encompass all of the Department's legacy estate. The Department describes its legacy challenge as affecting critical defence services, military platforms and enabling communication systems. The Department has started work to understand and address its legacy estate as a whole, beyond its current upgrade programmes, although this is at an early stage (see Part Two). Therefore, it is likely that legacy systems will continue to act as a barrier to digital transformation during the lifetime of the strategy.

1.8 The nature of the Department's business adds additional challenges to digital change. The Department handles data across three security classifications (Official, Secret and Above Secret), including some of government's most sensitive data. This means the Department has to acquire and maintain multiple systems for these different classifications, and the need for additional security accreditations can lead to delays at higher classifications. The Department also has to consider that adversaries may be actively looking to degrade its digital and military capabilities, with the risk of cyber attack among the highest risks managed by the Defence Board.

1.9 The Department has the challenge of needing to work closely across the Armed Forces, which use technology in hostile environments. These environments can require the Armed Forces to operate with intermittent or limited bandwidth, and against challenges from adversaries. For example, the Royal Navy has a limited amount of time to perform work on ships' digital systems while they are in port and often have limited connectivity while at sea, adding to the difficulty of keeping deployed technologies up to date. Where the Department wants to share data with international partners, it must be able to work with their technical solutions and security policies.

The Digital Strategy for Defence

1.10 The *Digital Strategy for Defence* (2021) describes how the Department intends to address these challenges and transform its approach to improve Defence outcomes. The strategy identifies three strategic outcomes it wants to achieve by 2025:

- A digital ‘backbone’ – this is how the Department describes the technology, people and organisational processes that will allow it to share data seamlessly and securely with decision-makers across all the military and civilian domains.
- A digital ‘foundry’ – a software and data analytics development centre. This will use the capability and access to data provided by the ‘backbone’ to rapidly develop digital solutions in response to emerging needs. **Figure 3** overleaf gives an example of this rapid capability development.
- An empowered digital function – a skilled and agile community of digital specialists who will help deliver digital transformation and closer integration across Defence.

1.11 The Department hopes that, collectively, these will help it realise its vision for 2030 of allowing users across all Armed Forces and Defence organisations to access and use the data they need without barriers, and support better, more joined-up decision-making.

1.12 The strategy is consistent with good practice we have identified from our wider work on digital transformation across government:

- Government often does not understand the quality of its data, does not see data as a priority, or tolerates data that are not fit-for-purpose. The strategy sets out the Department’s intention to recognise that data are a strategic asset. The Department’s data strategy identifies the frameworks and rules needed to achieve this.
- Government often does not see technology as part of a service that involves people, processes and systems. The Department’s digital ‘backbone’ approach recognises digital change is as much about people and the right processes as it is about data and technology.

Figure 3

Example of the Digital Foundry's rapid response capability, September 2021

How the Digital Foundry created a secure case management capability for the Afghan Relocations and Assistance Policy (ARAP) team

What happened: At first the ARAP team were reliant on email to share data, which was not a secure way of working. In September 2021 an administrative error resulted in a significant data breach, potentially compromising the safety of Afghans who had worked for UK forces.

Digital Foundry response: Working with the Chief Data Office, the Foundry's automation team used common architectures and systems to build a secure, accredited data platform for the ARAP team in six weeks.

Outcome: The Department reports that all ARAP caseworkers can now access data and process cases through a secure platform including a dashboard and tools to analyse the data better. This allows the ARAP team to track and assist more than 10,000 individuals between Afghanistan and the UK.

Notes

- 1 The ARAP scheme was launched in April 2021 by the Home Office and Ministry of Defence. The scheme offers relocation or other assistance to former locally employed staff in Afghanistan.
- 2 The Chief Data Office is a directorate within the Defence Digital organisation.

Source: National Audit Office analysis of public media reporting and Ministry of Defence documents

1.13 Both central government in general and the Department in particular have been slow to implement digital strategies in the past. We have reported (see footnote 5) that 11 central government digital strategies spanning 25 years failed to change a pattern of poor performance in digital change programmes. The challenges and aims reflected in the Department's 2021 strategy are not new – it has tried to address them in previous strategies. In 2009 the Defence Information Vision identified inefficient processes, data that were insecure or difficult to share, and a lack of interoperability. Its 2011 digital strategy spoke of information as a strategic asset and the need to transform how the Department exploits information and to become more joined-up with partners.⁶

1.14 The current strategy benefits from strong support among the Department's senior leaders. Its four most senior officials have made accelerating digital transformation one of their top priorities.⁷ We spoke to all 16 TLB chief information officers across the Department.⁸ All were either aligned, seeking to align, or supportive of the strategy. The high level of support and strategic momentum may help the Department achieve more fundamental change this time.

6 Ministry of Defence, *MOD Information Strategy 2011: Better Informed, Better Defence*, October 2009.

7 The chief of defence staff, vice-chief of defence staff, permanent secretary and second permanent secretary.

8 The number of chief information officers does not correspond to the number of Top-Level Budgets. For more information, please see Appendix One.

Part Two

Progress with implementing the Digital Strategy for Defence

2.1 This part sets out how the Ministry of Defence (the Department) has begun implementing the Digital Strategy for Defence (the strategy), including its efforts to transform its digital function and its delivery of technology.

Monitoring the implementation of the strategy

2.2 Digital activity and change within the Department are led by Defence Digital, an organisation within Strategic Command led by the Department's chief information officer (CIO), supported by the Department's Top-Level Budget (TLB) organisations. The CIO sits on the Department's Executive Committee and reports jointly to the commander of Strategic Command and the second permanent secretary, who holds senior accountability for digital across Defence. Comprising around 3,000 staff, Defence Digital is responsible for digital strategy and policy, capability development, supporting operations, and supplying IT to users across Defence. Defence Digital is implementing the strategy through its portfolio of organisational change and technology upgrades.

