Ministry
of Defence

DEFENCE INFORMATION AND COMMUNICATIONS TECHNOLOGY STRATEGY

OCTOBER 2013

Document Control

Document Identification	
Document Issuer	Chief Technology Officer
Document Author(s)	CTO – Air Cdre Mark Neal OBE CEng FIET RAF
Programme/Project Name	Defence Information & Communications Technology Strategy
Document Version	1.0
Document Date	30 October 2013
Document Classification	Not protectively marked

Document Version Control			
Version	**Date**	**Author**	**Change(s)**
0.1	12 Jul 13	CTO	1* Circulation
0.2	24 Jul 13	CTO	Industry Circulation
0.3	30 Aug 13	CTO	2* Circulation
1.0	30 Oct 13	CTO	1st Publication

Table of Contents

DEFENCE ICT STRATEGY 2013
Architected, not accidental

APPLICABILITY AND PURPOSE – What it is and what it is for

This Defence ICT Strategy 2013 supersedes the Defence ICT Strategy published in October 2010. It applies to the full breadth of the Defence enterprise[1] and includes the necessary ICT enablement of information flows between MOD organisations and their government, military, industrial and other partners across the Defence enterprise. It has relevance in all existing security domains (and across the new tiers of Government Security Classification to be introduced from 2 April 2014) but places emphasis on transformation at the lower levels of classification.

The Defence ICT Strategy 2013 is an articulation of the actions to be taken over time in order to ensure that ICT is procured, used, supported and replaced in an increasingly coherent manner; one that aligns with Government and Departmental Strategies, is compliant with Policy and coherent with appropriate target architectures.

A wider Defence, rather than solely MOD, focus is essential as it becomes increasingly important for MOD to adopt common approaches and solutions with that of other Government departments and agencies, at home and abroad.

The Strategy responds to the business and operational needs, and the resultant information needs and flows, set out in relevant strategies and plans. These include, but are not limited to, the Government Digital Strategy, MOD Information Strategy, Digital in Defence and the Cyber Strategy (at an enterprise level), the C4ISR and Logistics IS Strategies, and the relevant Capability Management Strategies and Plans owned by the Joint Forces and Front Line Commands (and most notably the C4ISR Capability Management Strategy).

It considers the full range of information policies set for MOD by the Chief Information Officer (CIO), through the Head of Strategy Policy and Practice, and the resultant ICT technical policies he delegates through the Chief Technology Officer (CTO) to the Defence Technical Authority, and seeks to shape these where necessary to improve coherence.

It describes the actions necessary to apply target architectures (which are to be set out in business, information and technical layers) designed to meet Departmental needs and those of the Interim Force in 2015 and the Future Force in 2020.

Whilst providing clear direction, this Strategy does not seek to determine balance of investment in MOD ICT. Hence, the pace of transformation and measurement of progress along the ICT roadmap are not set out here but in the ICT Transformation Plan and in the relevant Capability Management Strategies and Plans owned by the Joint Forces and Front Line Commands (and especially the C4ISR Capability Management Strategy and its subordinate Capability Management Plans).

[1] In this context, the Defence enterprise is all encompassing and includes all 7 MOD TLBs and their agencies, as well as allies, partners and the Defence supply chain.

The MOD Information Strategy 2011

… sets the **Defence Information Vision** of …
Agile exploitation of our information capabilities to improve effectiveness and efficiency on operations and in support areas through access to, and sharing of, timely, accurate and trusted information
… and espouses the **strategic benefits** of *Improved Effectiveness, Agility, Efficiency and Compliance*

- …through the application of 7 information themes

Digital in Defence

… part of the Defence Vision's requirement to introduce **"modern, innovative ways of doing business"**. It is largely not concerned with Digital in the battle space but aims to strengthen the Dept's Digital leadership; working closely with the GDS and OGD on Digital issues; developing our Digital capability; and exploring the redesign of its principal interfaces with citizens, focused particularly on recruiting and veterans

Defence ICT Strategy 2013

… a compelling narrative, applicable and useful across the whole Defence enterprise, that challenges the way that ICT is demanded and supplied and how this relationship is controlled. It provides a vehicle for **driving greater coherence into our investments in, and use of, Defence ICT**

C4ISR Strategy

… places NATO at the heart of **operational Defence activity** and drives towards a **Single Intelligence Environment**. It is divided into 3 Epochs to: Mitigate contingency now (next 2 years); Enable enterprise reach (2 to 4 years); and Configure for FF2020 and enduring contingency. It also seeks to improve UK cyber resilience and safeguarding

JFC Joint Enablers Capability Management Strategy
C4ISR Capability Management Plans

… articulate the balance of investment, through life, of the necessary capability enablers in line with the preceding strategic direction and in order to enable the satisfaction of Defence outputs

FORMAT – How it is set out

The Defence ICT Strategy 2013 builds on its predecessor (published in October 2010) and retains the same overall format. The first major section looks at the Defence **DEMAND** for ICT now and into the immediate future, and examines what the wider Department must do in order to gain more value from its investment in, and use of, ICT across the enterprise.

The next major section looks at those factors that must be addressed if MOD is to be more efficient and effective in its satisfaction of these demands, and sets out principles that are to be followed by those involved in the **SUPPLY** of ICT such that MOD can secure coherent and beneficial outcomes.

The final major section looks at the need to improve **CONTROL** of the demand for, and supply of, ICT in order to ensure that Defence gets, and can sustain, what it needs in a coherent and affordable manner.

DEMAND

CONTEXT – Where the Defence user is today

MOD has benefited greatly from its investment, over the last decade, in the Defence Information Infrastructure (DII) Programme and its underlying networks. Not only was it able to secure well over two billion pounds worth of efficiencies, its business was enabled by resilient and global connectivity within each security domain. Email connectivity is possible across the enterprise, in the office and on the move, and has, for some time now, provided the core of our ways of working. However, as Defence has grown more to appreciate the value and power of information, it has also come to recognise the limitations of its over reliance upon email. A user has limited control over its receipt with a resultant management overhead to extract value from it, and email can only be transmitted from point to point, carrying a limited payload in its attachments, reducing its usefulness as a means of collaborating over or consuming its content.

More recently, the DII Programme has delivered collaborative tools with richer functionality but the pace of delivery has been slow and older designs pertinent to the time in which DII was designed limit the utility of these tools when compared to the marketplace today. Other equally large enterprises in the private sector have implemented an enterprise social layer on top of SharePoint and desktop video-teleconferencing facilities, which have seen impressive rates of adoption and had a transformational effect on the organisation. However, it is proving incredibly difficult, within the finance and time available, to apply the remaining DII investment both to the modernization of the office environment and to the provision of operational capability to users deployed and afloat; the operational user overseas cannot always rely upon the availability of high bandwidth, low latency (i.e. broadband) connectivity and yet must interoperate effectively, within each security domain, with a wide range of partners and allies.

Similar non-DII examples can be found across the Defence estate and at all levels of classification, with the resultant and still growing ‘legacy’ landscape increasing the challenge to find coherent outcomes. These competing demands have resulted in an array of highly bespoke solutions, the integration of which impedes an agile response to change or innovation; enterprise pace is frequently set by the slowest moving element.

ENDS – What the Defence user needs

As current and future users of Defence ICT we want assured access to our information across the Defence enterprise and tools that enable rather than constrain our daily function. We want to reap the benefits of the modern consumer marketplace while recognising the need to manage the increasing cyber threat.

Defence ICT users must exhibit the confidence and competence to get the most from the full range of tools available to them, operating with an appropriate understanding of the value of information to their role and the wider Defence community.

Recognising the financial and security limitations, we do not seek to provide the exact same capabilities in the office, on the move or when deployed, but we do wish to consume information services tailored to each of these environments; a single information environment enabled by ICT (services and end user devices) suited to the point of need. In many cases, it will not prove economic or sensible to provide users on the move the full suite of services available at their home base; the business or operational architecture that is being enabled by ICT must clearly show which services are required where.

A smaller workforce means we individually have less time to contribute to each Defence output and that we need to shed the unnecessary burden of manual information management and assurance; we need easier access (i.e. single sign on) and increased levels of automated information management. We also seek intuitive ICT that reduces the training burden and increases the poor levels of utilisation evident across the DII toolset.

We no longer wish for prescriptive solutions and practices but seek agility in the ways in which we can consume and share our information, wishing increasingly to do so on the move. We need to work more collaboratively and with greater agility, reaching out to people and information as required to gain knowledge, through enterprise and social networking within and outside the MOD boundary; ‘crowd sourcing’ will be part of how we choose to operate, both within the community and, on occasion, reaching out to the wider world.

