Ministry of Defence

DEFENCE ICT STRATEGY

CONTENTS

1	CIO FOREWORD

Information and Communications Technology (ICT) is critical to enabling and supporting success on operations as well as the achievement of Departmental and pan-Government goals. Owing to the changing nature of operations some ICT requirements will remain unique to Defence. However, over the next 5-10 years we will see Government change the way in which it invests in ICT; the current Government ICT project review being a good insight. During this period Defence will become increasingly aligned with Other Government Departments (OGDs) as we realise the utility and benefits of common services.

This Strategy will address the following key areas:

- **The Requirement for ICT Investment.** The Strategy provides the strategic intent for the acquisition and use of ICT in clear and unequivocal terms and sets the scene for portfolio management of Defence ICT programmes and services in the future. It also describes how ICT enables the Department's operational and business processes to be more effective, efficient and agile, and sets out the Department's approach to reducing the year-on-year running costs for ICT.

- **Commonality and Economies of Scale.** The Strategy understands the unique requirements that drive the need for specialised ICT for Defence. However, it also recognises the opportunity and obligation to make more use of common ICT where our requirement is shared across Defence, OGDs, Allies and Industry.

- **Effective Control.** Traditionally, ICT budgets and investment have been de-centralised and because of this Defence has no way of establishing a clear picture of our total spend on ICT. If we are to reduce our year-on-year running costs we need better information capture, visibility and control in relation to Defence ICT spend.

- **Maximising Value for Money.** Ensuring that there is an enterprise-wide approach to supporting operational and business needs requires that all ICT investments should adhere to a common set of Guiding Principles. Application of the Guiding Principles enables re-use and maximised utilisation of existing ICT Services. Their application also allows for a simpler, more agile and more innovative approach to procuring new ICT Services, responsive to changes in operational and business need, and to technological advances.

The ultimate aim of this Strategy is to provide clear and concise direction on how we are to invest in and use ICT. As CIO for Defence, it is my pleasure to introduce the first issue of the Defence ICT Strategy which I commend to you. I expect to update and re-issue the ICT Strategy at appropriate junctures as the Defence Structural Reform Plans emerge, and I look forward to your support and engagement in the implementation of the Strategy.

John C T Taylor
Defence CIO
Ministry of Defence
October 2010

2 EXECUTIVE SUMMARY

The Defence ICT Strategy provides direction on how to invest in and use ICT to enable success on operations and the achievement of Departmental and Government goals through a common Value for Money (VfM) approach that supports local accountability. It looks out 10 years and its scope encompasses all of Defence including the need for interoperability with Other Government Departments (OGDs), NATO, Allies and Industry. The intent is that by more effective control and supply of ICT[1], Defence will become more **effective**, **efficient** and **agile**.

ICT is critical to enabling success on operations and to the achievement of Departmental and pan-Government goals. Owing to the changing nature of operations some ICT requirements will remain unique to Defence. However, much of the ICT required to support Defence is the same or very similar to that required by OGDs. Thus, to deliver VfM the key tenet of this strategy is that Defence will increasingly use common services across Government to support its objectives and will only use unique (or differentiated) services where the achievement of Departmental objectives necessitates this: **Defence shall strive to align its ICT across Government where possible, recognising that the achievement of the Departmental objectives is the highest priority**.

The CIO Systems Direction Group (SDG), led by the Defence CIO, will govern the implementation of this Strategy and the transformation to increasingly common services. The governance of Defence Networks and the delivery of ICT services is delegated to the Network Capability Authority, the Network Technical Authority and the Network Operating Authority. Through good governance Defence will ensure a focus on reducing costs, re-using existing services and applications, balancing risk against benefit and ensuring that we are agile in our approach to acquiring and using ICT. This will enable Defence to lower year-on-year running costs. To achieve this goal, ICT programmes and services will be scrutinised for adherence to this Strategy's 10 Guiding Principles. These will be applied to programmes and services from inception and through life.

Defence will work more closely with wider-Government and ICT suppliers to drive down costs through economy of scale. Work is underway to deliver a new approach to acquisition and maintenance of ICT services, led by the Defence Core Network Services (DCNS), which aligns with the OGC portfolio approach to improve agility, provide greater financial visibility and enable cost savings. Action is also being taken to ensure Defence extracts maximum value from its investment in applications through an Enterprise Approach to delivery and governance, including better re-use and utilisation of applications already acquired.

As ICT capabilities continue to evolve rapidly, a common services baseline will be derived to allow Defence to exploit better these new technologies. Many commercial and government organisations are gaining comparative advantage through using ICT to transform the way goods and services are delivered. Defence will look to embrace this trend by adopting best practice where it can and benefiting from a more co-ordinated approach to ICT innovation.

[1] Approximately 4.4% of Defence's operating costs

3 INTRODUCTION

The purpose of this document is to provide direction on how the Department is to invest in and use ICT[2] to enable success on operations and the achievement of Departmental and Government goals. Through adherence to the Guiding Principles laid out in this Strategy, better informed decisions will be made resulting in cost reductions and improved effectiveness from our ICT.

The scope of this document covers all Defence ICT programmes and services. These programmes and services are critical to enable the Department's Process Owners (PO)[3] and Top Level Budget-holders[4] (TLBs) to deliver their required outputs in support of the Defence objectives. Each PO and TLB is responsible for their own Defence Sub-Strategy[5], which in turn deliver the overall Strategy for Defence. The Defence ICT Strategy is designed to help shape the operational and business areas investment in ICT to deliver their respective outputs more efficiently and effectively and to derive best Value for Money (VfM) in ICT. The enabling relationship of the ICT Strategy to the Defence Sub-Strategies, including MODIS[6], is shown in the 'diamond' at Figure 1.

Learning from industry best practice the document uses Gartner's IT Strategy Toolkit as a baseline for its construct. Accordingly there are 3 major sections to the document:

Demand: The role of ICT in support of Defence outputs. This section will describe the context within which ICT is used to enable the achievement of Defence objectives and how the requirements for ICT will vary depending upon the nature of operations planned and unforeseen. It will also describe how ICT investment needs to change to improve effectiveness, efficiency and agility and to deliver ICT VfM.

Control: How Defence will govern the delivery and use of ICT programmes and services. This section will describe how management control will be exercised to ensure that the demand and supply for ICT services is matched through governance, prioritisation and VfM scrutiny.

Supply: A framework for the effective supply of ICT products and services. This section will describe a set of Guiding Principles to be used by operational and business areas when acquiring and utilising ICT services to deliver VfM.

To inform the subsequent development of a supporting plan for ICT each section highlights activities that are already taking place, activities that are planned (and may require resourcing) and activities intended for the longer term.

This is the first issue of the Defence ICT Strategy. It will be updated regularly, in line with Defence Structural Reform and wider Government ICT initiatives.

---

[2] 'Information and Communications' Technology

[3] Service personnel (Deputy Chief of Defence Staff (Personnel)); Civilian workforce (Director General Human Resources and Corporate Services); Healthcare and medical operation capability (Surgeon General); Information management (Chief Information Officer); Corporate communications (Director Media & Communications); Logistics (Chief of Defence Materiel (supported by ACDS (Log Ops))); Financial management (Director General Finance); Commercial (Director General Defence Commercial); Health and Safety, Environmental Protection and Sustainable Development (2nd Permanent Secretary (supported Director Business Resilience)); Security and Business continuity (Director Business Resilience)

[4] Navy Command; Land Forces; Air Command; Defence Equipment and Support (DE&S); Defence Estates (DE); Permanent Joint Headquarters (PJHQ); Central TLB (CTLB)

[5] Strategy for Defence is delivered by a number of sub-strategies which are owned by: Royal Navy; Army; Royal Air Force; Capability; Logistics; Defence Estates; Service Personnel; Civilian Workforce; Sec Pol & Ops; Acquisition; Commercial; Corporate Communications; Financial Management; Healthcare and Medical Operational Capability; Information Management; Safety; Environmental Protection and Sustainable Development; Security; Business Continuity