2.3 The Department does not have an overarching delivery plan for the strategy and as a result, cannot easily measure its performance with implementing it. Although it has individual plans supporting each of the workstreams and programmes within the strategy, it has not brought these together to provide a complete picture of progress across the strategy. In our wider work on implementing digital change across government, we stress the need for an overall plan and design for how a business can transform itself that clearly sets out the associated ambition and risk. Such a plan would also allow the Department to prioritise its activity effectively when delivery challenges emerge.⁹

2.4 To assess the Department's progress, we have drawn together the key achievements and challenges in its work aligning digital practitioners and delivering improved common technology across Defence. This is not an exhaustive account of the work the Department is doing to realise the strategy. We also discuss other aspects such as its approach to addressing digital skills and the wider business changes needed beyond its digital practitioners in Part Three.

⁹ Comptroller and Auditor General, *The Challenges in implementing digital change*, Session 2021-22, HC 575, National Audit Office, July 2021.

Transforming the digital function

2.5 The CIO and Defence Digital are responsible for overseeing the Department's digital function, which ensures that digital activity across all of Defence, including its TLBs, is coherent. The Department intends that this coherence will enable the use and rapid scaling of data and technology across Defence. It requires the Department to adopt common standards, technology and ways of working to ensure solutions used by individual organisations are interoperable with others.

2.6 To this end, the Department restructured Defence Digital (**Figure 4**) into a series of functional directorates to develop these common approaches:

- A new Chief Data Office (CDO) has developed a Data Strategy for Defence and a series of rules for formatting and managing data to allow it to be more easily accessed and exploited across the Department. In future, it will support this with an assurance programme to test compliance against these rules and find common issues in their adoption across Defence. The CDO also works with programmes and TLBs to develop and embed data tools.
- The chief technology officer (CTO) directorate has developed a technology sub-strategy and a common technology architecture, which it intends will allow digital systems to be interoperable across the Department. It has carried out some early exploratory work on managing legacy and obsolescence across the group and is setting up a coordination office to develop its understanding further.¹⁰ The CTO also oversees the exploitation of information through the Foundry (see paragraph 1.10) and the Defence Artificial Intelligence Centre, which develop central digital solutions for use by all TLBs, reducing unnecessary duplication of tools.
- The cyber defence and risk directorate has developed a cyber resilience strategy and put in place controls to identify and address cyber security risks. These include cyber compliance framework audits of Defence organisations to assess the maturity of cyber security controls and cyber vulnerability investigations to identify specific gaps. The directorate has a programme of initiatives to continually improve the Department's cyber risk position.
- The functional integration directorate oversees how Defence Digital works with TLBs through the Functional Coherence Board, which it has refreshed following the strategy. TLB CIOs attend this board, which monitors compliance with the rules developed by the other directorates, identifies common issues that TLBs face and encourages collaboration between them. It also works to cohere the function better by aligning TLBs to its workforce initiatives and developing its understanding of the total digital spend across Defence. This will allow it to identify efficiencies by reducing duplication across the Department.

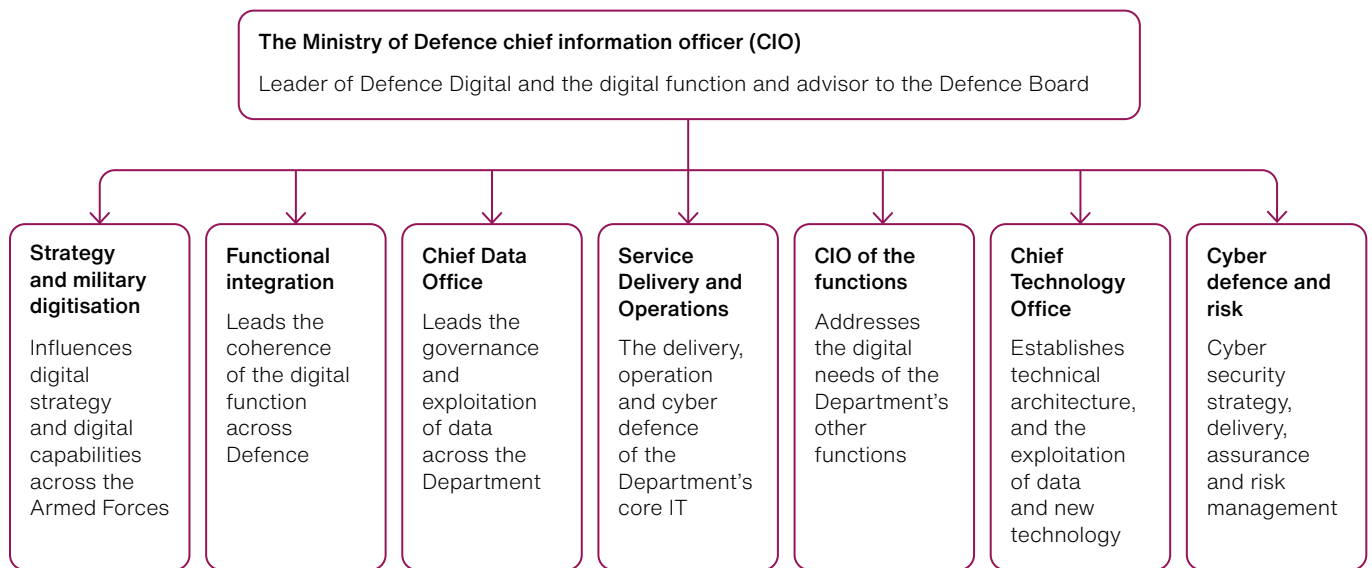
¹⁰ Legacy refers to systems and applications that have been operationally embedded within a business function but have been overtaken by newer technologies or no longer meet changed business needs.

- The Department also established a strategy and military digitisation directorate, which develops digital strategy for Defence, coordinates digital transformation activity and represents the military perspective in the development of digital capabilities. It also has an oversight role for some of Defence Digital’s major technology programmes.