Data holdings across the Defence enterprise continue to grow exponentially and we wish to harness and exploit the power of this data in ways that we have yet to achieve and which we may choose not to predetermine. We wish to interrogate these data holdings at a time and place of our choosing to derive maximum value in a dynamic setting and to inform our decision making in a timely and cost effective manner. We need active data management and analytical tools capable both of manipulating the breadth, depth and diversity of our data holdings (be they numerical, text based or imagery) and of presenting the findings clearly. We recognise that such tools will continue to depend on the trust we can place in the quality and source of the underlying data, which can be enhanced through use of enterprise social tools and techniques.

Finally, we seek a more dynamic approach to our information risk management that enables us better to balance inherent and emerging threats against the need to secure outcomes and benefits.

WAYS – How Defence must set the context for ICT investment

Successful provision of such ICT in Defence depends upon our ability clearly to establish the business context. Essential prerequisites to successful ICT investment include a detailed understanding of our business and operational processes and their resultant information needs and flows, as it is the latter that must be efficiently and effectively enabled by ICT. Today, although much work has been done across the Defence enterprise, too many of our processes remain poorly articulated, or are out-dated and unsuitable for modern ICT enablement. Furthermore, we often lack the skills necessary to procure and use modern ICT services effectively and need to invest more in appropriate training.

There are two particular challenges that we must address. First, in taking a more user-centric view of ICT provision, we must examine our core processes in order to satisfy ourselves that the individual staff burden is minimised and that corporate tools add value to the end user as well as the appropriate functional specialists and senior management. All too often, end users are an essential contributor to, but not a satisfied consumer of, such processes. Second, we need to think more carefully about where and how users will interact with our business and operational processes and tailor our tools and user interfaces accordingly. This is particularly important where we expect users to consume information services on the move. For example, the presentation of all the HR tools to the user in a portal may be appropriate for office consumption but it is much easier to provide selected HR services safely and securely to a tablet or smartphone than it is to provide the full suite (including tools that users would not find useful on the move).

In many cases, the continuous improvement of efficient and effective processes can be enabled through simplification, and the procurement of commercial-off-the-shelf (COTS) ICT can aid in achieving such economies. Itself cheaper to procure than bespoke solutions, use of familiar COTS ICT can also ease interoperability between processes and their integration (where appropriate), as well as reducing the training burden. This is true internally within MOD and across the wider Defence enterprise. However, these benefits can only be realised where processes are adapted to consume the COTS ICT (and not vice versa).

A limiting factor to date in our deployment of ICT has been the manner in which we express the requirement and the benefits we seek, which can exacerbate our occasionally weak understanding of the information needs and flows to be enabled. Users get the most from ICT when they have had an opportunity to explore its potential and this greater understanding shapes the way in which they choose to work. It is rare for a detailed upfront specification to match this more iterative approach either in user satisfaction or in the realisation of benefits. In a complex, adaptive system, a series of ‘safe-to-fail’ experiments in applications’ design and deployment are more likely to yield positive results, and introduce innovation, than adherence to the meticulous, up-front specification of ICT solutions. The provision of a stable infrastructure platform with a clear technology roadmap is an essential enabler to such experimentation.

MEANS – What Defence must do to realise success

A consistent expression of the business and operational processes that must be applied to secure Defence outputs is essential both to inform SDSR 15 and to derive ICT needs from its capture. Defence policy and process owners, functional leads and TLB holders must therefore act to architect their business improvements (where a consistent architecture is not already expressed). The CTO and DE&S Engineering Group are able to support this work through the provision of suitable tools and advice.

While it is vital to capture the key information requirements of the Defence business, this alone will not provide adequate focus on the needs of the individual Defence user. Defence policy and process owners, functional leads and TLB holders must therefore also adopt a user-centric view as they architect their business improvements.

In some areas, these responsibilities call for further investment in skills. TLB holders must therefore support the workforce planning of the 2* Information Skills Champions and the subordinate Heads of Profession through appropriate investment in courses and training time for their personnel.

In articulating the required business process improvement, we must seek to exploit the economies of COTS ICT wherever possible and ensure that our business process does not require unnecessary development of bespoke ICT.

Regardless of whether the ICT solution to the articulated need is bespoke or COTS, the ICT must be suited to the user environment. Defence policy and process owners, functional leads and TLB holders must therefore act to ensure that individual staff burden is minimised and that, where appropriate, users can operate effectively on the move or when deployed.

We must also act to improve data quality and access, establishing and enforcing appropriate management of those data sets upon which the Defence enterprise most depends and which are widely shared. As we modernise, we must free data from the legacy (and often proprietary) applications in which it has been locked in order to enable its wider and more dynamic exploitation. Separation through immediate, wholesale modernisation is not necessary to achieve this, as it is also possible dynamically to extract information that is trapped within legacy data representations.

Too many of our line of business applications, of which we have circa 1500, are inadequately supported and we probably lack the funds necessary to move them all, in their current guise, onto a new operating system as Windows XP goes out of support. We must therefore work together to streamline our business, minimise our dependence on this legacy landscape and invest in retained or new applications and services that possess a funded Through Life Management Plan that keeps pace with future network upgrades and consumption methods.

As we make new investments, we must describe our user need (i.e. URD) using a functional description method developed by the CTO such that consistent language and shared understanding drive greater levels of coherence.

We must also examine how we control the specification, procurement and use of ICT, seizing the immediate opportunity, generated by the appointment of a 3* CIO, to review our corporate governance arrangements and ensuring that they are fit for purpose in the provision of agile, innovative and fast-paced ICT services.

SUPPLY

RESPONSE – How the ICT community must react to this clearer Defence demand

A clearer articulation by the Defence community of its needs of ICT and the beneficial outcomes it seeks from its investment in, and use of, ICT permits those responsible for its supply to adapt processes and solutions to deliver with agility capabilities of appropriate cost and performance. However, the ICT community is not yet positioned to meet the demands of a more intelligent customer, and must transform in order to do so. We need to look at the services to be provided; the means by which this is done; and the behaviours, mind-sets and attitudes of those involved.

THE CURRENT LANDSCAPE – From where MOD must begin to transform

In recent years, Defence has worked hard to integrate its multitude of various ICT systems, consolidating them, removing duplication and linking systems, often through a small number of very large programmes, such as DII. Defence now primarily operates effectively and efficiently on a single, joined up and common infrastructure. In tackling this significant integration challenge, the Department chose to minimise risk by placing a large 10-year contract for a single information infrastructure with a prime supplier, Atlas.

While Defence has achieved huge benefits in creating a single information infrastructure, the procurement approach has brought other challenges. The sheer size and complexity of the undertaking hindered competition, reducing viable bidders to a handful of potentials, and meant that timescales to enact the required changes were necessarily long - there was much to do. Readily identifiable benefits in enabling corporate HR processes were tackled early on, while the tougher challenges of enabling operations at higher levels of classification, on deployment and afloat were tackled later, when time and risk contingencies were dwindling.

Today, Defence transformation demands the application of modern ICT solutions to improved business and operational processes at the same time that Government and MOD must limit spend on ICT investments in a period of increased fiscal constraint. Planned reductions in ICT spend between 2010 and 2015 of the order of 25% must now be extended to accommodate the conclusions of the 2013 Spending Review, which included a further £300m reduction in MOD expenditure on ICT and commodities. We have significantly less to invest in ICT and yet we cannot even sustain the capabilities we have without reforming how ICT is delivered; capability gaps remain unfilled and data holdings and user demands continue to increase.

In the midst of an Information Revolution, Defence users wish to exploit a range of smart phones, tablets, social media and modern discovery and analysis tools that we had not anticipated when the existing ‘big 4’ ICT contracts were placed a decade or more ago. Our procurement approach has tied us into long-term commercial arrangements that have hindered our ability to seize opportunities and to be innovative and agile in our adoption of new information services and technologies; there have been few successful interventions.

Our core programmes have failed to keep pace with changing user demand to such an extent that some Defence organisations are choosing instead to invest in alternative solutions that more readily meet their parochial needs; this may achieve the desired outcome locally but it can be detrimental, and carries a consequential cost, to enterprise coherence and interoperability. Our ability to exploit the knowledge of those close to the business, in their application of local innovative solutions, remains important but should not circumvent the efficient and coherent use of core services. In addition, individual users are on occasion motivated to deliver their output using policy non-compliant technologies and practices, increasing our collective exposure to information risk.

The way in which we procure and supply ICT services to Defence users has to change. Services must be delivered with greater economy and agility and be readily adaptable to changes in demand. In providing ICT solutions, we must strike an appropriate balance between desired benefits and necessary security. We have an extensive and complex legacy landscape, which we must seek to simplify as we modernise it, making maximum use of COTS solutions and open standards wherever possible, including the use of COTS as modules of bespoke end-to-end solutions where the user need requires it. Bespoke processes that demand bespoke ICT solutions represent a significant cost driver that Defence can ill afford in these times of fiscal constraint.