[6] MOD Information Strategy 2009

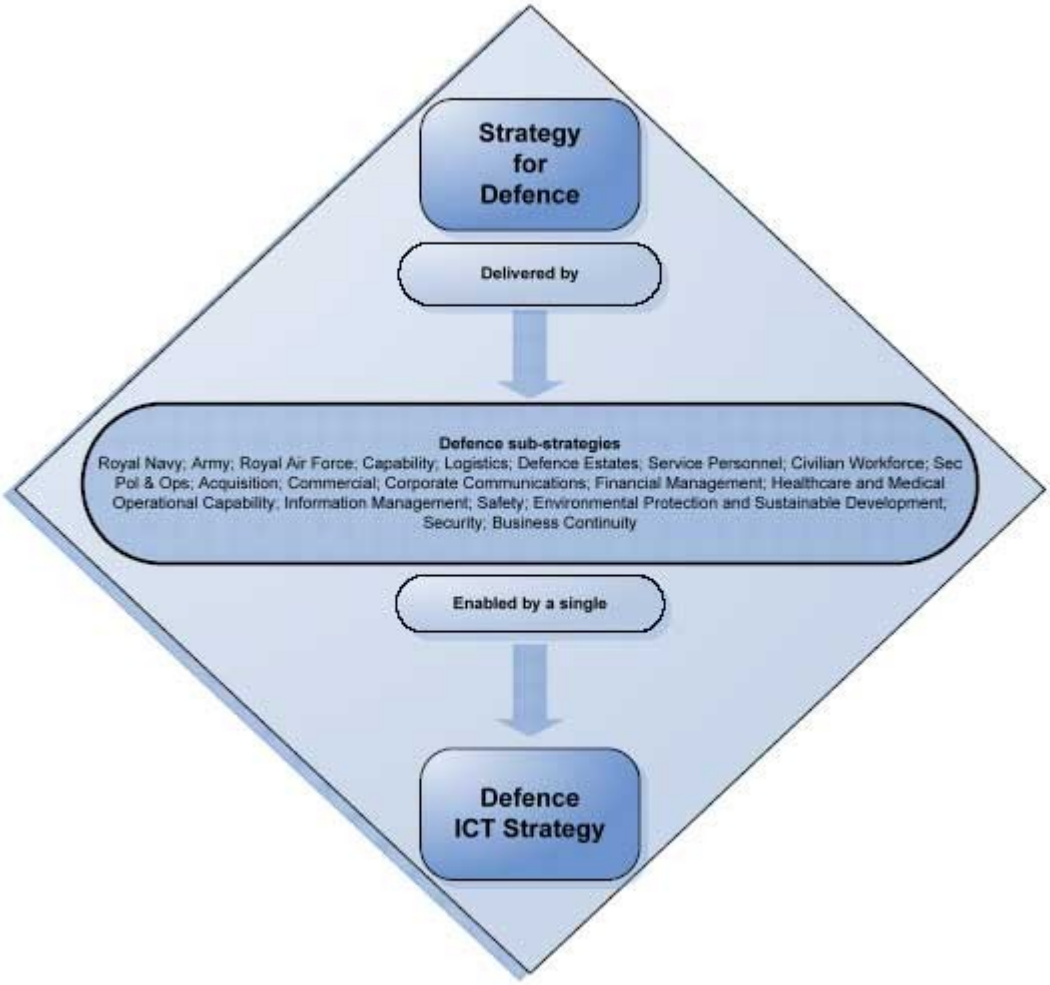


Figure 1 – The Defence Strategy 'Diamond'

4	DEMAND

CONTEXT

Defence has a key role to play in a World where change is both far reaching and fundamental. To deliver this role effectively and efficiently the Defence Plan 2010 lays down Defence objectives as articulated in the Defence Board Strategic Objectives (DBSOs). Defence is required to deliver these objectives using agreed processes, suitably trained staff and battle winning technology. Funding to deliver these objectives is delegated to the three Services, managed by their respective Front Line Command (FLC) and other TLBs. In addition, a number of POs are appointed to bring uniformity and good governance to key cross-cutting processes such as finance, HR and Information Management. Whether a TLB, FLC, Trading Fund, Agency or PO[7], all are investing in ICT to achieve the Defence Objectives and in particular to:

- **Achieve success in the military tasks we undertake, at home and abroad[8].**
- **Be ready to respond to tasks that might arise.**
- **Build for the future.**

The current annual Defence operating costs to deliver these outputs is £37bn. ICT is a key enabler of these outputs, with current spend accounting for about 4% of the Department's operating costs. By delivering more efficient and effective ICT services this 4% can significantly improve how the remaining 96% is utilised to deliver Defence outputs.

To deliver better VfM and reduce costs, Defence must ensure that more control is applied to how ICT programmes and services are delivered and supplied; this will include establishing a better understanding of the current ICT portfolio and associated costs and how these could benefit from wider Government initiatives.

The Government, through the CIO Council, is seeking opportunities to deliver ICT efficiencies by removing unnecessary overlaps between Departments and avoiding costly duplication of capability acquisition. This started with the recent ICT Moratorium initiative and will be continued with the impending publication of a new Government ICT Strategy, which coincides with the Department's own activities to focus on effectiveness, efficiency and agility within ICT. These factors are also a major focus of the Strategic Defence and Security Review (SDSR), the Spending Review and Defence Structural Reform.

It is recognised that the ICT required to support much of Defence is the same or very similar to that of Other Government Departments (OGDs)[9]. However, in some cases the ICT requirements are unique to Defence or to the National Security Council members (such as deployed operations or intelligence). Within the Cyber context ICT may be viewed as a weapon system and is therefore subject to an 'ICT arms race' whereby countering threats to National or Allied ICT capabilities is vital to operational success. Defence must also interoperate with various actors, as depicted at Figure 2, and although this presents different ICT challenges depending who these actors may be and how they may vary during a campaign, there are opportunities for better alignment. Ultimately our goal is to deliver better VfM from our investment in ICT and **Defence shall strive to align its ICT across Government where possible, recognising that the achievement of the Defence objectives is our highest priority**.

[7] Referred to collectively as 'Operational and Business Areas' in the rest of the Strategy

[8] ICT plays a critical role in current operations in Afghanistan and elsewhere world-wide as well as on contingent operations

[9] For example the requirement to respond to FOI requests

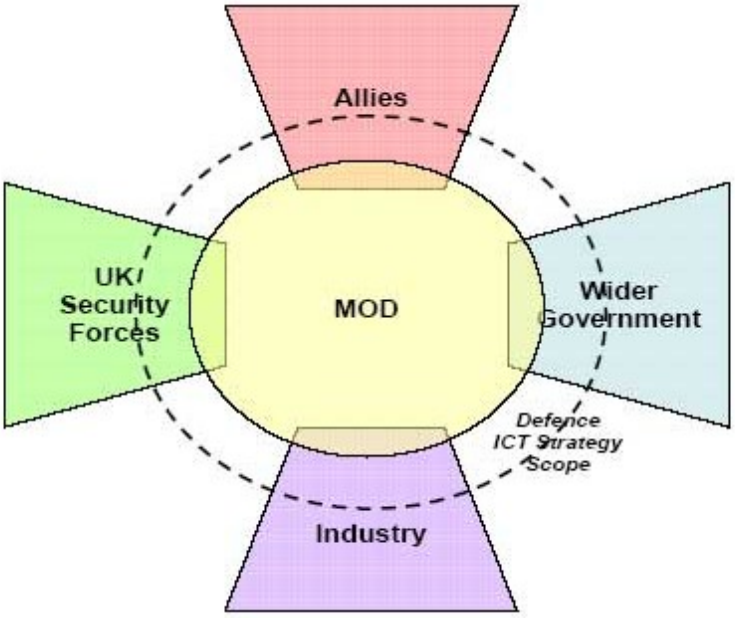


Figure 2 – Opportunities for better alignment

CHANGING ICT INVESTMENT

Defence ICT needs to be more **effective** so that we can improve our work with Allies, OGDs and Industry. It also needs to be more **efficient** so that we can reduce our year–on-year running costs. Our ICT will need to be more **agile** in order to respond to the changing needs of our operational and business users and to respond to the pace of technological change in the ICT industry.

Over the course of the next 10 years Defence will increasingly use common ICT. Only where there are unique Defence requirements (such as Operational, Security or Intelligence) will dedicated (or differentiated) ICT be allowed[10]. The challenge for Defence is therefore to understand better where ICT investment should be aligned with wider Government initiatives and to support these activities, while preserving those capabilities that are unique and are required to deliver the Defence objectives.

The change in ICT investment promoted by this Strategy is best summarised by Figure 3.

The **2010 diagram** represents the 'present state', where some services are common[11], acquired and supplied to Defence by our specialised ICT supplier organisations[12]. The remaining 'differentiated[13]' services are procured across Defence by operational and business areas; these tend to be unique to Defence to support the full range of military operations.

The **2020 diagram** is our desired 'future state', where more of our services are common across Defence and wider Government; these services will be purchased by users from Government or Defence catalogues and may be supplied to OGDs by Defence. The remaining differentiated services continue to be acquired to deliver unique 'mission-winning' effects. Although these differentiated services will be procured by the relevant mission experts, they will be subject to a rigorous approvals process to ensure coherence and VfM.

[10] This aligns with the application of the SOSA Rule Book to drive down diversity in the ICT systems that generate Defence capability

[11] Examples include: Defence Information Infrastructure, the Defence Fixed Telecommunication Services and Joint Personnel Administration

[12] Includes D ISS, Supply Chain, SPVA and PPPA

[13] Differentiated ICT – that which supports unique Defence requirements – such as mission support systems

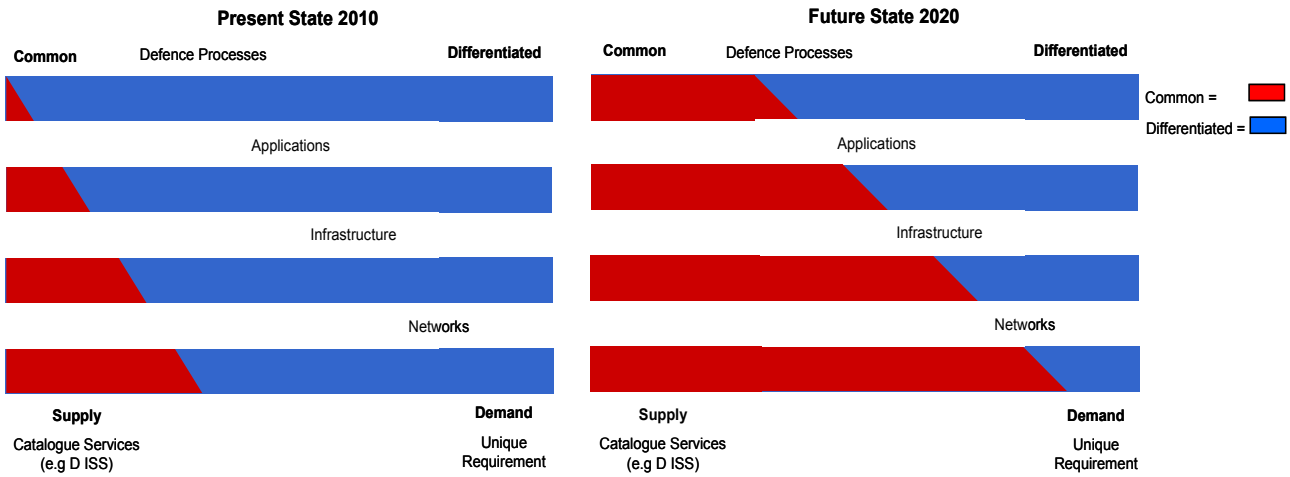


Figure 3 – Changing ICT Investment

Innovation

If Defence is to deliver the ICT services required in a much more cost effective manner - more for less – then we must be more innovative and agile in how we source and deliver new ICT capabilities. In particular, we must improve exploitation of the technologies and innovations developed in the commercial world and across Government; by doing so Defence can expect to:

- Improve the use of ICT to enhance the delivery of military capability.
- Maximise the return from our ICT investments.
- Find new ways to drive down the cost of providing ICT services.