2.7 These changes to governance, and other wider improvements, meant that the digital function reported achieving substantial assurance for the financial year 2021-22. This drew on evidence, such as the annual opinion of internal audit, which the Department’s directorate of assurance reviewed and supported. Substantial assurance means that the governance and controls it set up were working effectively with some minor weaknesses.

Figure 4
Defence Digital’s organisational structure

The Ministry of Defence (the Department) restructured Defence Digital from 2019 into a series of directorates to develop common approaches to data and technology



→ Oversight

Note

1 Functions are all the activities that require common approaches across Defence, including finance, commercial, legal, and security.

Source: National Audit Office analysis of Ministry of Defence documents

2.8 This indicates that the digital function is well set up. However, the changes needed to comply with these common standards and approaches are substantial given the complex nature of the Department's digital landscape, and implementation is at an early stage. An internal review of the digital function in early 2022 found that not all technology teams even within Defence Digital had adopted the common data and technology standards, due to delivery pressures or a desire to innovate. It also found that there were multiple technology architecture initiatives across Defence that did not conform. The Department's understanding of its legacy estate is also immature. An internal audit in March 2022 found the Department did not have a centralised strategy for addressing legacy systems, and it has not fully mapped out its legacy estate.

2.9 The Department's cyber resilience strategy recognises that Defence must adapt to the shifting threat landscape. Its initiatives aim to make all Defence organisations resilient to known vulnerabilities and attack methods by no later than 2030. The Department implements plans where its cyber security audits identify it needs improvements. The Foundry and the Defence Artificial Intelligence Centre were initially not fully funded as part of the Department's Integrated Review settlement. They have recently established their core teams, with the intention to scale up further with the funding allocated by the Department (see paragraphs 3.2 to 3.4).

2.10 Defence Digital sets TLBs a series of annual tasks each year to progress implementation of the standards and activities needed for digital coherence. For 2022-23, nine TLBs report against a set of 32 functional tasks, making 288 tasks in total.¹¹ These tasks fall into different categories. Some are enabling activities such as agreeing a plan with the CDO on data curation or taking part in cyber compliance audits. Others are activities which themselves show coherence across TLBs, such as routinely using Foundry services, or verifying that their projects and initiatives follow the data rules.

2.11 As at the end of June 2022, TLBs reported that they were on track to complete, or face only minor issues in completing, 66% of tasks for 2022-23. However, TLBs reported moderate issues with, or risked not completing, 29% of tasks. Performance varied between the different categories of tasks (see **Figure 5**), as well as between TLBs. Defence Digital intends to build on its new governance and encourage greater collaboration between TLBs in addressing the challenges that they face.

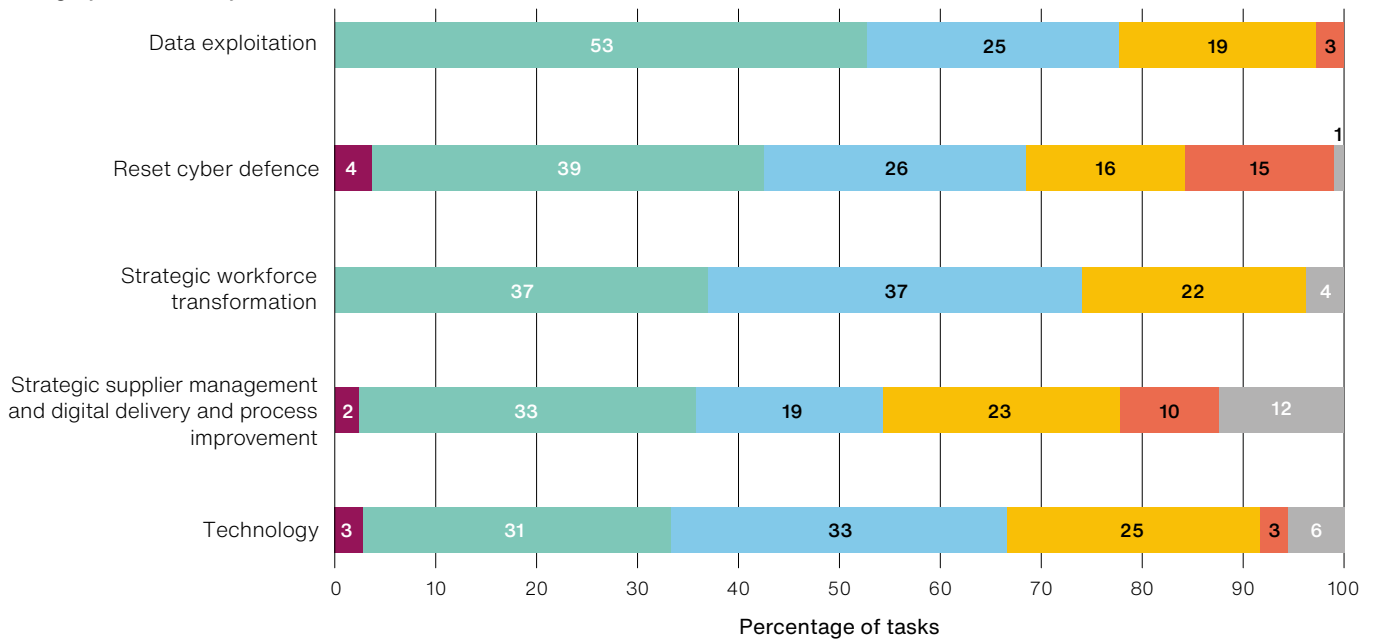
¹¹ For this exercise, the Defence Nuclear Organisation and the Submarine Delivery Agency report as one Top-Level Budget.

