Ministry of Defence

Digital & Information Technology Functional Strategy

Building Transformative Digital & Information Capability

V1.01

January 2019

Contents

Executive Summary

The effective exploitation of information and the systems that manage and process it are vital enablers of both operational advantage and business transformation. We are already using Digital and Information Technologies (D&IT) to support both, but there is always room for improvement. This document sets out how the establishment of a CIO-led D&IT Function will enable the changes that are needed, and the next steps on the transformation journey.

STRATEGIC DIAGNOSIS

MOD has come a long way in recent years in successfully updating its outdated IT systems and introducing the industry-standard Office 365 suite. We must continue to enable users to exploit new ICT services and tools as they are introduced. There remain too many different, unconnected systems, of non-standard design that are difficult and expensive to maintain, often running highly bespoke and costly software. D&IT is a central enabler in the operational space and must receive adequate funding. Skills must continue to be developed in the D&IT community across Defence and we must fully and efficiently exploit the external D&IT market.

VISION AND BENEFITS

The D&IT Function is needed:

> *To create transformative Digital and Information capability that enables sustainable military and business advantage, that is secure, integrated, easy to use and delivered at scale and pace to the Front Line.*

Of chief importance to achieving the vision and addressing the current gaps is to:

- Establish a set of **stronger functional governance mechanisms** that will improve coherence across the planning, investment and operation of our ICT and the information services they enable;
- Gain a **materially improved understanding through accurate Management Information** on the operation of our current ICT portfolio, to guide priority interventions and future investment plans;
- Build a **stronger, more unified and better integrated professional cadre** across the broad D&IT community, focussed on clear principles, priorities and goals; working alongside professionals in other Functions (notably Commercial).

This D&IT Functional Strategy is based on three critical principles:

- **Cohesion** – consistent architecture, standards and management processes;
- **Integration** – digital services and products that connect, integrate and share data by default, allowing information to flow seamlessly to the point of need;
- **Speed and Adaptability** - meeting user needs quickly; improving services wherever possible.

The Function will generate significant improvements in the following **Strategic Priority** areas:

- **Digitise the battlespace** – integrating existing and new information capabilities to achieve better interoperability, the decisive advantage that timely, data led decision-making will give the operational commander. A critical enabler for this plan is that MOD continues to move towards a single integrated D&IT system with strong cyber protection and ‘open architecture’ design that moves us from being platform centric to information centric.
- **Responsive cyber defence** – providing robust, and responsive cyber defence against an ever-evolving threat to ensure that our operational and business systems can perform resiliently, efficiently and reliably.

- **Promote information led wider business transformation** – working with other Function Owners to simplify and automate their processes; leading the technology contribution to the modernisation of effective Defence business. Simpler, more effective and cheaper processes will allow staff to be employed more efficiently and allow savings to be reinvested towards the front-line.
- **More effective and efficient IT services** – providing better and more relevant services that are intuitive and easy to use. Fundamentally reconfiguring our D&IT processes to allow us to design and deliver information systems and services faster, make better use of industry partners and transform our operational performance.
- **Set up a capable and cohesive function** – build a single, connected function with the right skills and work environment, changing how we are organised and working more closely with users to design, build and operate the capability we need. This will improve staff satisfaction, retention and quality.

These strategic priorities will also generate immediate improvements to critical Defence initiatives, including supporting Transformation priorities for other Functions, and addressing known service-delivery issues.

IMPLEMENTATION

To realise this Strategy, CIO, as Function Owner will direct future D&IT design, investment and operation across MOD. This includes authority over technical architecture, policies and standards, IT operating processes and material D&IT investment proposals, to ensure pan-Defence consistency and strategic alignment. To help build a more capable professional D&IT cadre, CIO will be engaged in making D&IT related senior appointments across MOD.

To support, inform and guide the exercise of these authorities, a D&IT Coherence Board will be established, comprising Top Level Budget (TLB) CIOs, the D&IT Function COO, Directors of Cyber Defence and Digital Enablement, and CEO ISS.

The D&IT function will work with colleagues across Defence to exploit technology and turn Defence into a data driven organisation. The CIO will achieve this by challenging pan-Defence functions to simplify, standardise and align their policies and processes, to better exploit commercially available technology wherever possible.

Over the coming months, the D&IT Function will take the steps needed to stand up. In parallel, a comprehensive transformation programme will be designed and set up to meet our strategic priorities, and the necessary underpinning capabilities. This will move MOD decisively towards becoming a truly data-driven organisation, that is constantly alive to, and in tune with, the transformative potential of D&IT.

1. Introduction: a function fit for tomorrow's challenges

As the Chief Information Officer for the MOD, I am pleased to introduce our Digital and Information Technology (D&IT) Functional Strategy. It describes how, as Function Owner, I will lead the people in the Function and their ways of working. It complements the Defence Information Strategy, which is now being revised and updated to fully set out the capabilities we need, and the ways, ends and means through which they will be achieved.

Defence has an ambition to put modern digital capability at the heart of how it operates to create winning advantage. This is driven by an underpinning premise that emerging digital technologies together with the effective capture, analysis and use of information will enable transformative military and business performance.