Innovation is playing a key role in existing ICT projects being delivered and Defence is participating in a number of collaborative ICT innovation activities such as the Information Assurance Technical Programme (IATP). However, the CIO study[14] recognised the need for centrally driven, information-led innovation to ensure that opportunities are fully realised and to avoid uncoordinated or competing initiatives. CIO plans to lead the way in building a portfolio of innovation work to help derive maximum value from the investment being made. In particular, CIO will:

- Identify evolving best practice in the use and exploitation of ICT in the commercial, Government and Defence environments and sponsor and coordinate the adoption of that best practice across Defence.
- Deliver a series of initiatives to help those sponsoring and delivering ICT rich programmes to innovate effectively.
- Develop a process to identify innovation opportunities in conjunction with stakeholders. Stakeholders will manage and coordinate delivery.

[14] CIO study completed February 2009 – conducted by KPMG.

Innovation Example - IATP

Defence is an active participant in the cross-Government Information Assurance Technical Programme (IATP) to develop future sovereign capabilities and produce innovative solutions to Information Assurance (IA) issues. Defence fulfils the roles of Senior Responsible Owner and Programme Director for the IATP delivery on behalf of HMG. Defence will continue to embed the IATP solutions into the delivery of ICT capability.

OUTCOMES AND BENEFITS

Successful implementation of this ICT Strategy will contribute significantly to the following outcomes for Defence:

- Success on Operations.
- A better understanding of how ICT enables Defence to meet its operational and business objectives within the broader context of the Government ICT Strategy.
- A better understanding of ICT investment and how to manage effectively the portfolio of ICT change activities to deliver required benefits and savings.
- Increased re-use and exploitation of ICT services and applications.
- Clearer direction to ICT projects on investment decisions to inform:
  - Technology choices.
  - Compliance with standards.
  - Acquisition and supplier relationships.
- Support to cross-Government and Allied Government ICT initiatives.
- Delivery of year-on-year ICT operating savings to allow re-investment in new battle-winning ICT capabilities.
- Up-skilled staff who are better at exploiting ICT.

Through the application of, and adherence to, the Guiding Principles set out in this Strategy, Defence can expect to realise the following benefits:

Effectiveness:

- Following common agreed standards we will increase the degree to which information can be exchanged seamlessly between areas of Defence, within Government and with Allies; increasing effectiveness and agility.
- Understanding where Defence's needs are truly differentiated will enable us to focus our future investments.

Agility:

- By using a standard approach to capture operational and business information flows a simple Architecture will be created. This Architecture will allow processes to be more interoperable and in turn lead to agility for the business. This agility will be derived from being able to re-use services, utilise all features of existing applications and rapidly procure new capability as the military mission, or the business need, changes.

Efficiency:

- Maximum efficiency will be realised by fully understanding and controlling our ICT cost baseline and drivers. Defence will be better positioned to drive down year-on-year ICT operating costs in addition to the cost savings that have already been assumed for current programmes.[15]

- Defence can benefit from, and play its part in, reducing pan-Government ICT costs through greater cross-Government collaboration and shared ICT, particularly where our ICT requirements are synonymous with OGDs.

CIO plans to lead on devising and agreeing suitable metrics and key performance questions to measure the attainment of the benefits. Progress towards achieving these benefits will be reported regularly to the relevant governance bodies to allow adjustment to priorities and investment decisions.

[15] Cap CCII has built in a 25% reduction in the replacements for DFTS, DII, DHFS and Skynet5

5	CONTROL

GOVERNANCE

The Defence CIO will own the ICT Strategy and related policies. Governance of the ICT Strategy, including its Guiding Principles, will be sponsored by the **CIO Systems Direction Group (SDG).** The Defence CIO will represent the Department's interests on the CIO Council to ensure that Defence interests and ideas are presented to shape cross Government policy and that Government ICT policy and initiatives are understood and implemented within Defence, where applicable.

Effective governance of ICT acquisition will ensure that Defence achieves VfM by balancing the demands from operational and business areas with the supply of enabling ICT. The right balance will mean Defence processes can operate smoothly, whilst ICT services are delivered efficiently and cost effectively. To achieve this, investments must remain compliant with corporate standards and the Guiding Principles outlined in this Strategy.

The adoption of the ICT Guiding Principles will result in more effective scrutiny and tighter control, albeit with ICT budgets remaining devolved to operational and business areas. To ensure balance, these organisations must identify and communicate their ICT requirements to demonstrate that they are vital to enable Defence outputs. CIO will operate in partnership with these business areas to ensure they understand their responsibilities and provide direction where necessary, particularly with regard to VfM decisions such as re-use and the use of a common approach. In conjunction with these areas and the, to be formed, **Defence Business Services**[16] organisation, CIO will collaborate to ensure that systems are coherent by using an Enterprise Architecture (EA) approach to connect business and ICT requirements and to ensure a coherent, logical and complete solution.

CIO will be the lead, as part of the Investment Approvals Board (IAB) process, for scrutiny and approval of ICT Services for Defence acquisition programmes, which are expected to adhere to the Defence Acquisition Operating Framework (AOF). Scrutiny will test that all ICT programmes and services are compliant with the ICT Guiding Principles; ICT specific requirements from projects and Urgent Operational Requirements (UORs) will be governed by network authorities. This will apply to **all** ICT projects, irrespective of size and delivering operational or business area.

Governance of the Defence Network and the delivery of ICT systems and services is delegated by the CIO to network authorities. The network authorities have the following remit:

- The **Network Capability Authority** (NCA), led by Deputy Chief of Defence Staff (Capability) (DCDS (Cap)) and delegated to Head of CCII, will ensure that the impact of future ICT investment decisions on the Defence Network is fully appreciated and prioritised. This will require the identification of the information requirements necessary to support the development of new capabilities across all capability areas and Process Owners. This includes Equipment Programme (EP) activity as well as UORs, Urgent Operational Tasking (UOT) and Non-Equipment Investment Programmes (NEIP). The aggregated information requirement for each capability will be used to develop a coherent solution through the Network Technical Authority and respective delivery teams.

- The **Network Technical Authority** (NTA), under delegation from Chief of Defence Materiel (CDM), will provide technical coherence, and will own and manage the Command, Control, Communications and Computing (C4) elements of the System of Systems Approach (SOSA) which describe the policy, rules and principles for

[16] A new organisation proposed by the Grimstone review

joining the Defence Network. Through Defence Equipment and Support Information Systems and Services (DE&S ISS) Programmes, the NTA will be responsible for developing the technical solution to meet the capability requirement developed previously by the NCA.

- The **Network Operations Authority** (NOA)**,** led by the Head Service Operations, under delegation from CDM, will provide operational configuration control and day-to-day operational management of the Defence Network and defence against the cyber threat.

An NCA led **Applications Governance Working Group** has been stood-up to provide better governance of how Defence applications are acquired and maintained through life and has issued draft principles through which the acquisition of applications will be undertaken.

RESOURCE MANAGEMENT

Defence operates de-centralised budgets, including ICT budgets, to deliver its strategic objectives. This must be balanced through central oversight and control, ensuring:

- ICT enables operational and business areas to deliver efficiencies across the enterprise, leading to continuous improvement and more effective Departmental outputs.
- ICT will be provided efficiently and the 'run and maintain' cost will be driven down year-on-year.
- ICT procurement will take sustainability into consideration.

Approach

CIO will lead on measuring ICT spend to deliver VfM. This will help ensure that the right ICT capabilities are provided to the Department and that they are delivered in a cost effective manner. By comparing Defence's performance with other similar enterprises, we aim to be amongst the best performing. MODIS articulates the need for Defence to provide optimum return on ICT investments in order to assure VfM.

To enable the delivery of VfM and the measurement of performance, CIO plans to:

- Measure how much Defence spends on ICT.
- Establish a reliable process for measuring VfM for ICT investment, with the focus on achieving the optimal benefit for Defence within available resources.
- Set targets for reducing year-on-year ICT "run and maintain" costs, which may enable re-investment opportunities to deliver further improvements.

Benchmarking

Government requires all Departments to deliver a reduction in ICT "run and maintain" costs, although precise targets have yet to be agreed for Defence. To address this CIO has already begun to measure how much we spend on ICT through Government-wide benchmarking[17] exercises. The reported Defence ICT spend for Financial Year 2008/09 was **£1,727M** and for 2009/10 was **£1,784M[18].** These figures provide us with a benchmark. However, the information gathered was not complete and is not sufficiently granular to support improvements to VfM. Therefore, a review is ongoing into the method for information capture

[17] Benchmarking undertaken to specified set of Government standards

[18] Run and maintain, and project costs

and will include the feasibility of making changes to the Department's accounting system[19] to reflect ICT spend. Once complete, CIO will introduce further changes to the benchmarking process to ensure we extract the required information.

ICT Review

In addition to the benchmarking, during summer 2010 CIO conducted a review of ICT projects underway within Defence, in support of a Cabinet Office and Her Majesty's Treasury (HMT) initiative. This review was to ascertain if ICT projects:

- Were key to delivering required Defence outputs and were consistent with Government priorities.
- Can be delivered based on their past record of keeping to time and budget and will deliver the agreed outcomes and a positive net present value or return on investment.
- Could be delivered in a different or more cost effective way - by merging with other projects or significantly reducing the scope/ complexity of the requirements.