THE TARGET LANDSCAPE – Where MOD needs to be

Defence is a massive, diverse and complex enterprise within and across which we need to exchange information and share knowledge in dynamic and sometimes unpredictable ways; this requires that we create and sustain a **Single Information Environment**.

Across its enterprise, Defence remains committed to the beneficial outcomes articulated in its Information Strategy; it wishes to be more effective, more efficient, more agile and more compliant; compliance is measured in terms of alignment with strategy, compliance with policy and architectural coherence. However, the means by which these benefits are to be secured must vary across the enterprise according to need and circumstance. The Defence enterprise shares many characteristics with other large-scale public and private enterprises, where it can learn much from best practice, but it also has unique characteristics which apply only to a Defence enterprise, and which merit peculiar consideration.

The required **Single Information Environment**[2] must be enabled by ICT (services and end user devices) suited to the point of need and tailored to the most applicable benefits. On Operations, we need to retain advantage through the timely delivery of resilient ICT that can function in hostile and often poorly connected environments, whereas in the more benign environments where the largest volume of users resides, we need to exploit the availability of assured connectivity and COTS ICT to drive necessary economies through commoditisation and standardised service delivery.

We will also see increases in the use of software (over hardware) to define different capabilities (i.e. cryptography and radios). This will permit a reduction in the form of devices and ease their integration into military platforms.

The target network architecture must provide for the simplest yet assured interconnection of the different fixed, deployed and afloat environments that comprise the Defence enterprise, rooted in the application of common standards. Infrastructure should be considered a commodity that is able economically to host and transport the users' information needs. MOD will satisfy these needs mostly (but not exclusively) through appropriate use of the Public Services Network and the Internet to access modern storage and hosting capabilities.

[2] The Single Information Environment is a logical construct whereby assured information can pass unhindered from point of origin to point of need.

END USER DEVICES – Where Defence users will access their information

Users need easily to access their information in all the environments that make up the Defence enterprise; reliance upon a majority of desktops, a minority of laptops and relatively few handheld devices is no longer appropriate. MOD must enable access to information from a range of end user devices (EUD), including tablets and smartphones. However, the current popularity of Bring Your Own Device (BYOD) is not yet suitable for application in Defence and the immediate target architecture does not make provision for users to bring their own devices to work and to connect them directly to the Defence network; such direct connection presents an unacceptable cyber threat.

However, the benefits of BYOD, of improved economy and user experience, can be applied to Defence through adoption of a Choose Your Own Device (CYOD) policy. CYOD sees the procurement of a range of modern EUD by Defence, the integrity of which it can manage, in order to offer users an affordable choice according to their needs and environment. CYOD can be supplemented to enable users to connect indirectly to the Defence network from their own devices where appropriate. For example, a user may wish to use a personal device to access HR services while commuting or from home. The target architecture will make provision for a selected range of device standards that permit users to meet their needs through the most appropriate mechanism.

MOD policy will need to adapt to enable this way of working, as encouraged through the introduction of the Government Security Classifications policy, and users will need to accept greater individual responsibility for the safe handling of information in this way.

STORAGE AND HOSTING – Where Defence users will keep their information

Defence must store required information and host necessary applications in the most economic and sustainable manner possible, while recognising that the different environments within the Defence enterprise will dictate different solutions. All new investments in data storage and application hosting, whether in new capability or as a refresh or upgrade of existing capability, will be tested against the following priorities, set out in descending order of preference:

- Cloud hosted.
- Government or coalition hosted (Sharing of OGD/Coalition facilities).
- MOD hosted.
- EUD hosted.

APPLICATIONS AND DATA – How Defence users will access their information

Delivery of an ICT service to the Defence user at the point of need is no longer synonymous with delivering an application to the desktop. A range of service implementations (comprising hardware and software components) are required to satisfy the users' information needs to agreed levels of service that are appropriate to the environment. This necessitates adherence to appropriate information-handling models, standards and codes of connection. In particular, delivering such services to users economically, even when they are mobile, while retaining the agility that they demand, requires that applications are presented in the following, descending order of priority:

- Browser based.
- Client - Server.
- EUD hosted.

Modern applications, presented in the most appropriate manner, are not in themselves sufficient to meet the users' needs. The target architecture will separate out data and applications, enabling the users more readily to access and exploit data in a variety of ways with a range of tools. In this way, users will be able to analyse a wider range of disparate structured and unstructured data held across the breadth of its enterprise, in ways and at speeds that they had hitherto thought

impossible, with concomitant improvements in the evidence available to decision makers at all levels across environments.

'Big Data' analytics allow the manipulation of data of variable quality and disparate origin, but there remains considerable value to the appropriate management of corporate data upon which the enterprise depends and which it wishes consistently to re-use. Hence, the target architecture will identify Departmental master data and seek to make it available for exploitation by all authorised applications and users.

ICT RISK MANAGEMENT – How Defence needs to balance risk and opportunity

Many across the Defence enterprise are critical of the manner in which security controls are applied to its ICT and the (real and perceived) impact that such application has on its utility. There are three underlying reasons for this widespread view. First, outcomes and benefits are often poorly expressed and ICT investments are frequently specified in input (rather than output) terms; shaping these investments, to balance risk against desired benefits, is therefore made more difficult. Second, until very recently, it has become a common practice to apply security controls to the management of sensitivity and the segregation of sensitive data between user communities; information has been classified as RESTRICTED and borne descriptors in order to manage its handling rather than in response to an identified security threat. Third, such security controls have been applied to ICT systems at an enterprise level, imposing common prescriptive handling controls (regardless of need or environment).

The introduction of a new Government Security Classifications policy in April 2014 provides MOD with an opportunity to revisit how an appropriate balance can be struck in managing ICT risk. Defence must continue to guard against increasing threats to its information security and availability through rigorous compliance with its information assurance and cyber policies[3]; these policies must themselves stay abreast of the opportunities provided by innovative technologies. It will be rare for compliance to be measured in a simple 'pass/fail' test and application of, and adherence through life to, appropriate (procedural and technical) measures will need to be proven.

MOD must conduct a risk assessment, in accordance with the Government's Risk Management Regime, whenever ICT is procured or used in a particular manner for the first time. In assessing the risk, Defence must address each attribute of Information Assurance (IA): confidentiality, integrity, availability, authentication and non-repudiation. The assessment will comprise a systematic examination of the technical aspects; seek to ensure the application of a coherent and comprehensive suite of IA controls; and confirm the presence of a process to ensure that IA controls continue to meet IA needs throughout the life of the ICT solution. That said, not every investment will merit the same level of assessment and, in conducting an assessment, it will be important to consider the threat environment, size of investment and novelty of the proposed ICT solution. The aim must be only to do the minimum necessary to inform timely decisions on how best to balance risk and opportunity, such that spend is minimised and agility is protected.

Defence seeks to delegate authorities as far as possible, and this applies equally to information risk management where Senior Information Risk Owners and Information Asset Owners in TLB organisations are empowered to make many ICT investment and usage decisions. However, global connectivity across the Defence enterprise can expose the wider community to increased risks deemed appropriate at a local level. It will therefore be necessary to escalate novel, contentious and innovative ICT proposals to central authorities. Where non-compliance with Defence ICT policy is accepted for a period, this is to be closely managed through the issue of authorised 'waivers', which set out the approved extent of non-compliant activity and the measures required over time to achieve policy compliance. ICT solutions that do not comply with Defence

[3] To include appropriate consideration of export control, commercial confidentiality and Intellectual Property Protection.

ICT policy and do not possess an authorised ‘waiver’ will be denied access to the Defence network.

The introduction of the new Government Security Classifications policy in April 2014 (while enabling the conduct of modern business practices through the application of good commercial ICT security) removes the opportunity to use the three lower levels of current security classification as the basis of the Defence information-handling model. The 2014 Technical Controls Framework facilitates easier sharing of OFFICIAL information across MOD boundaries but does not provide an adequate means of managing sensitive information across and between the many individuals and communities that make up the Defence enterprise. New Identity and Access Management services are therefore required.

Defence users will be permitted to pursue modern business practices at OFFICIAL, where COTS ICT can be used safely in line with good commercial practice. Greater emphasis is placed upon individual responsibility and accountability and Defence users will need to be competent to use the ICT provided appropriately. Corporate benefits and individual user experience will be enhanced when Defence holds as much of its information as is possible at OFFICIAL, taking advantage of cost effective COTS services, but there remains a need to ensure that business is conducted safely and securely in a resilient environment.

Those providing new ICT capabilities or planning upgrades to existing services should make use of the Cyber Defence Capability Assessment Tool.