This strategy outlines our approach to ensure that we can realise this ambition and fully exploit the opportunities afforded by the transformative nature of emerging digital capability.

To do this requires a bold mind-set that challenges the way we operate and recognises that success requires fundamental change and will not be achieved by just doing the same things better. Meeting the needs of Defence in the future hyper-connected digital society will require a cohesive and joined-up Function; the efficiencies and effectiveness we seek lie in building digital and information capability that integrates across existing internal and external boundaries in Defence. By creating new levels of teamwork, we can create value-based outcomes that achieve better performance and competitive advantage over our adversaries for each individual part of Defence. My aim is to create a Function where the digital and information outcomes are much greater than the sum of the parts.

The Functional Strategy, in service of this intent, describes the objectives and enabling steps we need to take, building on the existing solid foundations of D&IT. It also describes a revised operating model that will support the achievement of our objectives.

Ensuring that we have the right people, right skills and teamwork is critical to Defence's future success and we will establish a clear workforce strategy to attract, develop and retain the talent we need. We will continue to ensure a diverse and inclusive working environment making this a great place to work and develop careers.

This is truly an exciting time to be part of the D&IT Function inside MOD. Breath-taking technology is being developed at an unprecedented pace. Defence's strategic intent to exploit it means the D&IT Function plays a critical role in enabling its adoption and use. I am proud to be part of it, and I look forward to helping grow the already impressive contribution D&IT has made to UK Defence and to working with colleagues inside the Function and across Defence to achieve our vision.

Charles Forte

DG and CIO, D&IT Function Owner

2. Defining the D&IT Function

The Digital and Information Technology (D&IT) Function is the team which directs, acquires and controls our D&IT equipment and services. The scope of responsibility for the function is to provide technology for Defence ranging from the battle-space to the business space. The D&IT Function in Defence is aligned to the wider Government Digital Service (GDS) and the relevant government policies of the Department for Digital, Culture, Media and Sport (DCMS).

The total spend over the next 10 years is estimated to be £37Bn[1] and the opportunities afforded by emerging digital technologies will continue to drive up demand. Taking best advantage of these opportunities requires new levels of teamwork across the Function and the whole of Defence. It also drives the need for clear strategic intent, prioritisation and efficient use of resources.

Figure 1. The reach of the D&IT Function

D&IT services are acquired and managed through life by over 3,000 professional specialists in the D&IT profession[2]. The community of interest for D&IT reaches wider as shown in Figure 1. Successful exploitation of information requires the emergence of the 'digitally savvy' workforce and the D&IT Function will play a role in providing people across Defence with the skills and expertise they need to operate safely in this new world, protecting confidentiality, integrity and availability by building new skills and following the rules of use.

This document outlines how the Function will exploit the benefits of emerging digital capability, how we will undertake that journey and how the Function will work across Defence to achieve these outcomes.

[1] Modernising Defence Programme estimate, 2018.
[2] This estimate is of Knowledge & Information Management (KIM), Digital, Data and Technology (DDaT) and Cyber Security professionals across Defence; the figure may be higher. Work is underway to refine this estimate.

3. Strategic Outcomes and Objectives

The strategic intent for the D&IT Function is:

> *To create transformative Digital and Information capability that enables sustainable military and business advantage, that is secure, integrated, easy to use and delivered at scale and pace to the Front Line.*

The role of the D&IT Function is to harness the potential of new technology and, in close partnership with our colleagues across Defence, to deliver capabilities and new ways of working that match the increasing speed at which the world is moving. This is consistent with the aims of the GDS, DCMS and the associated Government Transformation Strategy.

3.1 The Case for Change

Our adversaries are rapidly expanding their information capabilities and if we are to sustain a competitive response we have to accelerate our ability to access and deploy game-changing technologies.

It is clear that:

- **Data needs to be easy to access, exploit and defend.** A common technical architecture and IT operation standards are needed to drive down costs, increase speed by which we deliver new solutions and to support the information exploitation and cyber capabilities that we want.

- **IT service quality must be consistently up to standard.** A Defence-wide IT operating environment supporting simple, standardised processes is needed to service Defence needs, at the speed that we should expect.

- **Costs must be minimised.** A single operating model that engages the market with one voice is a pre-requisite to achieve market competitive cost points. Simplifying requirements will also be fundamental.

- **We must achieve greater functional cohesion.** We need to work as an aligned function to a common strategy that will allow users to experience the speed and agility of service that they need and to benefit from the latest cutting-edge technologies.

Measures are being taken to address these challenges, but there is a need for a step-change. Establishing the D&IT Function is an essential step to achieving this. It will provide the CIO, as Function Owner, with the formal accountabilities and authorities to drive the necessary transformation.

3.2 What We Need to 'Dial-Up' – Three Critical Principles

To achieve our ambition, those in the D&IT Function must think and operate differently and this is encapsulated in three critical principles that will underpin how we will work:

Cohesion	Integration	Speed and Adaptability
We will act as one Function with the mechanisms to ensure that we work to a shared game plan, with clear accountabilities, working to a consistent architecture, standards and management processes.	We will design and produce digital services and products that connect, integrate and share data by default. This will act as a multiplier on effectiveness and allow information to flow seamlessly to where it is needed - internally and externally, including with other government departments and our allies.	We will continually seek to improve the speed at which user needs are turned into deliverables at scale. Opportunities will be taken, whenever possible, to adapt, modify and improve existing programmes and services to better meet customers' needs.