In total 277 projects were reviewed, 249 of which were excluded because they: provided direct support to 'front line operations'; were business as usual; or involved a specialist supplier – these exclusions reflect some of the unique aspects of Defence. While the picture gained is far from complete it has allowed Defence to begin gathering a baseline of ICT investment. Going forward, CIO will build upon this activity and continue to scrutinise all ICT projects based on the above criteria and alignment with the ICT Guiding Principles.

ICT Investment

The ICT Project review identified projected run and maintain costs, excluding project costs, for the next 5 years to be:

- 2010/11 £1.447bn.
- 2011/12 £1.402bn.
- 2012/13 £1.411bn.
- 2013/14 £1.411bn.
- 2014/15 £1.399bn.

These figures are pre-SDSR and Defence Structural Reform. Accordingly, they are expected to be revised downwards as the future size and structure of Defence becomes known and efficiency targets are agreed. As a guide and using the existing benchmarks, **it is expected that Defence's future ICT spend will be about 4.4% of MOD's Departmental Operating Expense**. This value is in line with the overall UK Public Sector average, and Gartner's 4.3% Peer Group comparator for Defence[20]. This Strategy sets the conditions to allow Defence to meet these targets by promoting a process that allows better identification of ICT costs and increasing the robustness of the efficiency targets.

In addition to setting appropriate efficiency targets, the Department must comply with Government initiatives issued via the Cabinet Office concerning the awarding of ICT contracts. This includes the intent to issue Government policy that directs that future ICT projects are to be designed with the presumption that they will not have greater than £100M

[19] The Chart of Accounts

[20] Source: Cabinet Office ICT projects review

total lifetime contract costs. Exemptions will be allowed if it can be demonstrated that by not endorsing the project will significantly increase the overall cost to the taxpayer, notably increase the risk of failure or increase the security threat. These changes will have implications for how Defence procures ICT capabilities, including the need for a systems integrator to manage potentially more numerous contractual interfaces. Such changes will be supported by the Department's intent to move towards an EA approach for defining and specifying requirements and the DCNS acquisition process that offers better agility and more incremental delivery. CIO will work with Defence acquisition organisations to ensure compliance with the policy.

RISK MANAGEMENT

In balancing its approach to ICT, risk Defence faces two conflicting tensions; on one hand to guard against the increasing **threat** from loss of data or service, whether accidental or through malicious act such as cyber attack; on the other hand to exploit the **opportunities** provided by innovative technologies and new generations of open source and Commercial Off The Shelf (COTS) applications. Such technologies offer the potential to deliver benefits through automating business and operational processes, but do not necessarily comply with Communications-Electronics Security Group (CESG)[21] standards or formal security certification requirements. However compliance is rarely as simple as a pass/fail test; appropriate risk/balance is key.

CIO is the Senior Information Risk Owner (SIRO) for Defence, ultimately responsible for accepting Information Risk within the Department. CIO will work with projects to advise them to ensure the **right balance is struck**. In particular the Risk, Capability, Cost balance should be considered in any investment decision process. Too often projects over-specify the required capability and costs escalate as a result. Alternatively projects, accreditors and scrutineers seek to push risk down to ever lower levels, again escalating costs for little return and stifling the opportunities that a new technology may offer. Too often Defence projects are risk averse and slow to adopt new, innovative technologies which offer significant benefits at little cost. If in doubt, ICT project managers should consult the CIO for advice.

CIO, NTA, Defence Security and Assurance Services (DSAS) and CESG staff will work to provide better guidance:

- To developers and system integrators regarding making COTS solutions secure.
- To project security advisors and accreditors regarding assessment of risk and raising a **risk balance case** to the SIRO.
- To project staff regarding weighing up cost savings and business benefits.

The aim should be that project security advisors and accreditors are able to provide a fully evaluated risk balance that enables the SIRO to make an informed decision for the benefit of Defence. In particular does the security risk posed to the Department of using an application or technology exceed the cost savings and business or operational benefits that use of the application would deliver? Project approval will be helped if projects demonstrate the **appropriate** risk/capability/cost balance case.

[21] The UK HMG National Authority for Information Assurance

ICT GUIDING PRINCIPLES

To ensure Defence ICT effectively enables the Defence Objectives we shall:

- Take an **Architectural Approach** to acquiring and using ICT, allowing the Operational and Business needs to be planned, understood and coherently delivered.

- Use common **standards** in that architecture to make delivery and re-use simple and better enable interoperability.

- Use common **services and processes**, aligned across Defence and Government and fully integrated with the enabling application to increase effectiveness and efficiency.

- Provide **common applications** from a managed portfolio that maximises reuse, fully exploits Off The Shelf (OTS) solutions and minimises the reliance on bespoke solutions.

- Manage an effective **network** and **infrastructure** that is **secure** and **sustainable** and common across Defence, Government and Allies where appropriate.

- Provide **staff** with the skills needed to exploit the capabilities provided and carry out their responsibilities more effectively.

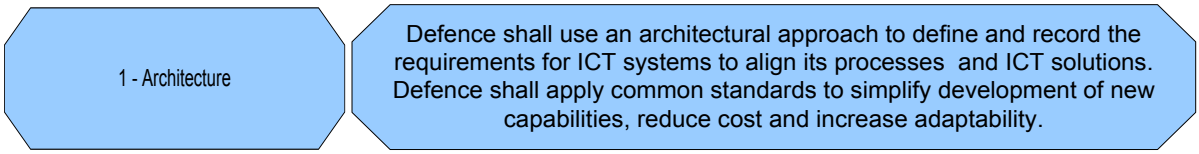
- Be effectively **structured** to govern, acquire and manage ICT to meet Defence needs such that costs are reduced, effects are maximised and operational risk is minimised.

A summary of the ICT Guiding Principles is documented in Table 1 below with more information on the rationale for each principle and the activities involved, provided in the remainder of this section of the Strategy. ICT programmes and services are expected to adhere to these principles from inception through life. This will be enabled through the application of the SOSA Rule Book. Any divergence from (or resolution of conflicts in application of) the principles will be managed by the CIO, or by the delegated network authority.

1 - Architecture	Defence shall use an architectural approach to define and record the requirements for ICT systems to align its processes and ICT solutions. Defence shall apply common standards to simplify development of new capabilities, reduce cost and increase adaptability.
2 - Interoperability Standards	Defence shall agree Interoperability Standards that are coherent with those laid out by NATO and Allies, recognising the need to interoperate with OGDs, NGOs and industry.
3 - Shared Services	Defence shall migrate its corporate processes towards using Shared Services, either Defence-wide or pan-Government, adapting processes where necessary to minimise diversity.
4 - Applications	Defence shall rationalise and standardise its applications portfolio and enhance the delivery of applications services such that applications can be re-used across Defence, Government and with NATO and Allies
5 - Networks	Defence shall develop its network such that it is interoperable with Allies, OGDs and industry, making use of pan-Government services (such as PSN) where appropriate.
6 - Infrastructure	Defence shall continue its drive towards standardising its User Access Devices and shall rationalise its Data Centres to provide ICT programmes with a common infrastructure.
7 - Sustainability	Defence shall ensure that Sustainability is recognised and embedded across all Defence ICT programmes in order to deliver or exceed government targets
8 - Information Access and Assurance	Defence shall address the pervading risks and strike an appropriate risk balance to ensure operational success
9 - Skills and Training	Defence shall develop the professional competences and skills of IT specialists and shall ensure that all staff have the requisite skills needed to use and exploit Defence ICT systems.
10 - Structure and Sourcing	Defence shall engage with industry to provide greater visibility of its ICT intentions and allow industry greater influence in shaping our future ICT solutions. Defence shall use project management best practice to deliver new capabilities effectively.

Table 1 – ICT Guiding Principles

ARCHITECTURE



Defence must become more efficient as well as more effective in its information exploitation. Efficiency and effectiveness are achieved through a greater understanding, and better management, of the flow of information along (and between) end-to-end processes, and of the way in which that information is utilised at key points.

This greater understanding and better management is to be achieved by establishing an EA, a standard approach to the capture of information about the Department that brings clarity and simplicity to an otherwise complex picture and supports improvement. The initial focus will be on information needs and flows and how these best enable the delivery of required outputs, operational agility and the necessary Departmental transformation. Defence has already successfully used EA on Mission Threads.[22]

Architecture Example - Helping to Improve Operational Effectiveness

The RAF, supported by Industry, has produced in excess of 20 'Mission Threads' using an architecture approach to improve shared awareness between operators and the acquisition community to improve operational effectiveness. Operators, including aircrew, were interviewed to establish their Tactics, Techniques and Procedures (TTP) and capture these in an operational view. Using this view, information flows were mapped and critical technology identified. The resulting benefits have included: clarity of TTPs across the operational community (including other Services and Allies); identification of capability gaps from information flows to allow focused investment; and capture of spectrum usage to inform decisions on future spectrum needs of Defence. Ultimately, this has delivered cost savings by targeting investment only where it is needed and improved the operational effectiveness of our Armed Forces.

Defence is too large, complex and diverse to capture all the relevant detail regarding information needs and flows in a single, meaningful view. Appropriate granularity will be achieved through the development of a federation of architectures that adequately describe and shape various processes and domains within the Defence community. However, each of these architectures will themselves conform to agreed architectural principles covered in detail in the Defence EA Strategy and the SOSA Rule Book that will form the basis of corporate governance.

As each PO seeks to shape the end-to-end processes for which they are responsible, they will capture and refine their information needs and flows. In parallel, operational and business areas will capture how information needs are to be satisfied and how assured information is to flow throughout their organisation in order to enable the required output[23]. By ensuring consistency in this capture, the CIO will be able to identify and share common and best practice, thereby enhancing coherence and efficiency at an enterprise level. The combination of these architectures will permit Defence to understand better its information

[22] An example is the Close Air Support Mission

[23] This will build upon the high level analysis of the defence information flows which were documented during the Defence Information Assurance Architecture study. This study provides the most detailed analysis of the MOD business domains (e.g. Military Capability, Military Operational Human resources, Finance etc.) and the "Trust Zones" this information needs to flow across (e.g. between MOD and Government, allies, industry, NGO, NHS, EU etc.)

needs and to identify safe, efficient and effective information flows. This, in turn, will allow more efficient and more effective investment in enabling ICT that supports the evolving business and operational needs.