ENABLING TECHNICAL SERVICES – The necessary underpinnings of user-defined solutions

Currently, Defence procurement begins with a Single Statement of User Need that spawns a Genesis Option or equivalent business case. However, the coherence and effectiveness of the target architecture depends upon the provision of enabling technical services upon which all Defence users depend but for which no single user is likely to call. In future, these enterprise-wide enabling technical services will be championed by the Defence Authority for C4ISR (CTO, C4ISR Cap and/or C4ISR Joint User); they include, but are not limited to, Identity and Access Management services, interoperability gateways, and an enterprise service bus.

IDENTITY AND ACCESS MANAGEMENT (IdAM) – The means to control information access

Identity and Access Management (IdAM) is a key enabler to delivering an effective ICT capability that allows information to be shared appropriately, including with our Allies, OGD and Industry. IdAM is an integrated set of policies, processes, standards and technologies that create and manage digital identities and associated access privileges for all people and other entities within an organisation and over the whole lifecycle of activity. Services are required at each security level and should be provided centrally in order to drive coherence and to achieve required economies. Above SECRET, the Safeguarding Initiative is setting the pace and direction of IdAM service delivery, while the establishment of the PEGASUS gateway services for the ‘5 Eyes’ community is achieving the same effect at SECRET. The roadmap for IdAM at OFFICIAL is to be agreed by Q3/13.

The CTO will lead on implementing IdAM standards and technologies as an enabling service for consumption by other Defence ICT programmes and projects. Requirement setters and system builders must ensure that their programmes and projects adhere to these IdAM standards, integrate the enabling IdAM technologies where appropriate, and consume the enterprise IdAM services whenever possible.

Implementation of IdAM will increase our ability to interoperate safely within Defence and with those who need to share information with us, whilst at the same time allowing us to enhance our security. IdAM allows us to go further than this in that it enables processes to be conducted digitally with greater levels of trust than has been possible to date – processes can be redesigned so that

secure information sharing with Allies, Industry and OGDs can be radically enhanced. Applicable services, tools and information can be presented automatically to an authenticated user according to their role or need, negating the need for multiple log-on and denying access to unauthorised sensitive information. The same services, where enabled by hard tokens, can be used as the basis of e-business, permitting automated access to buildings or automatically approving consumption of goods and services. However, hard tokens should only be deployed where the benefits outweigh the costs of delivery and operation.

GATEWAYS – The control of information flows at the boundaries

The management of authorised information flows and the denial of unauthorised traffic at the various internal and external boundaries of the Defence enterprise remain key to the safe conduct of Defence business. However, the nature of these information flows, between people and devices, changes over time and is becoming increasingly rich in function and content. MOD must therefore ensure that gateway provision is rationalised such that complex gateways are designed only once and reapplied as required. Reduction of unnecessary complexity is essential to achieve required economies and to improve connectivity with legitimate partners, while retaining appropriate levels of information assurance. The Defence Authority for C4ISR is therefore adapting its resource allocation to enhance its focus on international business and interoperability.

ENTERPRISE SERVICE BUS (ESB) – Enabling coherent enterprise wide information flows

In an enterprise as diverse and complex as Defence, it is inappropriate to establish the required Single Information Environment solely through enforcement of common ICT solutions. However, Defence does seek to share information across its enterprise and therefore needs to invest in an appropriate, corporate service oriented architecture that permits the connection of disparate applications, services and re-usable data stores to create a logical Single Information Environment. The Defence Authority for C4ISR must establish a logical coherent service bus, incorporating Business Process Orchestration, at an enterprise level if it is to prevent the continued proliferation of incoherent service buses across the enterprise, the connection of which will drive complexity and cost.

THE JOURNEY FROM CURRENT TO TARGET LANDSCAPE

ICT PROCUREMENT – Changing the way in which we buy ICT services

Procurement methods in Defence are optimised for the acquisition and through life support of major equipment and platforms and are not well suited to the provision of ICT services. They require users to provide detailed input specifications, limit direct selection of appropriate COTS solutions and restrict opportunities to iterate designs through user experimentation. This linear and prescriptive approach often results in user dissatisfaction, because it operates at a pace significantly slower than the typical lifecycle of ICT (resulting in obsolescent solutions), and/or because exposure to the final solution enables users to realise that the original input specification was flawed. A user would not readily be able to specify a need for smartphone functionality without first seeing one and understanding its capabilities. Defence seeks to embrace user experimentation as a core component of a more iterative ICT procurement method; such user experimentation could, for example, be enabled through use of 'model offices'.

The sourcing of ICT services is to be made more agile and effective by procuring services through smaller, shorter contracts; there will be some exceptions to this approach where global scales make it impracticable. This will increase competition by giving a large number of smaller, and often innovative, organisations such as SMEs[4] the opportunity to provide services directly to MOD. It will enable the Department to keep pace with emerging technologies and changing operational needs. In so doing, Defence seeks to become a more open and savvy customer, able to exploit an open marketplace for the supply of ICT services, with the agility to switch between suppliers relatively seamlessly, in accordance with the following key commercial principles:

- Transparency in the supply chain so that Defence understands the costs and opportunities of delivering new and improved services.
- A more segmented supply chain with shorter contracts.
- Use of pan-Government ICT frameworks whenever appropriate.
- Use of an integration function to integrate end-user services and to manage the supply chain.
- An incremental, portfolio-based approach to replacing existing contracts with new commercial arrangements.

For core enabling infrastructure delivered by ISS, this approach will be taken forward within the DCNS framework and its Target Supply Chain Model. DCNS will procure ICT services in towers, each tower grouping together similar services, ensuring they are appropriately integrated, and supplying them across Defence. The specification of open systems will enable wider competition, greater interoperability, and agility, and permit the inclusion of SME suppliers and the retention of innovation. The integration of services will follow a Services Integration and Management (SIAM) model, with a single entity providing the SIAM function without holding any of the contracts for individual towers. In this way, Defence will continue to benefit from the good work already done to bring its infrastructure together into one integrated system; it will retain, simplify and build upon this coherent base.

A key component of successful SIAM will be continued and timely access to useful test and validation services, such as those available at the Land Systems Reference Centre at Blandford, and the adoption of an effective 'technology transition' methodology (such as the Alpha, Beta, Live model promoted in the Government Digital Services Manual).

[4] This aligns with the Government intent of promoting a public service economy based on open ICT markets with increased participation of SMEs, accepting that SMEs are unlikely to be well positioned to service many Enterprise-scale requirements.

CONFIGURATION NOT CUSTOMISATION – Reducing complexity and cost

To support this approach, standard commoditised products (e.g. COTS rather than bespoke solutions) and open standards are to be used wherever possible to provide ICT services. This will reduce tie-in to any particular supplier or service offering, ensuring Defence can switch quickly between solutions and providers as its business needs dictate or opportunities allow. Defence procurement agents are expected first to approach Crown Representatives when considering sourcing from the large ICT suppliers to Government, as advantageous pricing and licensing costs have been negotiated on behalf of all Government Departments.

NETWORKS – Enabling and protecting the flow of information to meet Defence needs

Currently MOD uses separately switched networks for voice and data in each of the security domains. This creates an excessive in-theatre equipment and support footprint. There are several ways that this situation can be improved, particularly by the introduction of Internet Protocol (IP) for all traffic, IP encryption and the use of Voice Over IP (VOIP) technology. This technology should yield a number of important benefits in the areas of reduced in-theatre footprints, higher usable data throughput and enhanced data/bandwidth efficiency. While some legacy services, particularly those operational systems utilising specialist protocols or low bandwidth communications, may not be suitable for IP transmission, MOD aims to achieve IP transmission wherever possible. New ICT investments should therefore assume this transmission method.

The MoD is currently using IP Version 4 (IPv4), but needs to move to IP Version 6 (IPv6). The transition to IPv6 will not be easy and MOD will operate a 'dual-stack' network running IPv4 and IPv6 for some time. Those specific systems that need to move to IPv6 soon to ensure continued interoperability between MOD systems and those of allies and coalition partners (et al) will be prioritised for transition.

Traditionally, our communications bearers have been protected by link encryption, which means that both the bearers and their contents were protected. However, by adopting IP, MOD can take advantage of commercial networks and 'bearers of opportunity' (without placing any security demands on that bearer) by moving from a 'protect the link' to a 'protect the traffic' mechanism; of course, some vulnerable links will still need protection.

STORAGE AND HOSTING – Embracing Cloud Computing

Cloud computing offers significant savings in ICT service provision when compared with traditional 'on premises' procurements; public cloud consumption can achieve tenfold savings, while private cloud offerings typically generate fourfold economies. Hence, HM Government is committed to a "cloud-first" policy, through which it aims for 50% of new Government ICT to be spent on public cloud computing services[5]. It has established a Government Cloud Framework to enable this approach.

Affordable ICT solutions that enable Defence outputs depend upon this approach and capability planners and delivery agents must migrate infrastructure and applications for which they are responsible towards this model at the earliest opportunity. The CIO has published (in April 2013) a DIN that sets out the activities currently required of MOD officials in procuring Government Cloud services, although there remains opportunity for financial and commercial authorities to update scrutiny and contracting policies to facilitate easier provision of ICT services from the Cloud.