Table 1. Three Critical Principles

These principles will help the Function respond to the pace of external change, enable connected capability and operate to the new levels of teamwork required.

3.2 Five Enduring D&IT Goals

The D&IT landscape across Defence is complex; to enable us to realise our intent, we will focus on five enduring goals as summarised in Table 2.

Digitise the Battlespace	Responsive Cyber Defence	Promote information-led wider business transformation	More effective and efficient IT services	A Capable and Cohesive Function
Integrating existing and new information capabilities to achieve interoperability, the decisive advantage that timely, data-led decision-making will give the operational commander.	Delivering robust, and responsive cyber defence against an ever-evolving threat to ensure that our operational and business systems can perform resiliently, efficiently and reliably.	Working with other Functional Leaders to simplify and automate their processes; leading the technology contribution to the modernisation of Defence business.	Transforming support to all aspects of Defence business, by providing better services, fundamentally reconfiguring our business and operational processes to allow us to make maximum use of up-to-date commercial software, and better contracting with industry.	Build a single, connected function with the right skills and work environment, changing how we are organised and working more closely with users to design, build and operate the capability we need.

Table 2. The Five Enduring Goals

3.2.1 Digitise the Battlespace – 'Information Advantage and Interoperability'

"Information, in all its manifestations, must change the way we execute business and prosecute warfare, both at home and overseas in an era of constant competition. Information is no longer just an enabler, it

is a fully-fledged lever of power, a critical enabler to understanding, decision-making and tempo, and a means of achieving potentially decisive influence. To regain the initiative and achieve information advantage we must rapidly up our digital game, fundamentally shift the way we think, act, invest, and move with pace through the incremental development of new capabilities"[3]

The desired outcomes are as follows:

- Enabling decision support for the war fighter.
- Understanding and demonstrating what Information Advantage and interoperability technologies are possible. Translating this knowledge into options and requirements to improve capabilities and to enable their successful delivery.
- Interoperability, communication and information sharing as a default. This includes enhancing connection at Official and Secret to our partners across government and international allies to enhance Fusion Doctrine.

These outcomes will be achieved by the following activities:

- Strengthening work in support of transformational military capability, including improving the teamwork across the Function and with stakeholders including Financial & Military Capability in Head Office and Directorate of Joint Warfare.
- Resourcing the Information Advantage initiative to strengthen the digital and specialist contribution and to accelerate the creation of options and delivery of information capability.
- Improving interoperability by adapting existing programmes and creating options for both short and medium-term intervention.
- Moving towards a single integrated D&IT system with strong cyber protection and 'open architecture' design; wherever possible running up-to-date industry-standard software (enabled by simpler processes) at lower cost and with greater resilience.
- Building Centres of Expertise in game-changing technologies and using them to coordinate action.

3.2.2 Responsive Cyber Defence – 'Resilience and Confidence'

Our digital and information environment must assure the confidentiality, integrity and availability of our data and our platforms. The threat is increasing and will continue to do so. Protection requires a holistic understanding of our estate and an ability to anticipate, sense and respond to threats. We will work increasingly in partnership across Defence, across government, industry and with allies. Our risk assessments and actions will be executed end-to-end.

The desired outcomes are as follows:

- An intelligence-led approach to anticipate and respond to risks across all operational domains.
- Resilience in the face of attack and strong protection against the exfiltration of information.
- A strong information security culture where everyone knows how to operate safely.
- Robust cyber defence throughout the supply chain.

These outcomes will be achieved by the following activities:

- Improving monitoring and sensing of network activity and building faster responses including through partnerships with Defence Intelligence and agencies.
- Streamlining and modernising secret and above communication and data handling services.
- Educating Defence people on safe cyber security practices and behaviours and setting compliance expectations.
- Building a stronger and more resilient infrastructure, addressing immediate exposures from obsolescence and process gaps.

[3] JCN 2/18, Information Advantage dated Aug 2018.

- Getting a greater understanding and improved management of cyber risk in the supply chain, including contracting for embedded assurance processes.

3.2.3. Promote Information-Led Wider Business Transformation – 'One Process – One System'

There is a big opportunity to simplify, standardise and automate core business processes leading to significant improvements in both effectiveness and efficiency. The complexity of the current D&IT portfolio limits the ability to access and effectively use the underlying information and generates high administrative operational costs. In modernising the portfolio, we will drive towards a common process with a single system under strong functional stewardship; in doing so, to automate to remove manual processing and free up resource for more value-adding activity. Our intent should be to drive towards the simplicity of 'one process – one system' and to establish a preference for 'software as a service' solutions to simplify and allow Defence to focus on integrating and exploiting information.

The desired outcomes are as follows:

- Modernised, standardised and effective business support processes where front-line resource is free from restrictive administrative work to concentrate on value-adding activity.
- A single information architecture that enables integration, analysis, exploitation and fast decision-making.
- Information that is routinely accessible and used by everyone to provide insight that enables understanding and action.