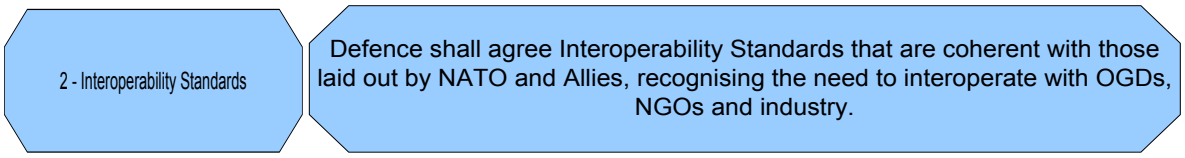
The ICT solution will conform to a technical architecture, using SOSA. New investments will be governed against this architecture, as exercised by the Network Capability and Technical Authorities, while the Network Operating Authority will ensure the continued compliance of in service solutions.

Given the unique infrastructure requirements on Deployed operations the NTA has created a Deployed Technical Architecture (DTA) to shape and ensure the coherence of the ICT services provided through EP and UOR funding. The DTA provides architectural guidance, logical/conceptual models and design principles, for contingent capability and current operations. This includes a set of standard designs that can be implemented dependent on the bandwidth available and the applications required at each deployed location.

Architecture Example – Improving Programme Delivery

The Logistics Network Enabled Capability (Log NEC) Programme has used EA to describe the relationships between strategy, process, information and information systems and services. The Log NEC Architecture provides system views and business viewpoints and has been very successful in providing support to the Future Logistics Information Systems (FLIS) programme. By presenting simple views of the problem the architecture has enabled important decisions on Management of the Joint Deployed Inventory (MJDI) future technology requirements and Air Movement Operations (AMO) solution architecture to be made and saved the programme £3.5M and avoided significant additional costs. As importantly an architectural approach has provided the Log NEC Programme with a methodology for planning and decision making which ensures a more robust and agile process.

INTEROPERABILITY STANDARDS



Defence ICT interoperability is a critical enabler. It ensures that Defence is able to communicate, operate, train and exercise in the execution of missions and tasks and can enable the critical business activities that provide the enduring support. This interoperability must be considered from 'Factory to Foxhole'. Each conflict and Defence operation is unique and the military response required must be tailored to meet objectives, using available resources and working with any Allies in theatre, hence each operation may have new interoperability requirements.

Successful ICT interoperability for Defence will ensure cross cutting interactions between OGDs, Allies, Non Governmental Organisations (NGOs) and Industry, where appropriate. Recent operations have demonstrated that Defence must have ICT interoperability with NATO, the United States (US) and other "5-Eyes" partners, and increasingly must also to have the agility to be interoperable with non-standard coalitions and our industry partners in order to deliver success.

Operations in Afghanistan have demonstrated that ICT services need to be delivered to an ever lower level of command, and the support across a range of business processes that Defence provides to the war fighter may well be achieved through reach-back services to the UK, including Industry. The unique challenges of the deployed and maritime environment may mean that the manner in which these services are delivered may vary. However where possible Defence must provide the user with similar ICT systems in the operational and business environment; acknowledging that the line between the two is increasingly blurred. Defence intends to have the capability to deliver rich services which can support a wide range of activities in an end-to-end manner.

On operations Defence will use a number of different Mission Secret Domains, often more than one domain per operation[24] whilst taking a Mission Configurable approach to systems such that they can be re-rolled for each new mission maximising VfM. This will require the use of interoperability standards to enable the passage of information and use of rich services between high and low trust domains.

An interoperability policy is being written by the Defence CIO to ensure that lessons identified from recent operations are translated into clear direction to inform the EP and other ICT interoperability activity to better support operations in the future.

Controlled Values Repository (CVR)

Critical to the success of information interoperability is the coherent and consistent use of terminology and standards. The MODIS Data Management Strategy[25] aims for common data standards to be made available and employed across Defence[26].

The common, authoritative, standards are mandated in JSP 329 "Information Coherence for Defence" and these are currently provided through the CVR. They include data definitions, data exchange standards, data schemas and reference information. To promote

[24] Typically this will include the SUKEO, Coalition Secret, 2 Eyes and 4 Eyes Domains

[25] The strategy defines good quality data as data which is fit for purpose, that is, data which meets the needs of Defence

[26] "Authoritative data that meets the needs of Defence."

interoperability the following hierarchy of data exchange standards[27] is mandated through CIO policy:

- Open Standards including International Standards.
- NATO Standards.
- British Standards Institute Standards.
- Government Standards, including Defence Standards and electronic-Government Interoperability Framework (e-GIF) Standards.
- Proprietary Standards.

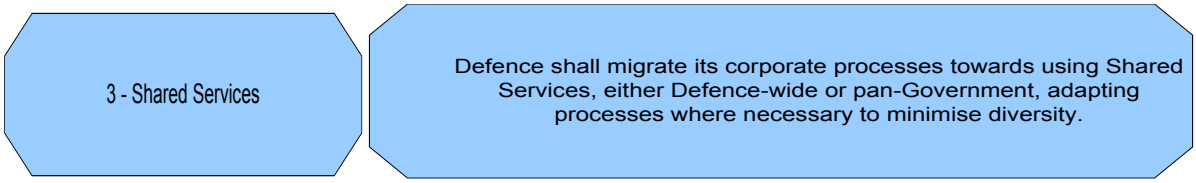
Available through the CVR are the MOD Metadata Standard, the UK Defence Taxonomy and the UK Defence Thesaurus.

JSP 329 and the CVR are owned and governed by the Defence CIO. Communities of Interest (COIs) shall define or adopt standards with future use and interoperability in mind. COIs shall include stakeholders in Industry and OGDs; in addition, Defence shall maintain its engagement with Government forums responsible for standards to ensure we remain consistent with Government thinking.

Projects shall use the SOSA process to engage with Systems Engineering and Integration Group (SEIG) and determine the most appropriate standards to apply in order to deliver interoperability.

[27] To be aligned with the National Codification work on ISO 22745

SHARED SERVICES



Shared Services are increasingly seen as a way of enabling common corporate processes both within and across Departments. Shared Services allow processes to be operated more efficiently and increases agility by allowing processes to more rapidly and effectively share information services.

To support the Defence objectives to optimise delivery of corporate services, a cross-cutting Corporate Services Delivery Strategy and Programme has been established. The programme drives the convergence of systems and related information and business processes for civilian Human Resources (HR), finance and commodity purchasing services and is aligned with the wider Government agenda. Governed by the **Defence Business Services Programme Board**[28], the programme will enable these services to be managed across Defence to corporate standards, leading to better decision making information on these services and more efficient service provision.

The following corporate services are within the current scope of the programme:

- Procurement: Purchasing and contracting, including P2P and E-contracting.
- Finance: In Year Management, Planning Bill payments and receipts, including Departmental Financial Management System (DFMS).
- Civilian HR: Payroll and Expenses, including Human Resources Management System (HRMS), and HR management, but excluding resourcing.
- For the purposes of Cross Functional Reporting and Management Information/Business Information:
  - Logistics: Interfaces with finance and/or procurement only (FLIS).
  - Military HR: Upgrade to Oracle 12, Oracle Financials[29] only (JPA).

To further promote the Shared Services agenda business processes and procedures should be adapted to align to existing ICT services, or OTS applications, thus minimising diversity. Longer term **Defence Business Services** will examine all corporate services[30] for rationalisation, coherence and commonality across Government, accepting that analysis may show that some of these corporate services are truly unique to Defence. This approach should be extended to how elements of expeditionary ICT services are provided on operations.[31]

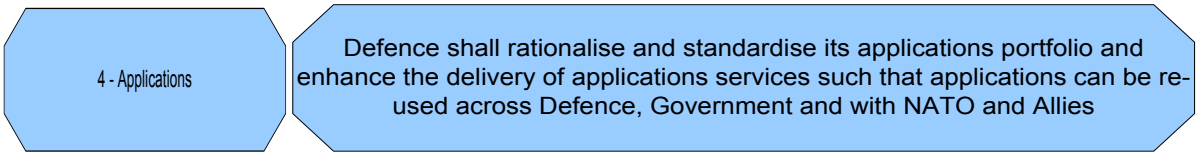
[28] Title under review

[29] Oracle Financials is the component of Oracle's E-Business suite that covers Enterprise Financials/Accounting

[30] Proposals to merge FMIS and PPPA IS have already been examined, as they fulfil similar functions

[31] JDP 6-00 (sponsored by CIO J6) describes how expeditionary ICT services are currently provided on Operations

APPLICATIONS



MOD needs to ensure it extracts maximum value for its investment in software applications through an enterprise approach to delivery and Governance of applications.

Defence has made solid progress over recent years with the process of migrating legacy and new applications onto DII(F). This work has been orchestrated by the CIO led Applications Coherence Working Group and supported by the formation of an Applications Services Team within DE&S ISS who have the role of ensuring a coherent and coordinated approach is taken to Application development and deployment. Development of the approach is planned, coupled with more effective governance and control, in order to:

- Ensure re-use of existing applications and to increase utilisation of the unused features of existing applications.
- Rationalise applications across Defence and wider government.
- Obtain maximum value by leveraging pricing and license costs through Enterprise Agreements whether pan-Defence or pan-Government.
- Align processes, wherever possible, with OGDs and international partners to ensure maximum re-use of developed applications.
- Foster acceptance within Defence that applications provided by OGDs or our Allies are fit for purpose, and that Defence might also provide applications to OGDs and our Allies, the latter supporting the intent to increase export sales.
- Maximise account usage and deliver increased VfM Defence, correlating user demands with available application licences, thus minimising the number of licences that need to be paid for.