There is more opportunity to move quickly to Cloud based ICT service delivery in fixed locations or within benign, well-connected environments at lower levels of security classification. Beyond April 2014, plans for the consumption of Cloud based ICT services across this large part of the Defence enterprise should be the norm (rather than the exception); the Government Cloud Framework, supplemented by some public cloud offerings provide the vehicles. Cloud computing should also

[5] As stated in the Government Cloud Strategy

be considered for the operational ‘manoeuvre space’ where appropriate but, for now, may remain the exception (at enterprise scale).

Cloud computing at SECRET and above is also possible and its economies should be sought at every opportunity. However, cloud based solutions will be more private, either limited to Defence or shared with selected OGD and industry partners; secure storage and resilience remain important.

In all cases, ICT solutions should seek to adopt ‘cloud techniques’ even when the overall solution does not fit the traditional description of cloud computing.

MOBILE COMPUTING – Enabling the mobile end user device

Defence Operations are by their very nature mobile and this mobility is now increasingly commonplace across the remainder of the Defence enterprise, with military and civilian users increasingly conducting ‘back-office’ activities away from traditional, fixed office locations. However, the provision of approved end user devices does not, of itself, provide users with the mobile information sharing, communication and response times they seek to gain operational effectiveness. MOD must also provide or enable mobile computing applications and services. There are several elements that need to be in place for MOD to embrace mobile computing:

- MOD policy must be updated to support mobile working and the appropriate use of MOD and personal devices.
- Infrastructure including gateways, and mobile device and application management are required.
- Wireless networks, both inside MOD sites and in public and personal spaces, need to be accessible and useable securely.
- End user devices need to be configured and managed to ensure security.
- Mobile applications need to be developed to support the various form factors, different network connectivity and variable working patterns.

The potential for mobile computing to improve the outputs of the MOD is immense but so are the challenges, especially in higher security tiers. To manage the expectations of users whilst moving towards a mobile computing paradigm, the MOD will start by developing capability in the OFFICIAL security tier.

ELECTROMAGNETIC SPECTRUM – Ensuring we can connect and operate safely

MOD will continue to release and share electromagnetic spectrum in order to drive necessary economies into its operations. ICT investors must remain cognisant of spectrum availability, now and into the future, and plan wireless solutions accordingly. Early dialogue with the Joint Spectrum Authority represents good practice and is encouraged.

APPLICATIONS RATIONALISATION – Creating an appropriate and affordable toolset

Today, MOD depends upon a portfolio in excess of 1500 applications, the majority of which have been procured locally, resulting in duplication of capability across the Defence enterprise. Many of these applications are tailored either to satisfy bespoke user requirements or to meet bespoke hosting requirements. This bespoke design approach is not always necessary but invariably drives cost and complexity, at initial procurement and in every subsequent refresh. Coherent capability integration is made more difficult and data is trapped inside this complex landscape, making its re-use much more problematic. The situation is frequently exacerbated by poor maintenance through-life; even where support is funded, the application maintenance plan rarely aligns with the through-life plans for the hosting infrastructure. The result is a plethora of applications, often customised and duplicated, that is too expensive for Defence to maintain into the future.

A Defence Applications Register (DAR) has been launched and is already well populated, albeit there is a need for applications' owners to ensure that their current and planned applications are correctly and promptly registered. In future, connection of unregistered applications to the Defence network will not be possible. The DAR enables Defence to see what applications are available for use across the enterprise, encouraging their re-use and negating duplicate investments.

Charged with driving greater levels of coherence, the CTO has re-launched the Defence Applications Governance Working Group, with pan-TLB representation, to assist MOD in the identification and elimination of unnecessary investments. Applications will be tested for coherence with the Defence Information Reference Model (DIRM) and unused or duplicate applications will be removed from Defence use. Where retention of an application is appropriate, the CTO will use this group and other expertise across the Network Authority to recommend, to the relevant TLB, capability planners or core programme managers, the most appropriate means of providing and hosting the application into the future. Each retained application will have a specified owner responsible for its through life management plan.

The cost of retaining necessary applications, and of introducing new ones, will be minimised by rigorous examination of proposals to customise them to meet bespoke requirements. The tailoring of applications to satisfy bespoke hosting requirements will be minimised by developing a standard infrastructure of known form and with clear upgrade plans (against which application owners can plan). The tailoring of applications to meet bespoke user requirements will be tested against the need to support a genuinely bespoke process (where it may be more cost effective to Defence to adjust the process to an appropriate commercial norm), and against the inability to support such a bespoke process through the provision of COTS modules combined and connected to achieve a bespoke solution. Independent Scrutiny and Approving Authorities will be informed of any misalignment with strategy, non-compliance with policy and/or incoherence with the target architecture deemed inappropriate, in the expectation that the proposed investment will be denied.

The development and deployment of Defence capabilities is, first and foremost, a national responsibility but as technology grows more expensive, and Defence budgets remain under pressure, there are key capabilities that we can only obtain affordably if we work together with our Allies to develop and acquire them. Such cooperation will deliver improved operational effectiveness, economies of scale, and closer connections between our forces. There is clear benefit in reusing NATO solutions and implementing the 'NATO first' policy adopted by other Allies and Partners. Hence, where appropriate, TLB and core programmes are expected to use available NATO applications to meet their need in preference to an MOD alternative investment. The same argument applies to Government applications.

In many cases, it will be important that Defence considers the changing way in which its applications will be used. Increasingly, applications will need to function appropriately across a range of EUD in the office, at home and on the move. It is imperative that Defence identifies the functions to be performed in each environment and provides tools suited to the point of user need. In most cases, the required functionality will differ across these environments and is likely to merit different but complementary solutions that consume the same 'back end' services.

Rationalisation of the applications portfolio to an affordable position is a key requirement of ABC14 and the CIO has launched an initiative, Project EMBRACE, to assist TLB with accommodating reduced budgets in a realistic manner that protects outputs. The scope of this initiative includes all applications at the lower levels of classification and supporting infrastructure that has fallen outside the scope of the core information infrastructure programmes.

MASTER DATA MANAGEMENT – Securing the value of Defence information

The timely provision of trusted and assured information to MOD and other Defence decision makers is, in large part, reliant upon the availability and accessibility of data of appropriate quality. Where a component of this trust is consistency of data across the Defence enterprise, we must take steps to manage adequately our 'master data'. This 'master data' is defined by a uniform set of identifiers and extended attributes that define the core entities of the enterprise (such as location, person and organisation), which are used by the multiple applications that make up Defence systems. We recognise two types of 'master data' in Defence, which are described in relation to the information towers in the Defence Information Reference Model (DIRM). 'Defence Master Data' is used across the Department in systems that span multiple towers, while 'Local Master Data' is used across systems within a single tower.

CTO and Data Management Services (within the Knowledge & Information pillar of Defence Business Services) are currently identifying producers and consumers of data in order to ensure that there is only one authoritative source for each type of 'master data'. CTO is establishing a governance framework to ensure that:

- 'Master data' is coherent with the DIRM.
- Producers of 'master data' comply with agreed policy and standards.
- Consumers with a legitimate need to use it have easy access to 'master data'; where possible using an Open Standards based, Service Oriented Architecture approach.
- Custodians manage their 'master data' to maintain quality and accuracy over time.

The achievement of requisite quality in, and accessibility of, 'master data' across the Defence enterprise will be a key contributor to the improvements in MOD Management Information (MI) sought in the published MI Strategy and pursued by the associated Steering and Working Groups.

STANDARDS – Reducing complexity and enabling interoperability

Defence ICT interoperability is critical. Interoperability ensures that Defence is able to communicate, train, exercise and operate in the execution of missions and tasks and that its supply chain can perform efficiently and effectively the essential business activities that provide enduring support. Interoperability is necessary across industry, OGD and international partners and the CTO is responsible for driving the end-to-end coherence required to facilitate it.

To promote interoperability, acquirers and operators of Defence ICT services are to apply and enforce open standards wherever possible. In all cases, the following hierarchy of ICT standards, mandated in CIO policy and set out in descending order, is to be applied:

- Open standards including International Standards and the Cabinet Office 'Open Data Standards Process'.
- NATO standards.
- British Standards Institute standards.
- Other Government standards.
- Proprietary standards; prior agreement to each application of proprietary standards must be sought from the Network Authority.

POLICY SIMPLIFICATION – Reducing complexity and improving compliance

Examples of weak governance in the procurement and use of ICT can often be traced back to uncertainties, omissions or contradictions in the extant ICT policy set. Defence is beset with too much, poorly expressed policy, which confuses those seeking to comply and, over time, provides reducing beneficial impact. With delegation of authority from the MOD CIO, the CTO will act, over time, to rationalise and simplify the ICT technical policy set. The CTO will delegate further responsibility to others (such as the Head of the Defence Network Technical Authority) for those policies that can be appropriately managed on a federated basis. The Network Authority will review improvements in the ICT technical policy set on a quarterly basis.