These outcomes will be achieved by the following activities:

- Simplifying D&IT processes and exploring the degree to which they may be automated.
- Working with other Function Leaders to simplify and automate their processes; leading the technology contribution to the modernisation of effective Defence business processes, so information enables insight and decision-making.
- Maintaining a strong contribution within the Business Transformations.
- Making data available and giving people the standards and tools to use it effectively. In partnership with other functions, we will take steps to improve data ownership and reliability.

3.2.4. More Effective and Efficient IT Services – 'IT Delivery and Operational Excellence'

D&IT capability underpins all aspects of our operational and business activity and is increasingly critical to how we work in real time. As a result, we must ensure we provide services and capability that are easy to use, relevant to how they are used in a 'business' context, available when needed, at appropriate price and quality points. This goal will focus on how the Function evolves internally to increase its ability to meet these challenges.

The desired outcomes are as follows:

- Customer-centric processes and capability.
- Relevant services that are intuitive and easy to use.
- Operational processes that allow us to design and deliver information systems and services faster, make better use of industry partners and transform our operational performance.
- Operational integrity that provides reliability against clear quality expectations.
- Cost to serve that maximises the available supply side economy of scale benefit, including exploitation of G-Cloud and government shared services.

These outcomes will be achieved by the following activities:

- Developing the TLB D&IT plans in line with this Strategy.
- Moving to a shared services delivery model to maximise efficiency and improve service performance.
- Establishing Defence-wide Service and Integration Management.
- Rationalising data centres and building common hosting platforms.
- Creating visibility and transparency of the D&IT portfolio, including costs and performance reporting.
- Improving MODNET service functionality and performance.
- Establishing a realistic and achievable plan, backed by benchmarking, to drive economy of scale benefits and assurance that the whole portfolio link effectively in support of agreed strategic outcomes.
- Working in partnership with the Commercial Function to improve agility and speed.
- Addressing IT Supply Chain efficiency and strategic supplier management.

3.2.5. A Capable and Cohesive Function – 'Greater than the Sum of its Parts'

We will work as a connected and single function with access to the right skills, qualifications and experience necessary to meet tomorrow's operational challenges. A connected D&IT community with a shared management process will ensure greater consistency in how accountabilities are defined and executed. We will update the Defence Information Strategy to support Defence ambitions and to strengthen coherent capability delivery. The challenge to find specialist skills in a competitive market is increasing and we need to improve how we build our brand to attract and retain the right people and to use them effectively, exposing them to cutting-edge programmes to enhance their personal development. We will create a diverse workforce and an inclusive working environment.

The desired outcomes are as follows:

- A single Function Strategy (this document) driving and enabling pan-Defence and TLB outcomes.
- The right people, with the right skills, qualifications and expertise in the right environment.
- Common ways of working, including standards and processes for the design, build and operation of D&IT across Defence.
- An effective supplier eco-system that gives access to specialist skills and expertise.

The outcomes will be achieved by the following activities:

- Recruiting the Office of the CIO team.
- Positioning ISS within the Defence Operating Model (DOM) and JFC Review.
- Establishing a strong D&IT leadership cadre across Defence and working to common objectives.
- Establishing a D&IT Coherence Board.
- Developing and maintaining a Strategic Workforce Plan that identifies and builds the in-house specialisms we need and buys complementary resources from industry partners in a strategic way.
- Addressing Portfolio, Programme and Project Management (P3M) capability gaps.
- Developing a diverse workforce and an inclusive working environment.

3.3 Enabling Objectives

A set of enabling objectives form the plan to stand up the Function. These link back to the strategy, principles and goals.