The NCA, drawing on the expertise of the Applications Services Team, intends to provide better governance of how Defence applications are acquired and maintained through life. An NCA led **Applications Governance Working Group** has been stood-up to undertake this role and has issued draft principles through which the acquisition of applications will be undertaken. Their role will include scrutinising **all** projects which propose to introduce new applications, significantly change existing applications or introduce requirements which are met through applications, to ensure that they are coherent with existing capability and comply with the application acquisition principles:

- Re-use of existing applications on the Defence Network (there are currently in excess of 600 applications on DII Restricted and Secret).
- Utilisation of Microsoft Office Sharepoint Server (MOSS). MOSS is a highly configurable tool which provides a collaborative working environment. MOSS must be considered as a potential solution to any new requirement.
- Use of existing NATO applications. The UK can influence the development of these applications so that UK requirements are incorporated within the wider NATO product. Moreover, the UK pays for these applications through its national contribution to NATO product, so these applications are essentially free at the point of delivery, albeit that support is chargeable and non equipment Defence Line of Development (DLOD) development costs will still be incurred.

- Use of existing 5-Eyes applications. In the Above Secret environment, where 5-Eyes working is the norm, applications used by these nations are to be considered on a par with NATO applications.

- Use of US OTS applications. US OTS applications can be used; however, they are not to be UK modified and the full cost implications need to be understood.

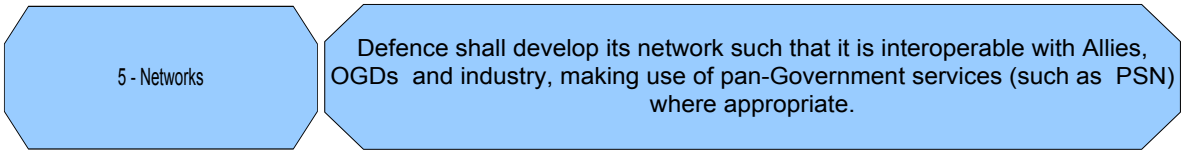
- COTS applications can be configured but not customised. COTS applications have their place; however, the full cost implications of customising these applications need to be understood. Only where prohibiting the customisation of a COTS application proves ineffective in terms of cost, time or performance will customisation be allowed.

- Bespoke specialist military applications can be developed or procured by exception. For example tools to model sonar propagation or to be compatible with coalition Allies. However, these must be the exception rather than the norm.

To support the governance process CIO plans to create a Defence-wide Applications Register with the requirement to examine the total cost of ownership of applications, and rationalise or retire applications where appropriate. This will also allow the identification of opportunities to deliver application services as a catalogue services or from Applications Stores, including any services available from a proposed Government Applications Store.

Acquisition of Defence applications needs to be more agile. Defence, working with Industry, plans to use more responsive and faster application development techniques, such as spiral development. Defence is already examining its acquisition processes in order increase agility, with a prime example being the testing of a new approach by Capability Intelligence, Surveillance, Target, Acquisition and Reconnaissance (Cap ISTAR) (highlighted later in the Structure and Sourcing section of this Strategy).

NETWORKS



The achievement of a common Network would drive economies of scale across Defence and Government and improve efficiency and performance. In addition to delivering these required improvements, a critical consideration for investment and use of the Defence Network is interoperability, which must inform every stage of network design and development.

Currently, the MOD operates 5 major enabling networks[32] and a number of additional supporting capabilities, each of which is operated under a separate contract. The intent is to replace all of these contracts over the next decade. To deliver significant efficiency improvements, remove duplication across Service Providers and ensure Architectural, Service Operations, commercial and financial coherence, DE&S ISS has planned an incremental, portfolio based approach to future acquisition of network services. This new approach has been called Defence Core Network Services (DCNS) and ultimately seeks to provide coherence for all ICT Capabilities delivered; its implementation is described in more detail in the Structure and Sourcing section.

Public Sector Network (PSN)

The PSN vision is to create the effect of a single network across the UK Government, delivered by multiple service providers. Defence supports the development of a PSN to enable sharing of information and services across the public sector and is already contributing to making the vision reality through Project PHOENIX. Defence will seek to converge with and exploit the capabilities and services provided through PSN, provided they meet Defence's interoperability requirements and represent VfM. Defence, through CIO, the NTA and DCNS, shall continue its engagement with the Cabinet Office co-ordinated PSN programme team as the PSN Operating Model is developed.

Networks Example - Project PHOENIX

Defence is already a major proponent of the importance of working to achieve Cross Government Collaboration to improve coherence and increase VfM. Project PHOENIX is an initiative to achieve cross-Departmental benefits across large scale BT contracts. Through Project PHOENIX; DFTS and equivalent British Telecommunications (BT) contracts in the Department for Work & Pensions, Department of Health, and HM Revenue & Customs have become the focus for the Cabinet Office led collaborative efficiency agenda. The contracts are being jointly reviewed to identify opportunities for benefits and early Public Sector Network alignment, under the governance of a CIO Project Board. Defence support for Project PHOENIX includes the opening up of the DFTS contract to allow significantly greater opportunities for sub-contract competition among other suppliers.

[32] Defence Fixed Telecommunications System (DFTS), Defence Electronic Commerce Service (DECS), Defence Information Infrastructure (DII), Defence High Frequency Communications Service (DHFCS) and Skynet 5

Cloud Computing

An emerging technology regarded as key to delivering the PSN is Cloud Computing. This is a style of computing in which scalable ICT capabilities, such as networks, servers, storage and applications, are provided as a service to users, enabling technology and service re-use, whilst increasing agility and reducing costs. The Government intends to establish a cloud computing approach (the G-Cloud) to provide services across Departments for common corporate functions such as HR and Finance.

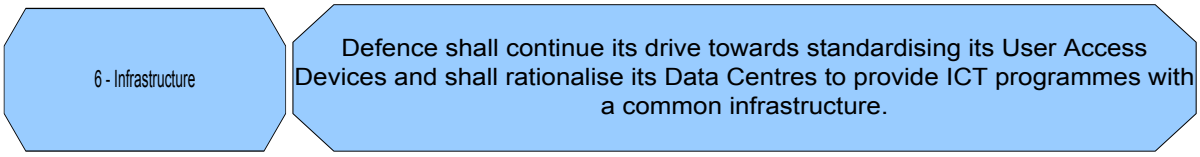
Updates to the Defence Network and wider ICT must consider migration towards cloud computing and in particular the G-Cloud. Cloud computing is most applicable to Defence's 'Fixed' environment, although there may be scenarios where cloud computing could be applied to the Deployed environment. The use of cloud computing will be sensitive to security classification and interoperability needs. The intent is for migration towards cloud computing as follows, although functionality will need to be properly worked through:

- Use of the G-Cloud (and potentially some public cloud services) for services below Restricted.
- Use of a private Defence Cloud for services above Restricted, sharing services with OGDs where applicable; The Defence Cloud would meet as much of the G-Cloud service specification as possible.
- Offering "cloud like" services for data and application services for specific Deployed scenarios.

As part of adopting the DCNS approach to sourcing, DE&S ISS will lead on defining the requisite ICT services that will benefit from using cloud computing. This activity will include working with vendors to define a Defence Platform as a Service[33] framework to allow the development of standard, interoperable solutions.

[33] Platform as a Service is a delivery model that allows the user to deploy onto the cloud infrastructure specific user-specified applications using tools supported by the provider

INFRASTRUCTURE



Only a few years ago Defence comprised multiple infrastructures, which when viewed as a whole were costly to maintain, presented huge interoperability challenges and failed to benefit from using common data centres, User Access Devices (UADs) and applications. The drive, that must continue, has been to move to a common infrastructure with the Defence Information Infrastructure (DII) programme leading the way. However, the journey is far from over with many disparate networks remaining outside the scope of DII. To help mitigate these shortcomings, Defence must continue to look for opportunities both internally and externally to drive down acquisition and operating costs such as the extant Single Source Maintenance (SSM) programme.

Defence Information Infrastructure (DII)

DII is being implemented and is a very significant step towards a fully integrated and coherent Defence Network. DII will provide collaborative working tools and infrastructure. By integrating this capability with Industry to create Collaborative Working Environments (CWE), significant savings could be derived from the Supply Chain. The DII Programme continues to extend its services to the Fixed, Deployed and Afloat environments and will be a mainstay of the Defence Network until 2015. From 2015 it is planned that DCNS will encompass DII alongside other in scope services[34].

Infrastructure Example - DII

DII is the largest Defence IT programme of its type in the world and is already delivering operational benefits to the UK's front-line troops and to the wider Department. DII is providing capability supporting activity in the Fixed, Deployed, Maritime and Mobile environments and, once delivered in full, will operate at all security domains; it is on track to deliver financial benefits in excess of £1.6 billion over the lifetime of the programme and a similar figure in enabled financial benefits.

User Access Devices

The DII Programme provides Defence with a common infrastructure and 'desk top services' across Defence for the Restricted, Secret and Above Secret domains. DII has delivered more than 100,000 UADs, office applications and functionality (e-mail, instant messaging etc). Defence shall continue to converge to a common infrastructure / common desktop solution in line with the Government ICT Strategy.

The existing SSM contract and the planned Integrated Print Strategy (which rationalises the Printer and Photocopier estate across Defence, leading to cost savings) are other good examples of where Defence is benefiting from a more common approach. These approaches, delivering economies of scale, would benefit OGDs.