Figure 5

Top-Level Budget (TLB) organisations’ progress with tasks set by the chief information officer (CIO) to strengthen the coherence of the digital function, June 2022

TLB progress was mixed across the different categories of task

Category of task set by the CIO



- Completed
- On track
- Minor issues
- Moderate issues
- At risk of non-completion
- Not reported

Notes

- 1 Nine TLBs each report against 32 tasks across these categories (a total of 288 tasks across the TLBs), which are set by the CIO. For this exercise, the Defence Nuclear Organisation and the Submarine Delivery Agency report as one TLB.
- 2 The 32 tasks break down across the categories as follows: data exploitation (4 tasks), reset cyber defence (12 tasks), strategic workforce transformation (3 tasks), strategic supplier management and digital delivery and process improvement (9 tasks), technology (4 tasks).
- 3 The 'data exploitation' task category includes tasks relating to the Digital Foundry and Defence Artificial Intelligence Centre.
- 4 Category totals may not sum to 100% due to rounding.

Source: National Audit Office analysis of Top-Level Budgets’ performance reporting against tasks set by the chief information officer

Delivering common technology

2.12 Defence Digital's Service Delivery and Operations organisation is responsible for supplying and maintaining core digital services and running technology improvement programmes for the Department as a whole. Previously, the ATLAS consortium provided the Department's core digital services through a contract that was let in 2005.¹² In 2015, the Department assessed that its core user experience was unacceptable: its operating system was out of date; users had limited storage and tools for collaboration; and its devices largely did not allow mobile working. As a result, the Department amended the ATLAS contract to progressively roll out upgrades including an improved core IT system (MODNet), new operating systems, new collaboration tools and mobile devices to facilitate home working. This included the roll-out of laptops, which let the Department sustain home working during the COVID-19 pandemic.

2.13 While the Department judges that its core IT is now fit for purpose, it has plans to deliver further user experience improvements. The Department concluded that the contract with ATLAS was too large, insufficiently transparent to understand user experience and lacking the levers to improve services further. For these reasons, it is breaking the ATLAS contract up and procuring replacement services separately. An operational service management team in Defence Digital, created in June 2020, is integrating these services. The new user service desk the Department procured in October 2021 supports this team, by gathering information on each service, to spot common problems. The Department hopes that this greater visibility will allow it to address issues faster, deliver improvements where needed, and manage overall risks to its IT services better.

2.14 Following the introduction of the new service desk there was a fall in service performance, but it has recently begun to show improvement. Its mean time to resolve incidents rose from 290 business hours in November 2021 to a peak of 463 in January 2022 before improving to 210 in July 2022, and it has reduced average service call waiting times from 55 minutes in October 2021 to two minutes in May 2022. Since late 2019, overall customer satisfaction with services has been broadly at or near its baseline target of 80%, with its February–March 2022 survey reporting 84% overall satisfaction. The Department aims to improve this to 90%.

2.15 These improvements to core IT are part of the Defence Digital's portfolio of more than 90 digital projects and programmes, including larger and more complex major programmes. **Figure 6** shows these major programmes and their recent performance. The Department needs many of these programmes to replace fragmented legacy systems and software with newer capabilities that are more secure and will allow the interoperable use of services and data across Defence.

¹² The ATLAS Consortium includes DXC Technology (originally HPE), Fujitsu, Airbus Defence and Space, and CGI. It provided the Department's core IT, including records management, print and a service desk.

Figure 6

The Infrastructure and Project Authority's (IPA's) assessment of Defence Digital's major programmes, March 2022

The IPA's assessment is that successful delivery is feasible for three of Defence Digital's publicly reported major programmes, but appears unachievable for two

Programme	Description	IPA assessment
Next Generation Core Network	Will deliver the core network connectivity for the Ministry of Defence (the Department), including the gateways linking into these networks, which allow data to move between networks at different levels of assurance.	●
SkyNet 6	Will ensure continuity of satellite communication services and secure the UK's satellite communication capability for the future.	●
Land Environment Tactical Communications and Information Systems	Will deliver the next generation of tactical military communications in the land environment, to enable informed and timely decisions.	●
New Style of IT Base	Will work through the ATLAS contract to make the Department's core IT fit for purpose. For example, the Department moved from Windows XP to Windows 7 and has recently rolled out Windows 10.	●
MODNet Evolve	Will move the Department from the single, large, existing ATLAS contract that provides users with core IT services to a new range of replacement contracts for individual services.	●
New Style of IT Deployed	Will deliver a modern and secure communications and information service to connect war-fighters and enable information advantage.	●
Joint Crypt Key programme	Will modernise the Department's communications security tools so that they are better integrated and more flexible, while remaining secure.	●

Notes

- 1 The IPA produces an annual report that assesses the likelihood of government major programmes achieving their aims and objectives on time and on budget. A 'red' rating means successful delivery appears unachievable; 'amber' that successful delivery appears feasible but that significant issues exist requiring management attention; and 'green' that successful delivery appears highly likely with no outstanding issues that appear to threaten delivery.
- 2 The ratings we present are from the IPA's 2021-22 annual report and reflect a snapshot of performance data at March 2022. The ratings do not reflect any changes in performance since that date.
- 3 The ATLAS Consortium includes DXC Technology (originally HPE), Fujitsu, Airbus Defence and Space, and CGI. It provided the Department's core IT services, including records management, print and a service desk.
- 4 The New Style of IT Deployed and Joint Crypt Key programmes are subject to IPA assessment but are exempt from public IPA reporting under Section 26 of Freedom of Information Act 2000 (Defence).
- 5 Defence Digital has an eighth major programme; however, information regarding this has been redacted with consideration to Section 24 of the Freedom of Information Act 2000 (National security).

Source: National Audit Office analysis of Ministry of Defence information and the Infrastructure and Project Authority's Annual Report on Major Projects 2021-22

2.16 Defence Digital's reputation for delivering digital projects and programmes has historically been poor and some TLB CIOs said this was a barrier to integration. Defence Digital's project and programme delivery has suffered from systemic issues including a lack of skilled and experienced personnel, immature project controls and a culture that excessively focuses on the approvals process. TLB CIOs told us that this undermined trust in Defence Digital's work on the strategy and incentivised TLBs to maintain or produce their own separate capabilities for certain requirements, rather than rely on shared ones delivered by the Department.