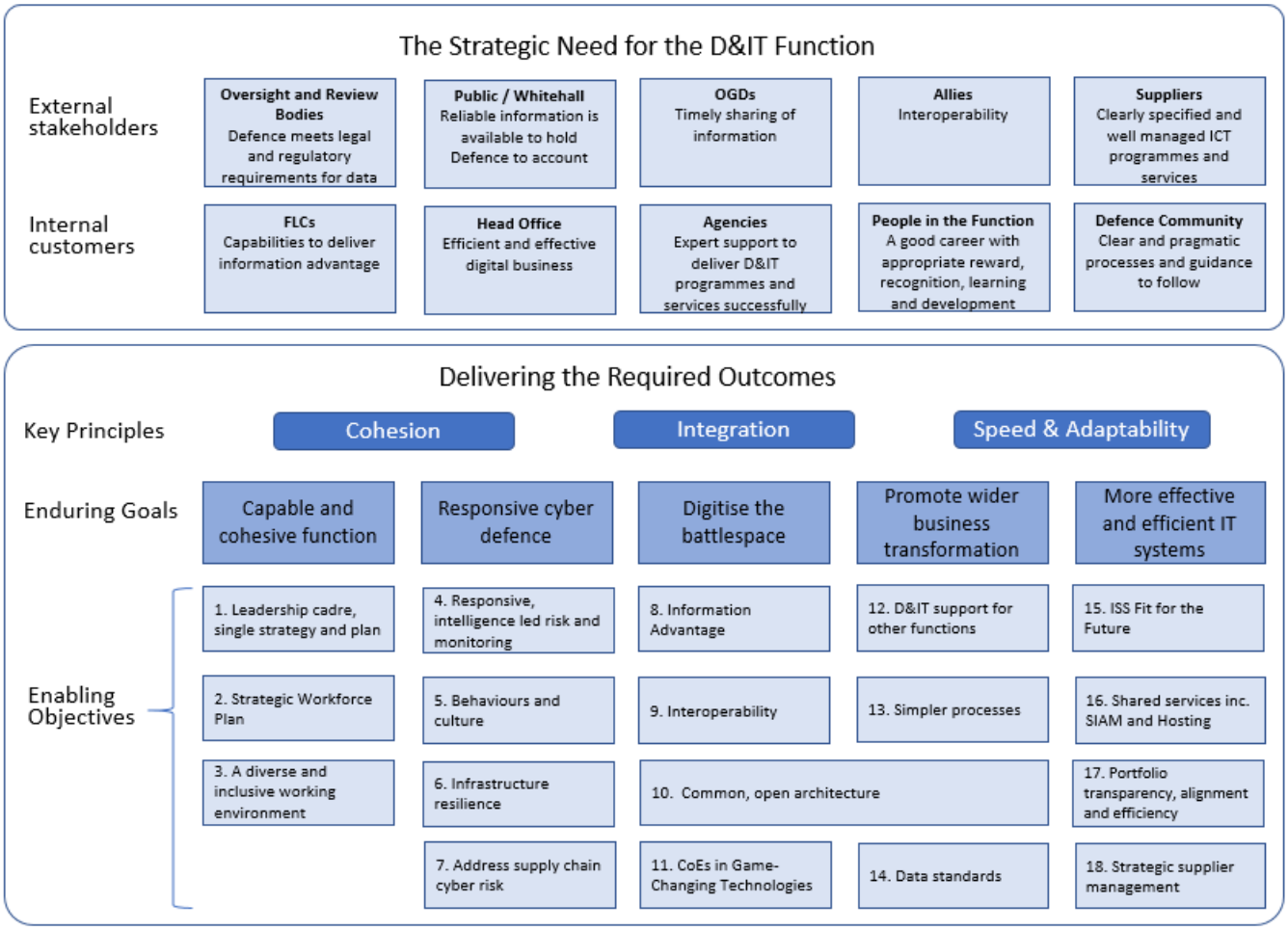

Figure 2. Linking strategy to outcomes

These 18 objectives will be the basis of the first phase of our functional journey. Each one will have an owner who will be accountable for creating the plans, engaging the right community across defence and for achieving against it.

4. Benefits and Measures of Success

The forthcoming D&IT Function Plan will set out in more detail the KPIs and measures of success for meeting this Strategy. Not all will be directly measurable, as the effect of this Strategy will reach across every part of the Department in the capability, effectiveness and efficiency of our military and business operations as measured in the outcomes of the TLBs.

Properly implemented, the vision will provide the following benefits.

Strategic Priority	High level benefit
Digitise the battlespace	*Military operation effectiveness* Improved decision support and more effective C2 by providing operational commanders (at strategic, operational and tactical levels) with better interoperable systems and access to quality real-time information, intelligence and analysis.
Responsive cyber defence	*Reduced risk of loss of sensitive data* Reduced risk of the loss of sensitive data, from more effective protection of critical information assets, early detection and faster response to attack.
Promote information led wider business transformation	*Business effectiveness* Simpler, more effective and cheaper processes used by other functions (Support, HR, Finance, Commercial etc) freeing staff and allowing savings to be reinvested towards the front-line. Information and analysis providing greater insight and better, quicker decision-making at all levels.
More effective and efficient IT services	*Service quality and customer experience* IT efficiency: a reduction on IT run costs can be generated progressively over 3 years, and fewer cost and schedule over-runs on projects and programmes. Service reliability and quality: a reduction in IT Severity 1 incidents and a reduction in business lost time from systems outages – achieved progressively over 3 years.
Set up a capable and cohesive function	*Staff satisfaction, retention and quality* Staff satisfaction, retention and quality. An improved brand and career will attract and retain better people and cutting-edge programmes will further build skills. A D&IT Function investment portfolio that is aligned with Defence priorities.

Table 3. Benefits of the D&IT Strategy

5. Functional Accountabilities and Authorities

This version of the Function Strategy proposes the following accountabilities and authorities that the Function, and the CIO as Function Owner, will exercise. These will be consulted, refined and agreed by the next iteration in 2019.

5.1 Accountabilities

Exploit Digital Technologies:

- Lead the creation and maintenance of a Defence Information Strategy in support of clear transformative outcomes in deployed and corporate domains. (Defence task 25.g).
- Ensure relevant TLB plans are consistent with this strategy.
- Enable digital innovation and transformation.
- Advise the Defence Board on D&IT opportunities and issues.

Cyber Defence and Information Risk:

- To ensure the cyber defence risks are identified and are appropriately mitigated.
- To work with the Functional owner of Defence Security to set Policy in this area.

IT Reliability and Quality:

- Ensure the operational integrity and reliability of systems and services, including locally-owned infrastructure, applications and tools.
- Establish a common technical architecture and operating processes, defining the supporting standards and ensuring compliance.