[34] DFTS, DECS, DHFCS, SKYNET 5, BOWMAN replacement, VLF/LF

Infrastructure Example - SSM

The Single Source Maintenance (SSM) contract reduces the cost of IT and audio visual hardware support across Defence. This contract has replaced multiple support contracts and continues to absorb further support requirements. Aggregated savings in the seven years since the inception of SSM are in excess of £15m. The current contract is restricted to MoD however informal discussions have been had with OGC about opening up the benefits of this contract across Government. This contract is a good fit for the cross Government funding and shared services initiatives.

Over the next 10 years it is expected that, as the boundaries between voice, data and video become increasingly blurred Defence shall enhance its approach to how end users will access ICT Services. The demand for access to "service on the move" will continue to grow, including much further forward on the battlefield. The DCNS programme has 'Unified Communications'[35] as a key driver and we can expect that future access devices will increasingly be mobile in nature.

Defence intends to examine different ways of accessing ICT services other than from a desktop or laptop devices (for example from PDAs or other handheld devices). The Internet Access Shared Services (IASS) has already been implemented to allow access to Defence HR application from any terminal with Internet connectivity and a web browser. Defence intends to run pilots, at selected locations, to de-risk the adoption of mobile UAD technology in the future.

Infrastructure Example - Internet Access Shared Service (IASS)

IASS has been implemented as part of a programme to modernise Defence HR services to reduce costs. Some 10,000 staff working at non-MOD locations across the globe needed to have access to online HR services. The IASS solution provides them with secure access to Defence HR applications from any terminal with Internet connectivity and a web browser.

This access need was not unique to Defence, so Defence worked with the Department of Work and Pensions (DWP) to develop a shared services approach, utilising the Government Gateway. This resulted in a solution that shares some components with the Employee Authentication Service (EAS), a secure solution for public sector employees to access multiple Government applications.

Using smart card technology and a hand held card reader IASS users access the same HR applications as internal staff. IASS redacts sensitive personal data to avoid unauthorised disclosure where users could be overlooked, such as in an internet café or open plan office in Industry.

[35] User Access Devices in the future are likely to encompass Voice and Telephony, Conferencing, Messaging, Presence and Communications Applications – all accessed from a form of Unified Client for the end-user, typically through the adoption of Voice over IP (VOIP) technology

Data Centres

DII has created application hosting capabilities for each security domain, upon which core applications for Defence are hosted[36]. However, there remains a large inventory of functional applications that continue to use dedicated application servers, and in many cases dedicated data centres.

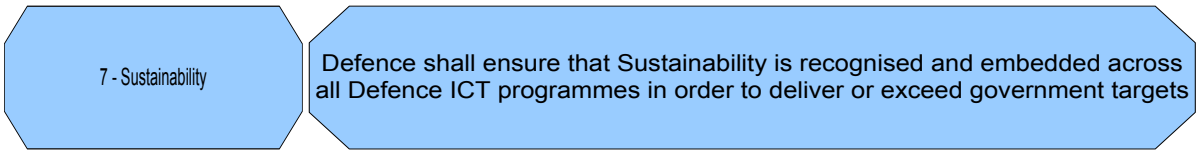
DE&S ISS plans to reduce the number of data centres across Defence allowing for discrete data centres where security classification or resilience needs dictate. Defence intends to share Government data centres and offer to Defence business and operational areas Government (and public) data centres as a service for hosting new application services.

Defence plans to rationalise our Data Centres using 'Virtualisation' technology that allows applications to share application servers. This will reduce the physical footprint of our Data Centres and Application Servers, and therefore enhances the ease of and increases agility when hosting ICT applications[37]. Applications teams must agree how their application can best be hosted at Data Centres with the Applications Services Team (under NTA governance).

[36] Defence is currently preparing a formal strategy for Application Hosting

[37] This will also lead to higher service standards, more resilient ICT services and will have a significant impact on our energy consumption

SUSTAINABILITY



Defence recognises the critical importance of ICT both as a large consumer of energy and primary resources, and as an enabler for environmental and cultural change.

The drivers for recognizing and implementing sustainable ICT across Defence fall into two groups:

- Mandatory requirements:
  - Compliance with Climate Change legislation.
  - Targets for sustainable ICT across government.
  - Introduction of Carbon Accounting.
  - Sustainable Operations on the Government Estate (SOGE) and Sustainable Development in Government (SDiG) targets.
- Efficiency agenda:
  - Preparation for future economic challenges (possible fluctuations in power supply, increases in energy costs, reduced budgets).
  - Sustainable procurement also means VfM.
  - Need to make best use of resources – infrastructure, people, ideas.
  - More efficient use of ICT can produce savings elsewhere

As the Policy Owner for Sustainable ICT, the **Defence CIO** will lead the work to ensure that ICT sustainability is recognised and embedded across Defence. Using the Concept, Assessment, Demonstration, Manufacture, In-Service, Disposal/Termination (CADMID/T) cycle, i.e. from requirement capture through to disposal/termination, sustainability must inform decision making. CIO is leading the development and publishing of a Sustainable ICT Policy and a Sustainable ICT Maturity Model, to share experience and information to embed sustainable principles into the fabric of our ICT systems and services, promote sustainable ways of working with ICT and initiate best practice throughout the Department.

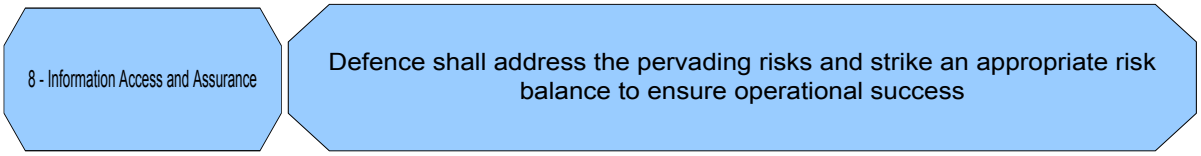
To support this activity a sustainable **ICT Task Force** has already been established which includes stakeholder representation from Defence operational and business areas, Sustainable Development, Sustainable Procurement and Defence Estates. Defence will also collaborate with OGDs, the ICT industry, Government CIOs and Government Chief Technology Officers (CTOs) in order to achieve these sustainability objectives and activities. Defence will play a major part in reducing carbon emissions from other areas of Government activity, for example through enabling audio and video conferencing, remote and home working.

Sustainability Example – Defence Disposal Authority

Defence has already completed or put in progress 61% of the Government's Sustainable ICT Goals and Quickwins. Implementation of a further 13% of the Sustainable ICT Goals has been planned.

The Defence Disposal Authority (DDA) through its Disposal process identifies and captures statistics as to what items, including ICT, have been sold, recycled and sent to landfill. The government is currently looking to expand the use of the Defence's eDisposals service for use across all Government departments and the piloting of an online auction site. The idea behind this initiative is to promote re-utilization across Government buyers of the equipment available for disposals, as well as encouraging departments to use the DDA e-Disposals Web Site for disposals.

INFORMATION ACCESS AND ASSURANCE



Identity and Access Management (IdAM)

A key enabler towards delivering an effective ICT capability that allows information to be shared, particularly with our Allies and Industry, is IdAM. The intent is to support the development of a Government-wide certification capability that can build on the early success of the Transglobal Secure Collaboration Programme (TSCP). TSCP has already demonstrated the principles for assuring identity and federated authentication, which benefits all relevant actors including Industry. The Defence IdAM vision is "A federated identity management capability that enables trusted access to, and secure sharing of, information by our people and partners across operational, support and business areas."

IdAM is an integrated set of policies, processes, standards and technologies that creates and manages digital identities and associated access privileges for all people and other entities within an organisation over the whole life-cycle. To achieve the Defence IdAM vision, we plan to transform our business which will consist of eight goals:

- Deliver Identity Management capability to manage digital identities of all MoD people.
- Provide all Defence staff with a single, trusted credential for identification and access to required resources.
- Provide an automated provisioning capability with self-service facilities.
- Deliver logical access management capability for Defence and trusted partner users.
- Implement information Handling Model across all domains.
- Enable secure information sharing with partners through federation.
- Implement an integrated physical access management capability.
- Exploit IdAM capabilities to realise operational, business and financial benefits.

The first step towards delivery of the IdAM Strategy will be to develop a roadmap. This will be carried out by CIO team in close consultation with key stakeholders. The target is to produce the **roadmap by 2011** in-line with the IdAM Strategy.

Information Security and Assurance

Information Security and Assurance is required to realise the benefits associated with modern ICT and is a theme that runs through this Strategy. Information Assurance (IA) and Data Protection maintains a high profile across Government and Defence. The cross-Governmental focus on these areas will not reduce and Defence will have to maintain an auditable account of how its IA is achieved. This will be achieved by reaching "Level 3" maturity in the CESG Information Assurance Maturity Model, as directed and agreed by **the Defence Board, by April 2012**, and maintained thereafter.

Information is a strategic asset for Defence, critical to making accurate and timely decisions both within the business and the operational context. To maximise its benefit information

must be managed, made available to those privileged to use it and secured from those who are not.

The Defence security environment is inherently challenging with a diverse range of cyber threats intent on gaining access to information or disrupting services. This threat comes from traditional operational adversaries and state actors, such as Foreign Intelligence Services to the less traditional non-state actors including computer hackers.

Recognising our increasing reliance on ICT services, Defence needs to develop robust ICT capabilities, which are designed from the outset to cope with the Cyber threat. Moreover, Cyber defence is a non-discretionary task and an enduring operation. Our cyber defences need to be dynamic and agile to mitigate the ever challenging and diverse threats the UK faces. This requires continued capability development and investment in our people. Additionally, Defence requires close partnerships with OGDs, our Allies, Industry and Academia for our Cyber defence effort to be effective.