Simplification of the ICT landscape will also be enabled by the similar rationalisation of information policies being conducted, on behalf of the CIO, by Head of Defence Security Assurance Services and Head of Strategy, Policy and Practice.

RESEARCH AND DEVELOPMENT – Seeking out innovation and continuous improvement

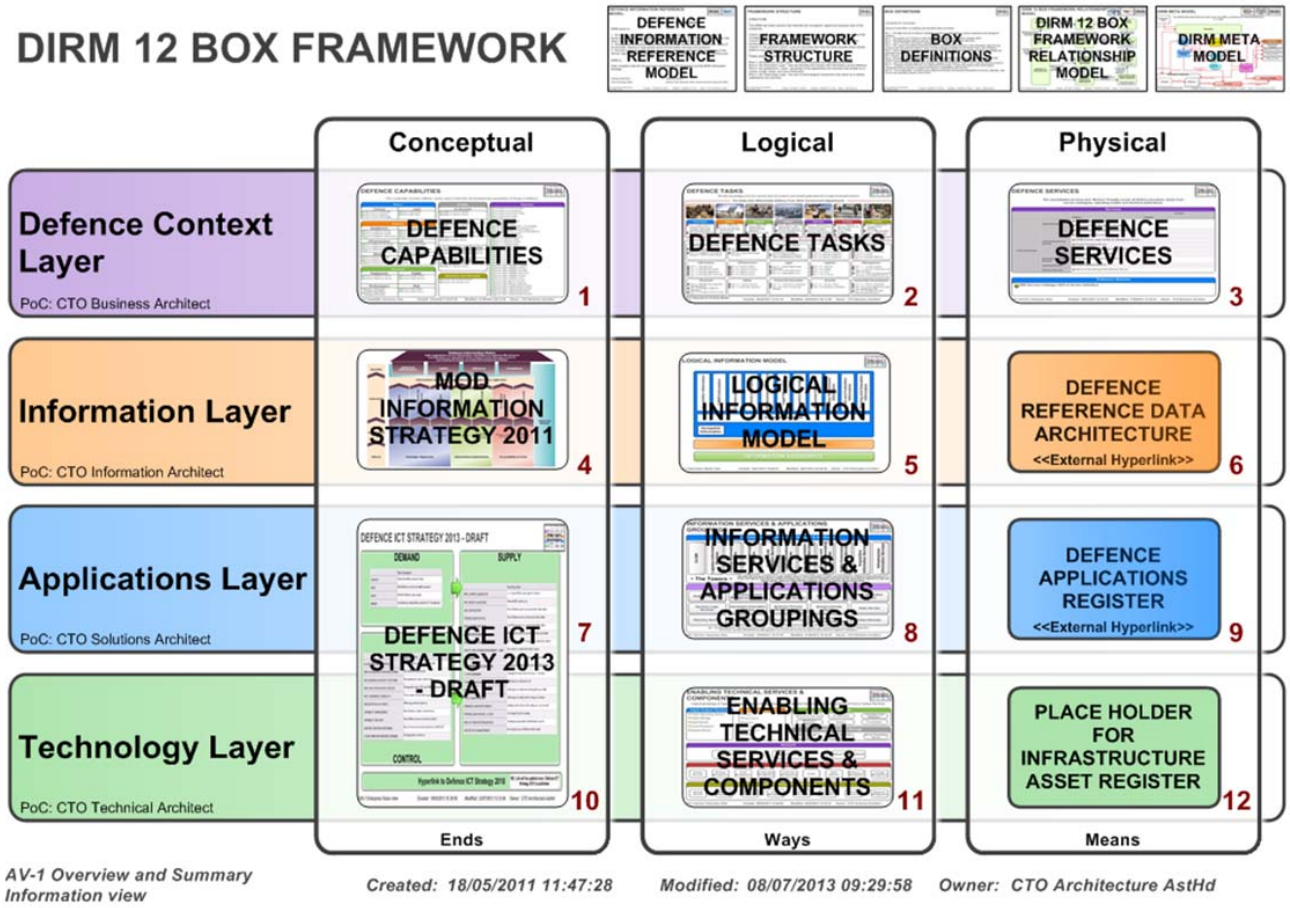
Regardless of methodology, procurement options should be informed by appropriate research and development, whether it is commissioned by Defence in its Science and Technology programmes or conducted, often at large scale, by the marketplace. However, current procurement methods frequently fail to identify appropriate intervention opportunities, and innovation is rarely fed into core ICT programmes in a timely manner. The Defence Authority for C4ISR is working with dstl and other scientific colleagues to ensure greater pull through of research and development into capability planning and, ultimately, into live service, including greater use of technology demonstrator programmes. Meanwhile, the CTO is examining how co-chairmanship of the Joint Information Group (under the Defence Suppliers' Forum) can be exploited to increase early visibility of pan-sector commercial investments in new technologies and good practices.

CONTROL

AN ARCHITECTURAL APPROACH – Understanding and reducing complexity

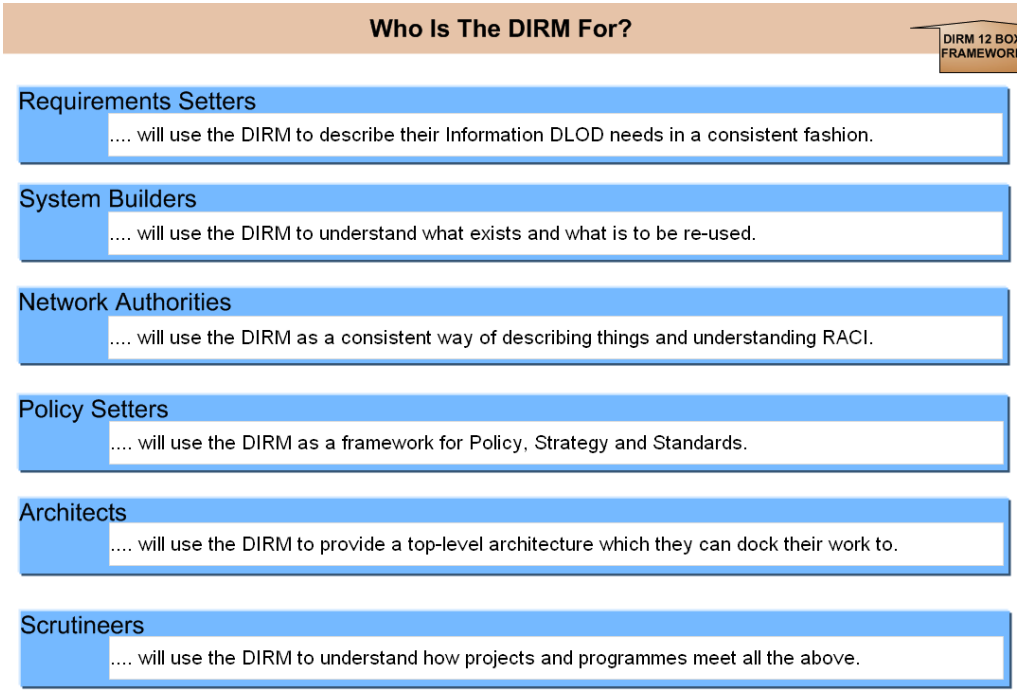
Coherent solutions and outputs are not natural products of an enterprise as large and diverse as Defence and must be managed. However, the same size and diversity argue against a centralist ICT governance model, which is likely to stifle agility and result in outcomes of the lowest common denominator; a federated approach provides the optimum balance of freedoms and constraints for Defence, capable of delivering outcomes of desired coherence and agility. Such an approach, must, however, contain sufficient central direction to prevent it from becoming decentralised.

Architectural disciplines have long been applied successfully to problems and solutions across the Defence enterprise, but they have until recently lacked the commonality of language and method to generate a coherent enterprise view. The creation in 2011 of the **Defence Information Reference Model (DIRM)** has provided the means to capture coherently the MOD architectural approach to its information domain, including ICT. The DIRM is an evolving expression of this domain, identifying and linking activities, policy, process and capability in a single coherent governance framework. Its primary purpose is to promote information and ICT re-use, coherence, interoperability and open standards across Defence. It provides a comprehensive framework that allows information capabilities to be described in a way that allows them to be consumed and shared across Defence. The DIRM 12 Box Framework is pictured below:



DIRM 12-Box Framework

The DIRM sits at the heart of Defence information and ICT coherence activities and has widespread applicability, as illustrated below:



DIRM Applicability

The DIRM has been constructed using models and standards set out in the MOD Architecture Framework (MODAF). It comprises a series of taxonomies, which provide the consistent terminology that should be used across Defence to describe ICT and C4ISR capabilities, and the relationships between them; in so doing, it describes:

- The broader Defence capabilities and activities that they support
- The information and data that these capabilities produce or consume
- The information and technology services that service the information needs and enable the information flows.