Functional Efficiency and Effectiveness:

- Maintain visibility of the D&IT portfolio of activity, resources and costs to ensure the function operates efficiently and accesses appropriate economy of scale.
- Ensure D&IT works effectively with other functions, the DOM and GDS.

Skills and Capability: Ensure the function has the right leadership, skills and expertise.

5.2 Authorities

In support of these accountabilities the function will have specific authorities and levers to ensure the strategic intent and supporting goals/ objectives can be met. The CIO will hold the following authorities:

Strategic Alignment:

- To lead the senior D&IT community to ensure effective alignment of D&IT activity with strategy.
- To hold TLB senior leaders to account for meeting in year objectives in service of strategy.
- To review and approve all D&IT investments to ensure alignment with strategy, architectures and standards. This will include the authority to drive D&IT strategic outcomes through the other functions in Defence (including acquisition).

Information and Cyber Risk:

- To lead the CIO and Senior Information Risk Owner (SIRO) community to ensure relevant risks are identified, assessed and mitigated.
- To be the Defence SIRO.

Technical Architecture, Policies and Standards:

- To define and set the common information and technical architecture and standards.
- To ensure new D&IT services are compliant.

ICT Operating Process:

- To define and set the D&IT service integration and management operating processes.
- To ensure these are consistently applied in all TLBs and stop activity the does not align with the standardised ICT.

Functional Skills and capability:

- Senior appointments: to be involved in the shaping of the role, the recruitment process and in approval of the appointment of SCS and military equivalent roles in the D&IT function.
- Training and professional development: to set the standards and define the professional development goals and programmes that will provide the skills we need.

5.3 Checks and Balances

The CIO will be subject to the following checks and balances:

- Held to account by Permanent Secretary (Perm Sec) and Commander JFC against the outputs in this Functional Strategy at the Defence Information Steering Committee (DISC).
- Formal consultation and engagement across Defence on the development of the Functional Strategy and associated implementation plan.
- Annual assurance review of the Function by Defence Audit, Risk and Assurance.
- CIO attendance or representation at the Transformation Board and Functional Leadership Steering Group (FLSG).
- CIO attendance or representation at the Defence Technology and Innovation Board.
- COO oversight of the coherence of the Function with other Functions, through the FLSG, and compliance with DOM.
- Continuous contact at many levels within the CIO organisation and wider Defence.

6. The Functional Operating Model

The Target Operating Model for D&IT across Defence will provide the people, processes, organisation and performance framework to realise the five themes in this strategy.

6.1 Three components

To enable this Strategy and to fill the anticipated roles and responsibilities of the D&IT Function, the Operating model will be developed around three components:

- Office of the CIO.
- Shared Services.
- TLB CIOs.

The capabilities and services in each area may be organised as in Figure 3.