2.17 In response to these systemic issues, the Department created a reset programme for the Service Delivery and Operations organisation. This involved improvements to project delivery controls such as management information and reporting. They also hired high-priority skilled personnel, including an additional portfolio delivery director.

2.18 The effects of these measures are not yet clear in its performance, which the COVID-19 pandemic has also affected. In financial year 2019-20, it completed 76% of its strategic and significant delivery milestones, but this fell to 57% in 2020-21, before recovering to 78% in 2021-22. As of June 2022, 66% of projects across its total portfolio reported delivery confidence ratings of green or amber-green, a level it has broadly maintained since the end of 2020-21. It has continued to find the delivery of its major programmes challenging; the Infrastructure and Projects Authority publicly rated five programmes for 2018-19, of which four programmes were rated amber-red and one amber, and of the five programmes it publicly rated in 2021-22 three were rated amber, and two red (see Figure 6).¹³

2.19 The Department has further improvement plans. It aims to complete 90% of its strategic and significant milestones each year and for 90% of its projects to be on time and budget by each year end, with 'back to green' plans for its major programmes. The Department has recently reorganised the Service Delivery and Operations organisation so that there are individuals accountable for each service, with the aim of giving clarity to users and improving service delivery. It is also providing further training in project delivery and further improving project delivery controls and reporting.

¹³ In June 2021 the IPA moved from a five-tier delivery confidence rating system to a three-tier one (green, amber, red) and, therefore, does not use the 'amber-green' or 'amber-red' ratings in its 2021-22 reporting. The five programmes it publicly rated in 2021-22 are not all the same as those it rated in 2018-19, as one was not yet on the Government Major Projects Portfolio in 2018-19, and one programme it rated in 2018-19 has since been exempted from public reporting. Across its portfolio of programmes, Defence Digital internally uses a similar rating system that uses amber-green and amber-red as ratings.

Part Three

Strategic challenges

3.1 This part sets out three areas of strategic challenge we feel the Ministry of Defence (the Department) will need to continuously manage to implement the *Digital Strategy for Defence* (the strategy) successfully. These are: funding and efficiencies, digital skills, and the Department's complex organisational structure.

Funding and efficiencies

3.2 The Department had not fully funded its planned digital transformation when it published the strategy in May 2021. Following the 2021 Integrated Review the Department sought £1,125 million over 10 years for digital transformation and £480 million for cyber defence. HM Treasury allocated the Department the cyber defence money in full and £1,040 million for digital transformation, leaving a funding gap of £85 million. However, the type and profile of this funding did not align with the Department's spending plans. While the Department had planned to spend £658 million in the first four years, only £410 million was available, which left a short-term funding gap of £248 million. Separately, funding was only available to create centres of excellence for the Digital Foundry, which it needed an extra £260 million to fully fund.

3.3 In March 2021, Defence Digital considered several alternatives for how it could prioritise digital transformation within the funding available, including delays to data centre rationalisation and some secret capabilities. However, the Department's senior leadership felt the impact of this would be too great and requested further work to explore how it could fully fund all planned activity.

3.4 Following its annual budget cycle that finished in March 2022, the Department considers it has now fully funded £1,840 million for the strategy.¹⁴ During 2021-22 Defence Digital and Strategic Command worked together to fully fund the strategy in future years and address wider financial pressures on Strategic Command. Defence Digital balanced its budget for the 10-year planning period by reviewing and refining its project and portfolio forecast expenditure resulting in a £190 million decrease; committing to find an extra £160 million of efficiencies; capitalising £110 million of resource expenditure; and stopping £60 million of lower-priority work. As part of the annual budget process, the Department prioritised allocating the additional £260 million it needed to fund the Digital Foundry. Although the Department is now confident in its funding position, we have raised concerns in our work on the Department's Equipment Plan that assumptions about reduced costs or efficiencies in future years can build up financial pressure over the longer term.¹⁵

3.5 Defence Digital has formal targets requiring it to find £1,370 million of cash releasing efficiencies between 2023-24 and 2032-33. However, Defence Digital has ambitions to go beyond these and find £2 billion of cash-releasing efficiencies. **Figure 7** shows Defence Digital reported in June 2022 that it forecasts making £1,215 million of cash-releasing efficiencies over the 10-year period.¹⁶ Defence Digital expects to overachieve against the formal target in the first two years by £40 million. Over the 10-year period it aims to find a further £160 million to meet its formal target and £790 million to match its full ambition, which Defence Digital is continuing to work toward. Defence Digital plans to find efficiencies in additional digital transformation projects, create a senior efficiency forum to strengthen assurance and expand and scale efficiencies made by TLBs.

3.6 Defence Digital's planned efficiencies include finding:

- £695 million through strategic supplier management, such as reducing duplication and increasing commercial leverage by buying software licences for the whole Department;
- £326 million by transforming its workforce and replacing contractors with less expensive civil servants (see paragraphs 3.16 to 3.19);
- £183 million through automation of manual business processes; and
- £11 million by reducing the number of physical data centres, through increased use of the cloud.

14 This includes £1,360 million for digital transformation, including the Digital Foundry, and £480 million for cyber defence.