All the terms used in the Information, Applications, and Technology layers of the DIRM have definitions, policies and standards that apply, and a nominated point of contact who is the subject matter expert who 'owns' that part of the DIRM. This means that, in addition to providing consistent terminology, the DIRM will also name the post of the singular person responsible for ensuring architectural coherence in a specific area.

One of the main purposes of DIRM is to provide the basis for construction of ICT architectures within a coherent but federated architectural approach:

- The Reference Architecture is captured within the logical column of the DIRM, which defines the enduring set of abstract objects that provide the building blocks and terminology against which requirements can be described in a solution agnostic way.

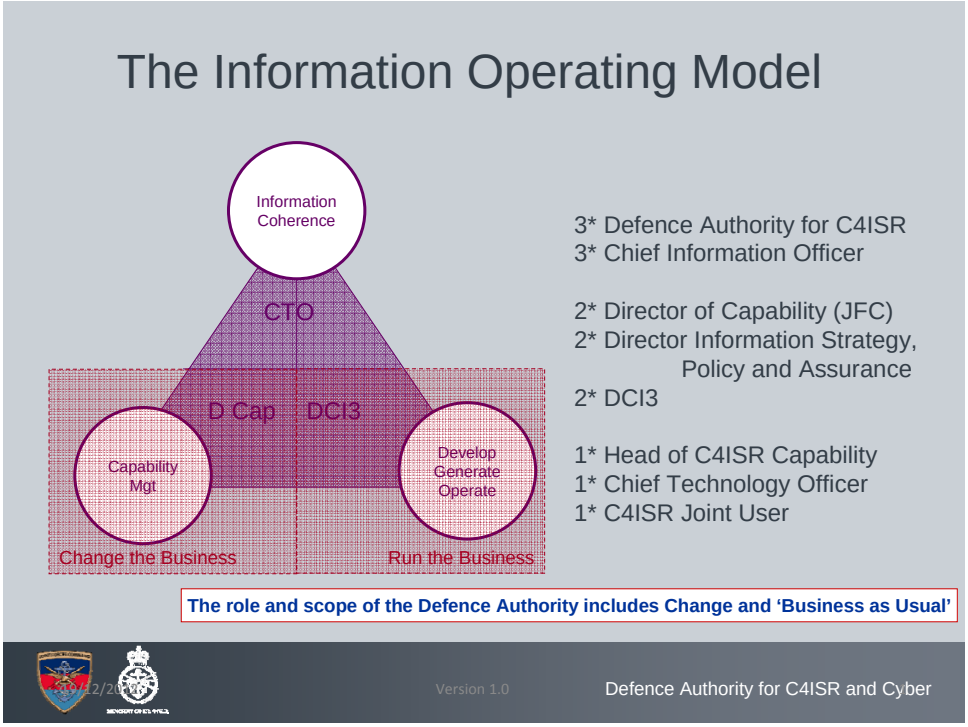
- The Baseline Architecture is the set of repositories that make up the physical column of the DIRM and define the 'as-is' (including programmed) components of the Defence information domain, categorised using the terminology of the Reference Architecture.

- Any one Target Architecture is a representative implementation of a capability in a specific timeframe, derived from strategic objectives and articulated in the context of the Reference Architecture components (or "building blocks") to enable cross-capability coherence. In capability terminology, the Target Architecture summarises the Capability

Management Strategy for a specific period of time and provides a benchmark against which new ICT propositions may be judged. The development of any Target Architecture will be an iterative process, starting with a high-level presentation of the concept in the Capability Management Strategy, and finishing with a more detailed description of the solution in the Target Architecture (as planned) at the emergence of the Genesis Option.

THE INFORMATION OPERATING MODEL – More effective governance

The 2012 Defence Operating Model created a leaner strategic headquarters focused on policy setting, and delegated appropriate responsibilities and accountabilities for enabling and delivering Defence outputs across MOD. While this better aligns authorities, functions and expertise, it also risks further degradation in the enterprise coherence of Defence information and ICT. Recognising this risk, Defence introduced an **Information Operating Model (IOM)** as a key component of its overall Operating Model, which was implemented from 1 April 2013.



The IOM comprised three key initiatives. First, it better empowered its **Chief Information Officer (CIO)**, enhancing his ability to enact Information and ICT strategy and policy and strengthening his roles as Senior Information Risk Owner and Information Skills Champion. It also gave the CIO greater direct control over ICT delivery, appointing him as Senior Responsible Owner for common information infrastructure programmes (such as DII, DCNS and the cryptographic programmes). Second, it established a Defence Authority for Command, Control, Computers, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR). Third, it created a new focus for driving coherence in the MOD Chief Technology Officer (CTO).

THE DEFENCE AUTHORITY FOR C4ISR – Recognising the value of information

Prior to Defence Transformation, MOD lacked a nominated senior proponent or champion for Information. Consequently, the value of Defence information was widely recognised across the enterprise but responsibilities for its exploitation were so diffuse as to limit their effectiveness. The appointment of Commander Joint Forces Command as the **Defence Authority for C4ISR**, enacted through the Chief of Defence Intelligence, secures the necessary focus and advocacy to drive change. It also clarifies responsibilities and gives leverage to the Joint User function exercised by Director of Cyber, Information and Intelligence Integration (DCI3), with responsibilities for advocacy, prioritisation, specialist advice and operational direction and guidance.

THE CHIEF TECHNOLOGY OFFICER – Driving information, ICT and C4ISR coherence

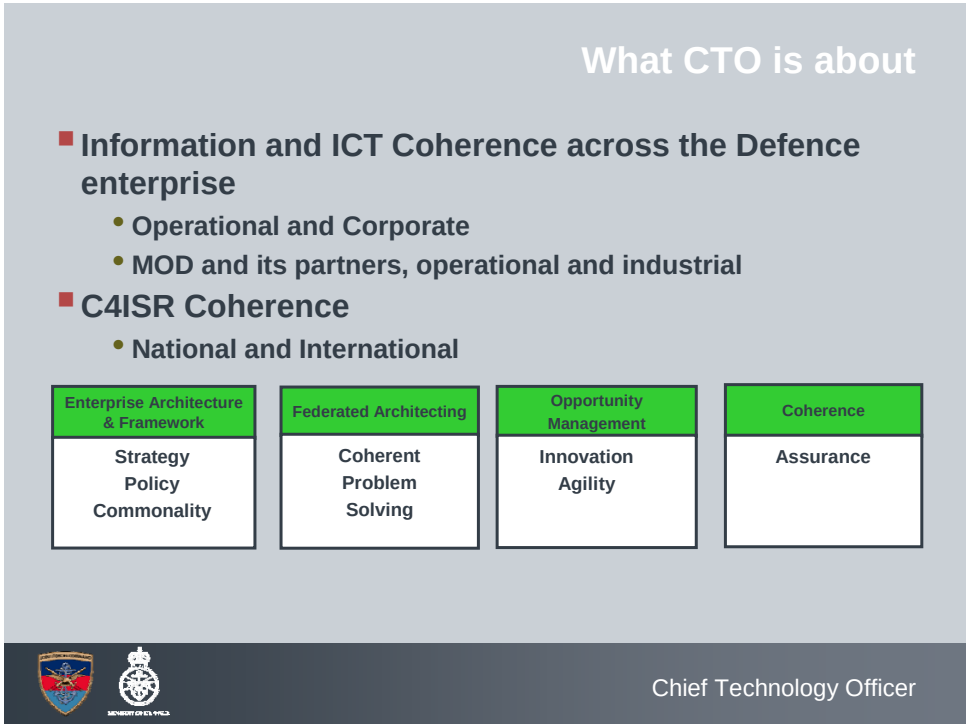
The Chief Technology Officer (CTO) is empowered by MOD to drive information, ICT and C4ISR coherence; coherence, in this context, is defined as alignment with strategy, compliance with policy and coherence with target architectures. The CTO is accountable both to the CIO for driving coherence in enterprise information and ICT, and to CDI (as the Defence Authority for C4ISR) for driving C4ISR coherence. In each case, this is to be achieved through prosecution of four functions:

- Opportunity Management. The CTO will provide the Defence Authority for C4ISR lead for Innovation, seeking both to better exploit emerging technologies and to imagine new uses and practices for existing capabilities. This function will comprise horizon scanning, technology exploitation and better access to, and use of, MOD and other science and technology investments.

- Architectural Framework. The CTO core team will provide the framework, methodology, standards and tools with which architecting is to be pursued consistently across the Defence enterprise. It will maintain the Architectural Framework (MOD moving to NATO) and its associated models and the DIRM for use by all. The CTO will also set enterprise architecture policy, lead the architecting community of practice and provide the Head of Discipline for Enterprise Architects within the IT Profession.