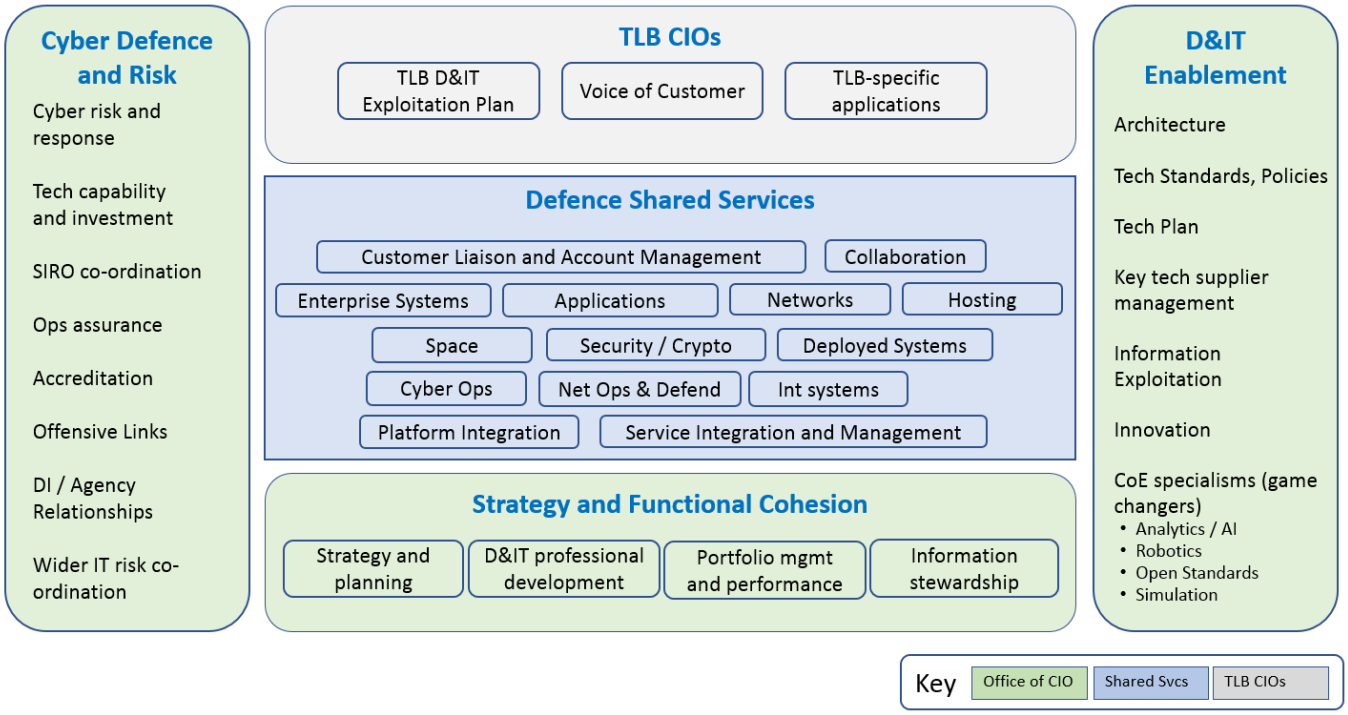

Figure 3. The proposed D&IT Functional Operating Model

The **Office of the CIO** will provide the core connecting mechanisms (shown in green in Figure 3) and will create leadership in the following areas:

- Digital enablement – to lead on technology architecture, standards and to play a leadership role in driving the adoption and exploitation of emerging technology. Centres of Excellence (CoE) to drive game-changing technology will be housed, led and co-ordinated from the centre including where 'virtual' teams are established across the wider organisation to be close to the customer. Their aim will be to pilot, prove, industrialise and deploy new technologies.
- Cyber defence and risk – to lead the strengthening of cyber Defence and to maintain an integrated view of risk and assurance. It will lead on wider D&IT risk identification and response.
- Information stewardship – to lead knowledge and information management across the department.
- Strategic and functional cohesion – to maintain a clear functional strategy, implementation plan, options and roadmaps and to provide a lead on optimising supply side economy of scale; to

manage performance across the D&IT portfolio; to develop suitability qualified and experienced personnel; and to link with other defence Functions and the wider GDS and DCMS.

The **TLB CIO teams** will:

- Drive the Digital transformation of their TLB. As an integral part of the CIO's Functional Team, the TLB CIOs will support the CIO by championing and driving forward the D&IT transformation.
- Maintain and fulfil a D&IT exploitation plan that ensures maximum value from the application and use of effective D&IT in line with this Strategy and in accordance with the Function's defined architectures, standards and policies;
- Represent the voice of their TLB within the Function, contributing to the establishment and maintenance of clear strategic intent and the plans, standards and processes that result; they will provide customer feedback into the D&IT Shared Services groups to help manage and improve performance.
- Deliver TLB specific applications – that are built and supported according to the Function's architectures, standards and processes; and using the centrally provided tools and systems as part of a collaborative defence D&IT franchise.

Shared Services will provide customer centric services that are best designed and delivered once, on behalf of Defence, to maximise effectiveness, operational integrity, security and efficiency.

6.2 How it will work

Governance for the Function will be through the DISC, the CIO Council and through objectives that the CIO will set with TLB CIOs.

- Defence Information Steering Committee (DISC): comprising Perm Sec, Commander JFC, the Vice Chief of the Defence Staff (VCDS) and an external Non-Executive Director; the DISC will set overall strategic direction holding CIO to account. VCDS will represent the views of Front Line Commands (FLCs).

- D&IT Coherence Board: comprising TLB and Function CIOs, D&IT Function COO, Directors of Cyber Defence and Digital Enablement and CEO ISS; the Board will be chaired by CIO and will hold the group individually and collectively accountable for meeting the Functional Strategy implementation plan and its outputs. This group will act as a steering board for the shared services components to act as the 'voice of the customer'.

- The MOD CIO will set in-year objectives for the Command and Enabling Organisation CIOs in addition to the objectives from within their Command or Enabling Organisation. These objectives will be in support of the Functional Strategy and will cover expectations as set out in Table 4.

Strategy Enablement	• Contribution to the development of this Strategy • Maintenance and fulfilment of a supporting TLB plan • Ensuring that the TLB requirement and voice is included
Cyber Defence & Risk	• Risk identification and response
Operational Integrity	• Compliance with standards and operating processes
Economy of Scale	• Maintaining transparency of Function activity and costs • Driving decisions to simplify, share and reduce supply side costs
People, Skills & Capability	• Ensuring staff are developed in line with Function plans • Creating and maintaining a diverse and inclusive environment

Table 4. CIO alignment objectives

6.3 Stakeholder Relationships

The CIO will build and maintain several important relationships which underpin the operating model, as shown in Figure 4.