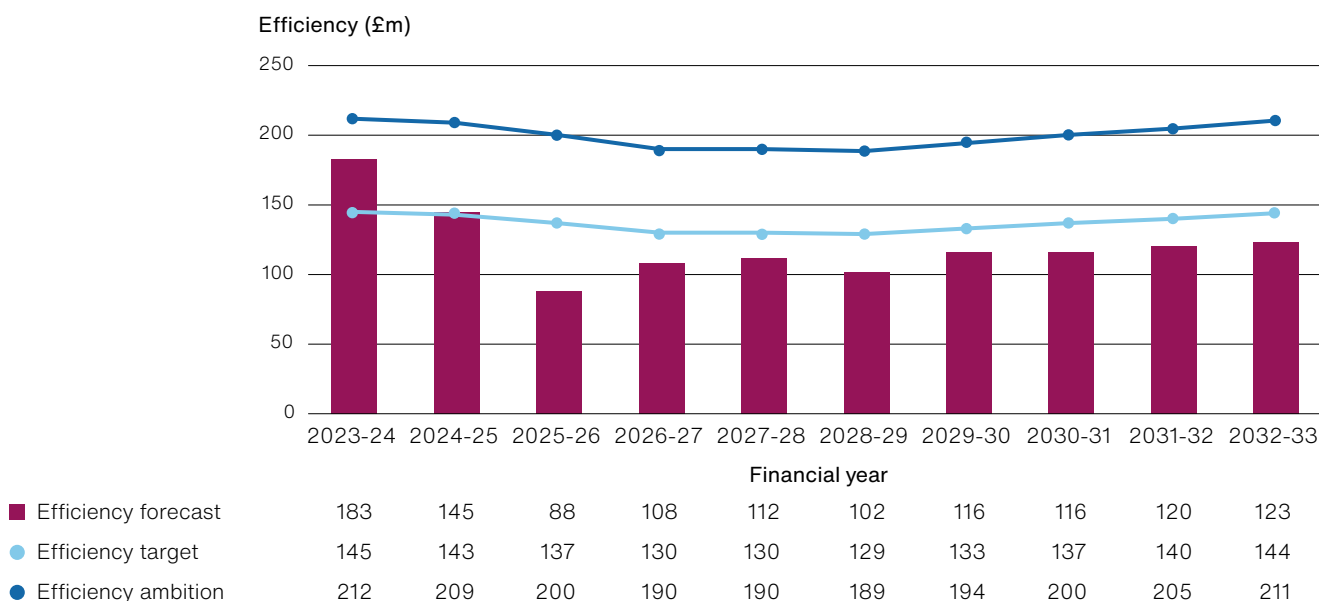
15 Comptroller and Auditor General, *The Equipment Plan 2021 to 2031*, Session 2021-22, HC 1105, National Audit Office, February 2022.

16 Although Defence Digital has identified £2 billion of potential efficiencies, after adjusting for risk in June 2022 it had confidence in realising £1,215 million of these. Defence Digital will continue to review this assessment over time.

Figure 7

Defence Digital's cash-releasing efficiency plans, 2023-24 to 2032-33

Defence Digital expects strong early performance and aims to continue to find efficiencies to meet its target



Notes

- 1 We define cash-releasing efficiencies as efficiencies that directly reduce the Ministry of Defence's budget.
- 2 The 'efficiency target' refers to £1.4 billion of cash-releasing efficiency savings allocated to Defence Digital by the Ministry of Defence, which it is required to make by 2032-33. The 'efficiency ambition' refers to Defence Digital's intent to go beyond this and realise £2 billion of cash-releasing efficiencies by 2032-33.
- 3 The data only include cash-releasing efficiencies, not other types of efficiency, such as cost avoidance or productivity increases.
- 4 Defence Digital does not set out in its routine reporting how it profiles its £2 billion efficiency ambition by year. Therefore, we have apportioned it across the period on the same basis as the efficiency targets.
- 5 The forecast data presented are after Defence Digital's adjustment for risk and represents the value it had confidence in realising at June 2022.

Source: National Audit Office analysis of Defence Digital's efficiency performance reporting

3.7 There is still uncertainty about the forecast value of some efficiencies.

The automation efficiency value is a 10-year estimate based on a small number of current examples. Defence Digital estimates Top-Level Budgets (TLBs) will turn 30% of productivity gains made by automation into cash by reducing the size of their workforces. However, it is not yet clear what workforce reductions TLBs will make.

3.8 Funding of the strategy is not directly reliant on achieving these efficiencies, as the Department could reallocate funds from elsewhere. However, the Department continues to be under financial pressure and finds it challenging to strike the right balance between increasing its capabilities and living within its means. Efficiency savings are an important way the Department can relieve this financial pressure and reinvest in priorities such as digital transformation.

3.9 The Department will likely continue to find it challenging to fund its full ambitions for digital transformation. Although Defence Digital's reviews have lowered project costs so far, this may not always be the case. In October 2022 the Department's Cost Assurance and Analysis Service (CAAS) forecast a 'realistic cost outturn' for Defence Digital's equipment plan programmes that was £1.4 billion (5%) higher over the next 10 years than the delivery teams' estimates. The CAAS 'credible worst-case scenario' cost forecast for the same programmes was £3.7 billion higher (13%).

3.10 There are also evolving demands for funding, for example, data skills capability emerged as a critical requirement after the annual budget cycle closed. Underperformance in finding efficiencies could translate into financial pressure. Inflation has risen significantly since the Spending Review, and there is a risk project costs will rise more than forecast as a result. It is important that Defence Digital continually monitors the affordability of its plans and makes informed prioritisation decisions if financial pressures increase.

The digital skills challenge

3.11 The Department recognised in the strategy that it has critical digital and data skills gaps and has fallen behind in getting the specialist skills it needs. However, there is a digital skills shortage across UK industry and elsewhere in the public sector. Our previous reports on digital transformation and programme delivery show that government experiences poor performance due to this shortage.

3.12 The Department finds it hard to recruit and retain talent. The Department cannot match private sector pay for digital roles, which chief information officers (CIOs) felt was a significant challenge. Government introduced the Digital Data and Technology (DDaT) pay framework with greater flexibility to help departments compete externally for talent and reduce competition within the civil service. However, not all TLBs have authority from the Department to apply pay uplifts for digital specialists, which is creating internal competition – Defence Equipment and Support, for instance, has greater pay freedoms that other TLBs do not have. The Department has recently endorsed the Defence-wide adoption of the DDaT framework and is working on proposals for additional pay freedoms targeted at the critical skills it needs.