- Federated Architecting. Current architecting activities, conducted under a decentralised model, will be federated through application of ‘light touch’ governance that ensures sufficient standardisation to enable enterprise applicability and re-use of the work. Expertise and support drawn from the DE&S Engineering Group will ensure that C4ISR and ICT architecting complies with the broader System of Systems Approach (SOSA), in order to maintain its usefulness across SOSA domains. Early on, emphasis will be placed on embedding an architectural approach to capability planning across the seven TLB.

- Coherence Assurance. The CTO will direct the activities of the MOD ‘coherence community’, through his leadership of the **Network Authority Steering Group (NASG),** in order to ensure coherent outcomes in the planning, procurement and use of enterprise ICT and C4ISR. In particular, the NASG will be responsible for managing coherence issues that arise from the (often un-governed) inter-dependencies between MOD ICT projects and programmes, facilitated by an ‘enterprise technology roadmap’ provided by D ISS.



Where exceptionally the CTO is unable to resolve issues appropriately, he will escalate them to the 2* **Systems Direction Group** chaired by the CIO (and comprising planning, delivery and operational functions).

The CTO is also responsible to the CIO for drafting the Defence ICT Strategy and has delegated responsibilities for the setting of effective ICT technical policies. Where appropriate, the CTO is able to onward delegate policy responsibilities (e.g. to the Head of the Defence Network Technical Authority).

THE COHERENCE COMMUNITY – The provision of specialist support and expert advice

In fulfilling his responsibilities, the CTO will work with the MOD 'coherence community' operating as a virtual team; members include the **Network Authority**, Defence Security Assurance Services, DE&S Engineering Group (SOSA and the Joint Spectrum Authority) and the Defence Cryptographic Authority.

Where applicable, the CTO will also call upon the **Joint Information Group** formed under the leadership of the Defence Suppliers' Forum. The CTO has taken up the MOD co-chair of this Group from Director Joint Support Chain because the information and ICT issues with which its MOD and Industry members are grappling have enterprise-wide applicability and no longer pertain solely to the acquisition and logistics arena from which the Group has evolved.

These virtual team members are all available to Defence for the provision of expert advice and assistance.

THE NETWORK AUTHORITY – Enforcing coherent outcomes

The Network Authority is responsible for all aspects of network coherence, regardless of the nature of the network whether wired and wireless (spectrum-based connectivity) and operating at all security levels. The established Network Authority is to be retained in its three constituent parts; mandates have been updated to reflect the new Defence Operating Model and IOM. The Network Authority remit extends across the Defence enterprise and is not bounded by the organisations in which its constituent parts reside.

The Network Capability Authority (NCA). The CTO assumes responsibilities as Head of the NCA, although the NCA team will continue to reside within the C4ISR capability area of JFC. The NCA is responsible for managing the coherent development of requirements for new services, systems, platforms and applications that require support from the Defence network, by assisting sponsors with the identification of information requirements relating to their capabilities, and is subsequently required to capture these requirements in order that the Defence network is designed, built, maintained and configured appropriately.

The Network Technical Authority (NTA). The Defence NTA operates from DE&S ISS but will increasingly act as the C4ISR and Defence ICT Technical Architect, albeit with authority to onward delegate some responsibilities where appropriate; such onward delegations include the Above Secret Five Eyes Enterprise Technical Authority led by the IIS Delivery Team and the PRIDE CIS Systems of Systems Team led by the IMAGE Delivery Team. The primary purpose of the NTA is to provide technical leadership and due diligence for Defence ICT and to champion a risk-informed, Defence-first approach.

The Network Operating Authority (NOA). The NOA is exercised on behalf of Defence by the Head of Service Operations in DE&S ISS. The NOA is empowered to commission and authorise the full release of all systems onto the Defence network and to operate and defend the Defence network to meet priorities and to isolate services or users where failure to do so would prejudice other higher priority tasking or users. It also works with the NCA and NTA to understand and manage any differences between the designed intent for the Defence network and its actual function.

The constituent parts of the Network Authority and other members of the MOD 'coherence community' will continue to ensure alignment of activities and priorities through the **Network Authority Steering Group** under chairmanship of the CTO.

CAPABILITY MANAGEMENT – How Defence creates a coherent plan

The Head of Capability for C4ISR will continue to plan centrally the majority of MOD expenditure on ICT investments, albeit from within JFC rather than Head Office, and will ensure coherence of pan-Defence C4ISR capability planning across the remaining FLCs. Six Capability Planning Groups (CPG), each with an area of responsibility aligned to elements of the DIRM, will conduct this planning. CTO membership of each CPG will ensure application of good architecting practice, appropriate coherence assurance and opportunity management.

As endorsed components of the Capability Management Plan are passed through for delivery, the CTO will ensure that project and programme mandates include appropriate direction and guidance on the freedoms and constraints necessary to achieve coherent outcomes.

Where ICT investments are considered by other Heads of Capability across TLB, the CTO will rely upon the NCA team member allocated the lead for the relevant TLB to connect experts in both domains in order to secure a coherent plan.

Core corporate ICT investments are currently managed outside the Capability Management construct and necessitate different treatment. In this instance, the CTO must work directly with individual process owners, their agents (e.g. DBS), and the **Corporate Services Systems Convergence Programme** to drive necessary coherence. Over time, it will be more efficient to plan this ICT investment alongside other Defence needs in one area of responsibility and a study is currently being conducted to look at opportunities created by the arrival of a 3* CIO.

CAPABILITY DELIVERY – How Defence secures coherent solutions

Having shaped delivery activity through the original project or programme mandate, the CTO will need to ensure that all ICT investment propositions, regardless of approvals category, are appropriately vetted for alignment with strategy, compliance with policy and coherence with target architectures. In each case, professional and timely advice to approving authorities is required.

However, it would be inappropriate to impose a singular, centralist model to achieve this end and maximum delegation to trusted agents is key to coherent yet agile capability delivery.

To encourage re-use and to facilitate swift procurement, the CTO will work with the NTA to establish and publish acceptable patterns and templates for Defence to apply to its solutions with minimal oversight. Where the need demands a solution outside these norms, CTO and NTA experts will provide timely advice to solution providers and policy setters to agree an acceptable and bounded outcome.

While a relationship with interested parties can be maintained for initiatives in higher approvals categories, it will be difficult for limited, central resources to interact effectively with scrutiny and approving authorities dispersed across TLB considering lower category approvals. The CTO will therefore establish 'trusted agents' within each TLB who are qualified to vet ICT investment proposals on his behalf and either to advise the TLB CIO and local approving authority that they remain within a safe bound or to escalate them to the central coherence team for further consideration.

Scrutiny and approving authorities may seek advice on strategic alignment, policy compliance or architectural coherence at any point in a project lifecycle.

CENTRAL CONTROLS PROCESS – How Government exerts its influence on MOD ICT

While MOD has decided to implement a delegated Defence Operating Model, HM Government has concluded that it must impose a Central Controls Process in order to drive necessary reforms and to significantly reduce expenditure on public IT. However, the two regimes are not mutually exclusive and transformation of the Defence ICT landscape (as outlined in this Strategy) will make it increasingly easier to gain necessary Government approvals.

Direction and guidance on the handling of investment propositions through Cabinet Office and HM Treasury is available from the CIO Secretariat.

STRONGER INFORMATION GOVERNANCE – Driving transformation

Building on the successful implementation of the Information Operating Model and the creation of the Defence Authority for C4ISR, PUS has decided to drive Defence and ICT transformation harder through the establishment of a 4* Information Board (to be co-chaired by PUS and Commander JFC) and the recruitment of a 3* MOD CIO (to operate out of JFC but answerable to both Commander JFC and PUS).

Upon arrival in January 2014, the CIO will assume responsibility for the extant CIO organisation and the majority of ISS (which will both transfer to JFC ownership in Apr 14). An 'ISS Portfolio Study' is currently underway to determine the size and shape of the future ISS portfolio, with options to extract other C4ISR delivery components (e.g. ISTAR PDG1 and elements of D Tech Engineering Group) from DE&S and/or to transfer current elements of ISS (i.e. BATCIS) to another DE&S Operating Centre.

The transfer of ISS out of DE&S provides MOD with an opportunity to adopt a revised procurement model that better aligns with the Government Digital Services Manual and is more suited to the through life management of modern ICT services. The 3* CIO is expected to make recommendations early in her tenure.

Meanwhile, the CIO Systems Direction Group has launched an ICT Transformation Plan, comprising 10 work-strands centred on DCNS, which seeks to drive innovation and modern practice into DII, DCNS and related programmes. The Plan is being coordinated for CIO by the Head of CIO SRO Team.