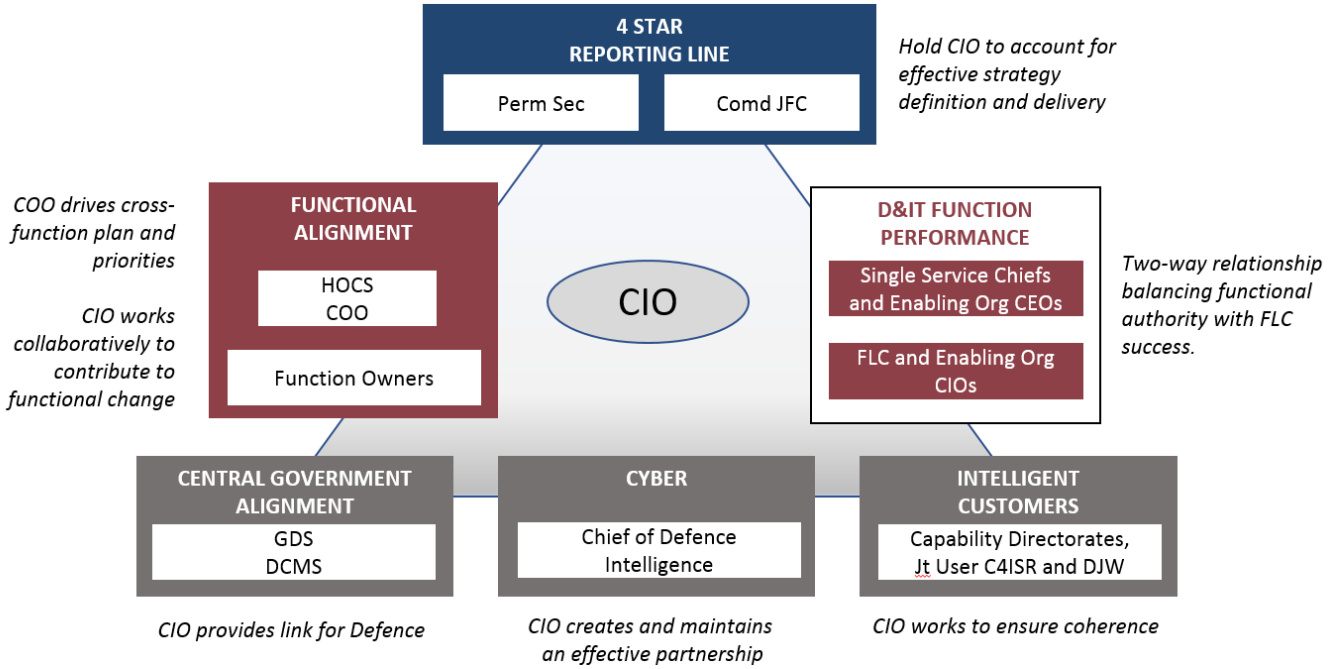

Figure 4. Stakeholder relationships.

- 4 Star Reporting Line: held to account by Perm Sec and Comd JFC for effective definition and achievement of the strategy for their respective areas of responsibility.
- Single Service Chiefs and Enabling Organisation CEOs: this is a two-way relationship where the CIOs functional ownership and its impact on FLCs is balanced by the input to the DISC and by the need for CIO to maintain effective working relationships and action that demonstrates an understanding of the FLC and the role of the Function in contributing to success.
- Front Line Command (FLC) and Enabling Organisation CIOs: The CIO will set specific objectives and hold individuals within the Function to account. Collectively the senior functional leadership will

work together to create a productive working relationship leading to strong D&IT performance for Defence as a whole, as well as for each constituent TLB.

- Transformation Board: The CIO will work with the Transformation Board to enable technology transformation across defence.
- Other Functional Leads: CIO will work collaboratively with other functional owners to ensure that the D&IT Function contributes effectively to the wider functional change agenda with particular emphasis on simplifying and automating business process. The Defence COO will have a role to play in creating a strong cross-functional plan and in resolving any conflict in priority, and each Functional Owner will have responsibility for data governance within their areas.
- Joint User Command, Control, Communications, Computers Intelligence, Surveillance and Reconnaissance (Jt User C4ISR) and FLC Capability Directorates: CIO will work with intelligent customers and capability sponsors to ensure that any D&IT elements of capability programmes are coherent with the D&IT Functional Strategy and to ensure that these programmes are effectively informed and driven by the emerging digital opportunities and innovation.
- Chief of Defence Intelligence: The CIO will create and maintain an effective partnership in service of a strong and collective approach to defensive and offensive cyber operations.
- Government Digital Service. The CIO will provide the link for Defence with the wider GDS, interpreting central direction for Defence, where appropriate.
- Department of Digital, Culture, Media & Sport. The CIO will provide the link for Defence with DCMS, interpreting central direction for Defence regarding data governance and AI exploitation, where appropriate.

7. The D&IT Function Plan

A D&IT Function Plan will be developed to realise this Strategy. The change activities and objectives will be managed together as a coherent change programme. We first need to stand up the D&IT Function and close critical leadership and skills gaps, as an enabler to the other priorities, working towards a data driven organisation. Priorities also include strengthening plans to improve battlespace interoperability and support Information Advantage; addressing critical risks in cyber defence and leading the technology component of transformation for all Defence Functions; and improving IT service quality and reliability.

An essential part of the next stage of work is to develop the detail of the Defence Information Strategy, which will set out the capabilities needed in Defence and the associated strategies to achieve them.

Funding is required over a 2-year period to set up these workstreams (both new capabilities and efficiencies) and define the requirement and scope of the Transformation Partner to lead implementation. An overall D&IT Function Transformation Investment Case is being prepared, and individual business cases will be brought forward for supporting projects.

Over the coming months, we will continue to develop a comprehensive D&IT strategy to meet our strategic priorities, and the underpinning capabilities needed to enable this. This will move MOD decisively towards becoming a truly data-driven organisation, that is constantly alive to, and in tune with, the transformative potential of IT.