3.13 An internal review of Defence Digital identified that technologists do not see the Department as an exciting opportunity for many reasons, including that:

- they see the Department as bureaucratic and slow-moving;
- there is little public visibility of the interesting technology the Department is using and developing;
- the Department's locations are not ideal for hiring talent. Around 60% of Defence Digital people are based in Corsham, where it finds recruiting digital specialists increasingly difficult; and
- hiring and on-boarding takes too long in a competitive labour market.

3.14 The Department's future workplace strategy intends to help recruitment and retention, including by making flexible working the default. Roles with access to sensitive information need security clearance from United Kingdom Security Vetting. In June 2022, the average wait time for a routine 'Security Check' clearance was 44 working days and routine 'Developed Vetting' clearance was 211 working days.

3.15 If the Department does not overcome these challenges then its ability to deliver the strategy will suffer. **Figure 8** overleaf shows how a lack of technical expertise caused problems for the Department's programme delivery. Our wider work across government suggests that based on its current plans, the Department will find it difficult to make progress on this issue fast enough to achieve the full ambition of the strategy at the pace it wants. Our survey of digital leaders across government in 2015 identified the same problems as the Department's internal review in 2021.¹⁷

3.16 To address its skills shortages, Defence Digital put in place a number of workforce initiatives. Its strategic workforce programme, established in April 2020, aimed to transform its workforce over three years through:

- a recruitment campaign to bring in high-priority technical skills;
- investing in training and redeploying people;
- reducing non-digital roles and focusing on the skills it needs for the future; and
- reducing contractor workforce costs and converting contractor roles into civil servant roles.

3.17 The complexity of developing a workforce plan for Defence Digital, while managing emerging requirements, meant this has taken longer than planned. Defence Digital has begun implementing key elements of its plan while it finalises it. By June 2022 it had hired 42 of the 151 people with critical skills that it wanted and was in the process of bringing in 39 more. Defence Digital has 3,090 workers, of whom 570 are contractors (18%). It intends to reduce workforce costs further, through further organisational restructuring and by reducing the cost of contractors.

3.18 Defence Digital's 'Digital Skills for Defence' programme aims to enhance digital skills across the Department for its digital professionals, Defence leaders and its remaining workforce. This follows on from its previous learning initiatives, and it has begun establishing partnerships with industry to assist with this activity.

3.19 Defence Digital has also started to expand its strategic workforce planning approach to TLBs. TLBs have started to complete skill gap assessments, participate in the department-wide education programme, and agree specific skill initiatives where needed. In June 2022, collectively the TLBs reported being on track or facing only minor issues with 74% of workforce tasks for 2022-23. However, TLBs themselves still face issues acquiring skilled people, with the majority of CIOs stating this was a key challenge for their TLB.

17 National Audit Office, *The digital skills gap in government: survey findings*, National Audit Office, December 2015.

Figure 8

The shortage of technical expertise on the MODNet Evolve programme, May 2022

A lack of technical expertise contributed to the Infrastructure and Projects Authority's (IPA's) judgement that successful delivery appears unachievable

Background: The Ministry of Defence (the Department) established MODNet Evolve to move from the large, existing ATLAS contract to a new set of individual contracts, which provide users with core IT services, including future secret capabilities and end user services and devices (EUS).

The skills challenge: The IPA's May 2022 review gave MODNet Evolve a delivery confidence assessment of red, meaning that successful delivery appears unachievable. One of the biggest risks to the programme it identified was resourcing and technical expertise. The review identified these as critical issues because of multiple vacancies, resignations, a heavy reliance on contractors, and Department staff often being asked to take on roles they did not have the experience for. The IPA recommended that the Department urgently strengthen the programme's technical resource, arguing that if left unresolved, the programme would fail to deliver future secret capabilities and EUS.

Note

- 1 The ATLAS Consortium includes DXC Technology (originally HPE), Fujitsu, Airbus Defence and Space, and CGI. It provided the Department's core IT services, including records management, print and a service desk.

Source: National Audit Office analysis of Infrastructure and Projects Authority reporting

The Department's organisational structure

3.20 The Department is a large, complex organisation with many constituent parts, and the CIO and Defence Digital do not have all the levers needed to deliver the strategy. The CIO is accountable for the whole Department's use of technology and data, leading the digital function and implementation of the strategy, but only directly controls Defence Digital and its £2.7 billion of spend, against the Department's estimated £4.4 billion of digital spend in 2021-22. The CIO and Defence Digital, therefore, must influence the rest of the Department through working with TLB CIOs and the digital function. This includes delegating functional tasks through to TLB CIOs and setting 50% of their appraisal objectives. However, TLB CIOs also need to deliver digital capabilities for their own organisation's priorities and some CIOs felt they still needed greater authority over digital activity even within their own TLB.

3.21 Defence Digital sits within Strategic Command, meaning its strategic decisions and financial management are subject to oversight from Strategic Command, which has other priorities to consider and manage. For example, Defence Digital had to work with Strategic Command in the 2021-22 annual budgeting cycle to help address wider funding shortfalls, alongside efforts to fully fund the strategy. The CIO must work with Strategic Command if they want to redeploy resources across Defence Digital. This is because Defence Digital commits most of its expenditure to Equipment Plan programmes, which are managed through a different funding path within Strategic Command from the rest of Defence Digital.

3.22 There are business changes needed to realise the strategy, which the wider Department will need to deliver. For example, the Department's approvals and acquisition processes are unsuited to the faster, more iterative approach favoured in technological change. This has been a factor in slowing some digital delivery and can mean that technology is out of date by the time the Department delivers it. The Department recognises this and its acquisition and approvals transformation portfolio includes the Technology Exploitation programme, which is trialling the use of agile project delivery methods to assess their feasibility. However, the Department needs to do further work before it can adopt these methods and guidance.

3.23 The Department acknowledges that Defence Digital and the digital function need more support to deliver the strategy. The Department's four most senior officials¹⁸ commissioned an independent review in February 2022 into how transformation across Defence is prioritised and governed. They now view digital transformation as wider than Defence Digital's existing work and concluded that trying to influence the wider Department through the digital function is not enough. They are now examining how they might build on this as part of a wider agenda to exploit digital for wider defence objectives.

18 The chief of defence staff, vice-chief of defence staff, permanent secretary and second permanent secretary.

Appendix One

Our evidence base

1 This report examined the effectiveness of the Ministry of Defence's (the Department's) implementation of *The Digital Strategy for Defence* (the strategy). Our objectives were to:

- provide greater clarity of the Department's digital landscape to parliament and the public;
- improve transparency and public accountability for the Department's performance in implementing the strategy, as well as delivery of its major digital programmes; and
- influence the Department to maximise value for money from its digital activities.

2 We collected our evidence between 14 November 2021 and 18 August 2022 and analysed it between 15 November 2021 and 19 August 2022.

3 We focused our scope on digital activity and change within Defence, especially those activities which the Department highlighted as being vital to the objectives of the strategy. Our main sources of evidence were:

- Defence Digital, as the enabling organisation for digital within Defence;
- the Department's digital function, as the community of digital professionals responsible for policy and delivery; and
- other digital activity across military commands and organisations.

Our analysis and conclusions are based on this evidence base, together with insights from our wider digital work across government.

Interviews with the Department's chief information officers (CIOs)

Selection and recruitment

4 We interviewed all 16 of the Department's CIOs from across Top-Level Budget (TLB) organisations, and other Defence organisations, to gather their views of the strategy and challenges to its implementation. Some TLBs and organisations have more than one CIO, for example, where they oversee Defence-wide functions such as people or support.

Fieldwork

5 We conducted the interviews using online calls, which were sometimes attended by additional members of the CIO's team. We conducted the interviews between 22 April 2022 and 7 June 2022.

6 We created a list of questions to keep our interviews consistent and provide coverage of the full range of relevant issues. The themes we sought the CIO's views on through these questions were:

- the CIO's role, responsibilities and the digital landscape and activities within their TLB or business unit;
- programme delivery and performance;
- the Digital Strategy for Defence and their alignment to it;
- how progress with implementing their own digital activities is measured and monitored including governance arrangements;
- how effective Defence Digital is and their experiences of working with Defence Digital; and
- the key business challenges they face across the strategy's themes of people, technology, process, data and cyber.

7 Although we used a consistent set of questions, the extent to which we covered each varied between interviews, depending on what each CIO felt was most relevant to their organisation and role.

Analytical approach

8 We organised our interview notes by theme in Microsoft Excel. Using this approach, we were able to determine varying degrees of consensus among the CIOs against the themes listed above. We used this summary analysis as evidence to support points of detail in the report, such as how the strategy is regarded across Defence and the extent to which the Department is aligned with its objectives.

Interviews with wider stakeholders

Selection and recruitment

9 We worked with the Department to speak to a wide range of stakeholders that were representative of the work of Defence Digital and the wider digital function to implement the strategy. This included the Department's CIO, and the second permanent secretary in their role as the Department's digital champion.

Fieldwork

10 The interviews and briefings took place between 15 February 2022 and 13 July 2022 via a mixture of online calls and in-person site visits and covered topics including:

- Defence Digital's largest programmes;
- progress implementing the strategy so far;
- challenges faced by the Department;
- the funding and efficiencies position; and
- efforts to cohere and strengthen the digital function.

Analytical approach

11 We collated each interviewee's notes under broader themes and used the interviews to guide further lines of enquiry.

Document review of background material

Focus and purpose

12 We reviewed a small initial range of departmental documents to assist with defining the parameters of the audit and deepen the study team's understanding of the strategy. This included a review of:

- business cases;
- governance documents;
- strategy papers; and
- guidance documents.

13 Our review of this initial material was carried out between 14 November 2021 and 6 January 2022. Documents reviewed covered the period between June 2020 and October 2021.

Analytical approach

14 We reviewed each document against our overarching audit questions. The review was used to refine the scope of the study, including defining our more detailed audit questions and methods.

Systematic document review

Focus and purpose

15 During the fieldwork stage, we reviewed further departmental documents to assess the Department's implementation of the strategy and the performance of its major digital programmes. Documents reviewed covered the period between July 2015 and August 2022. This included a review of:

- business cases;
- board meeting minutes;
- risk assessments;
- internal and external assurance and evaluation reports;
- guidance documentation;
- performance monitoring dashboards;
- financial documents;
- governance and organisation structure documents; and
- letters and internal correspondence.

Analytical approach

16 We reviewed these documents against themes which were chosen based on the Department's categorisation of the parts that form the strategy and our framework, which was derived from our Digital Hub's framework for digital transformation.

17 Our analysis was related to performance of programmes with a particular focus on governance, management, skills and people resource issues, dependencies, legacy and obsolescence, data, supplier and commercial issues, and scope and timetable. Given the importance of cloud technology for the digital 'backbone' and cyber security and resilience for the strategy's 'Secure by Design' principles, we included these as separate themes. Our analysis was used to:

- inform further discussion and follow-up with the Department; and
- triangulate findings from other sources, including interview and case study data.

This report has been printed on Pro Digital Silk and contains material sourced from responsibly managed and sustainable forests certified in accordance with the FSC (Forest Stewardship Council).

The wood pulp is totally recyclable and acid-free. Our printers also have full ISO 14001 environmental accreditation, which ensures that they have effective procedures in place to manage waste and practices that may affect the environment.



National Audit Office

Design and Production by NAO Communications Team
DP Ref: 011076-001

£10.00

ISBN 978-1-78604-449-5



9 781786 044495