All ICT related projects must address the IA attributes of security, integrity, availability, authentication and non-repudiation, by complying with the SOSA Rule Book and following the technical IA principles:

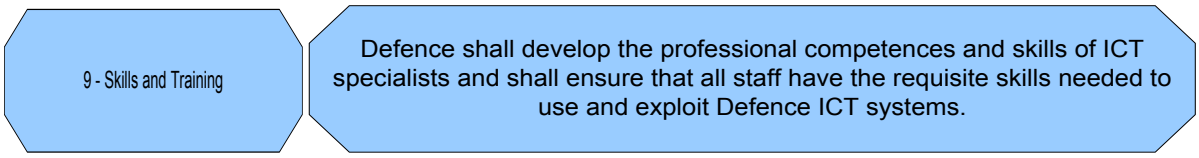
- Systematic examination of the technical aspects, such as Information Security Policy and Access Control, taking into account threats, vulnerabilities and impacts at all stages of service development, implementation and operation.

- Design and implement a coherent and comprehensive suite of IA controls for actively managing tasks.

- Implement a management process to ensure that IA controls continue to meet IA needs through the life of a service.

ICT programmes need to be delivered within this threat environment and allow Defence to demonstrate that IA is embedded from the strategic headquarters to tactical operations. However, the risk/benefit/cost approach, described in the Control Section, must also be adopted to ensure that the correct balance is struck.

SKILLS AND TRAINING



Against a background of reduced training budgets, pressures on Travel & Subsistence and the forthcoming reduction in the number of Electronic Learning Centres, meeting the people challenge will require much endeavour and the active involvement of Heads of Profession, TLB CIOs, Service Leads and Process Owners. Senior ICT posts will increasingly be filled by a mixture of Military, Civilian and external personnel. Greater commonality in describing the skills/qualifications will be necessary and the means of developing future leaders will need to recognise this mixed economy in the workplace. Training will need to be fully justified against workforce plans and stringent VfM tests whilst the challenges posed by a smaller workforce and the Cyber and ICT rich operational environment will require up skilling and a focused approach to continuous professional development.

An Information Skills Strategy is in place to build an organisation that understands and responds to the Information skills requirements of Defence. The Skills Strategy seeks to ensure all staff have fundamental IT[38] skills alongside sound IM skills via the IM Passport. In addition it seeks to increase the professionalism of those working in ICT in line with the wider Government IT Professionalism agenda. CIO will lead Defence's future approach to the development of skilled personnel to support this ICT Strategy. This work will include the following workstreams:

Defence Personnel

- Define the core IT skills/competences (based on the Defence Information Skills Framework and PSG frameworks) required by Defence personnel to obtain maximum benefit from our Information Systems and Applications.

- Develop training/awareness to address any shortfall identified in training i.e. over and above Basic IT Skills, DII: START, European Computer Driving Licence (ECDL) and Information Management (IM) Passport interventions.

- Establish a forum to collaborate with related disciplines (for example, Commercial, PPM) on future skills and workforce requirements needed to deliver this Strategy and to align their own skills and workforce plans to the CIO's direction of travel to enable full benefits to be realised across the Department.

ICT Professionals

- Define and detail IT Professional roles and associated responsibilities and where appropriate, benchmark cross-Government.

- Update IS/IT functional competences to complement work being led by the Knowledge Council on Professional Skills for Governments (PSG) core competences and ensure that these are embedded into our recruitment and performance management processes.

- Identify current and future training gaps and the training interventions necessary to maintain an appropriately skilled cadre of IT Professionals to lead the development,

[38] This section focuses on IT skills, rather than ICT skills. This reflects the descriptor used by the Government wide "IT Profession board" which draws upon the SFIA skills framework. It also avoids confusion with the Communications skills framework owned by DMC and the Comms skills used by those in the Defence Telecomms area and the Communications Engineering skills in the three services

implementation and delivery of ICT investments and ensure a culture of continuous improvement and professional development is embedded within the Department.

- Provide individuals who can develop critical IT skill sets for the future and an essential pool of potential future IT leaders through the Defence Graduate Recruitment Programme.

- Consult with CIOs, Heads of Profession and Branch to agree which Defence posts will need to be included in the requirement to mandate minimum professional qualifications in key senior IT roles. This will be led by the Defence CIO and will be in line with the qualifications framework provided by the Government IT Profession for those working in Government IT.

- Put in place the processes necessary to capture the management information required to demonstrate progress towards ICT Strategy milestones, and thereby also supporting cross-Government requests for statistical returns and the Transparency Agenda (for both civilian and military personnel).

- Build an active community of IT professionals across the Department with links to the wider Government.

- Build in resilience to any framework to develop the IT profession in MOD through embedding networks across appropriate areas of the business.

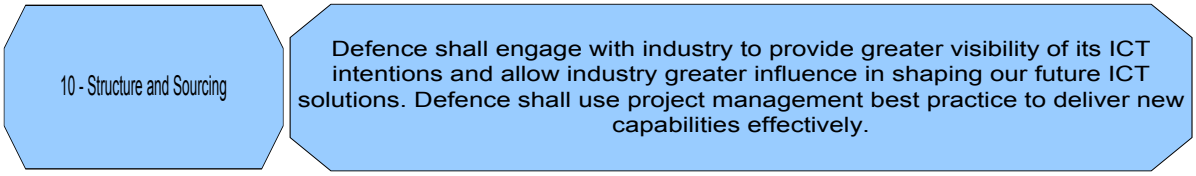
Skills and Training Example – Head of Profession for IT

A Head of Profession for IT has been appointed for Defence. A Head of IA Discipline who will report to through the HOP for IT to the Defence CIO has also been appointed.

It is clear that as Defence prepares itself for the future any reduction in personnel numbers will place a greater requirement on the Department to have appropriately skilled / trained staff. The approach to IT skills development will be focused on delivering business benefit and VfM. One construct in place that will be utilised to measure these benefits is the Defence Information Management Skills Maturity Model (DIMSMM). Other constructs may have to be developed / exploited once firm targets and milestones have been agreed.

In combination with appropriately skilled Defence staff, outsourcing will be used to deliver services and capabilities when it offers VFM and acceptable risk. However an increasing focus on reducing external assistance, contractor and interim support will rely on the exploitation of existing IT skills in Defence and across wider Government. The Senior IT Staff Skills matching service established by the Cabinet Office will be a potential area for exploitation of skilled staffs across Defence.

STRUCTURE AND SOURCING



In general, improved delivery of ICT services is achieved where partnerships or collaborative relationships have been established, particularly as the traditional separation between telecommunications IS and System Integrators is being eroded as part of changes in the commercial market. In addition, the Government is centralising and rationalising public sector procurement to ensure that fewer ICT contracts are being placed and leading to efficiency and cost reduction. Accordingly, Defence ICT acquisition must adapt to these changes and explore new ways of incentivising our ICT Industry partners, which is driving the new DCNS approach described later in this Section.

To help shape a new approach to ICT acquisition, Defence's supplier relationship will follow four principles:

- Defence will engage with industry (outside of its procurement projects and contracts) to provide greater visibility of its ICT intentions and allow industry greater influence in shaping future strategies, plans, innovation and solutions.
- Defence and industry will work together in open, collaborative relationships underpinned by rigorous project and contract management.
- Defence will continue to pro-actively support pan-government supplier relationship activity.
- Whilst the broad principles of successful supplier relationship management are unlikely to change, Defence's detailed implementation will evolve as the ICT Strategy develops.

Project Management

To ensure successful delivery of ICT projects Defence will use best practice project management techniques as described in the AOF. Through Life Capability Management (TLCM) will be used to manage the requirements and acquisition of portfolios of ICT capability. This capability will be offered to users as services either via a Defence or wider Government catalogue. However, it is also recognised that no standard project management approach suits all projects and in particular ICT delivery would benefit from a more responsive and agile approach. A pilot is planned, to deliver Operational capability in the ISTAR area, and CIO will work with the Head of Capability and the Project Team to assess the benefits of such an approach and how it could be applied elsewhere.

Structure and Sourcing Example – Agile Acquisition

Defence is examining its acquisition processes in order increase agility.

Cap ISTAR intends to test a new acquisition approach for one of its current programmes. This will involve engaging suppliers more extensively, at an earlier stage, to contribute to requirements articulation, without prejudicing our ability to determine Value for Money. Defence will supply a robust and understood architecture to an industry supplier, who will use test or reference facilities within which prospective solutions can be assessed prior to an investment decision being taken. Subsequent capability delivery would be incremental, enabling a faster and more agile process for technology development.

Defence Core Network Services (DCNS)

DCNS is a transformational portfolio based approach to the acquisition of integrated end-to-end ICT Services across Defence in order to improve agility and reduce cost. It will be employed by DE&S ISS to take forward the replacement of existing commercial arrangements and place new contracts. DCNS is aligned with the OGC portfolio management approach and plans to use common services and processes, aligned across Defence and Government (including PSN), to increase effectiveness and efficiency.

The majority of the existing service contracts for ICT Services within Defence tend to be high-value, long-term and afford limited access to the benefits of rapidly changing ICT Service market forces (technological, service value or price reductions). The requirement to reduce ICT Services expenditure by £250M[39] a year from 2015 and the need for further SDSR savings requires fundamental change to the way Defence acquires deploys and controls demand for ICT Services. This is against the background of increasing demand for C4ISTAR services and the requirement for increased flexibility and agility.

The DCNS Acquisition approach will drive new ways of working with industry, including a new Target Supply Chain Model (TSCM). The key objectives for the DCNS TSCM are:

- Enhanced financial clarity and control through supply chain separation and improved linkage between costs and pricing.
- An effective integration layer to translate ICT Services needs into supply chain capability to create end-to-end coherent ICT Services for Defence.
- Increased contract agility through re-procurement cycles linked to pace of market change.
- Leveraging wider government benefits through adoption of commercial, technical and service best practice in the public sector.

Defence intends to incrementally transition to the TSCM with parallel evolution of its structure and boundaries with industry. This transition is shown in Figure 4 below.

[39] This is an indicative Departmental target relating to a measure from PR09

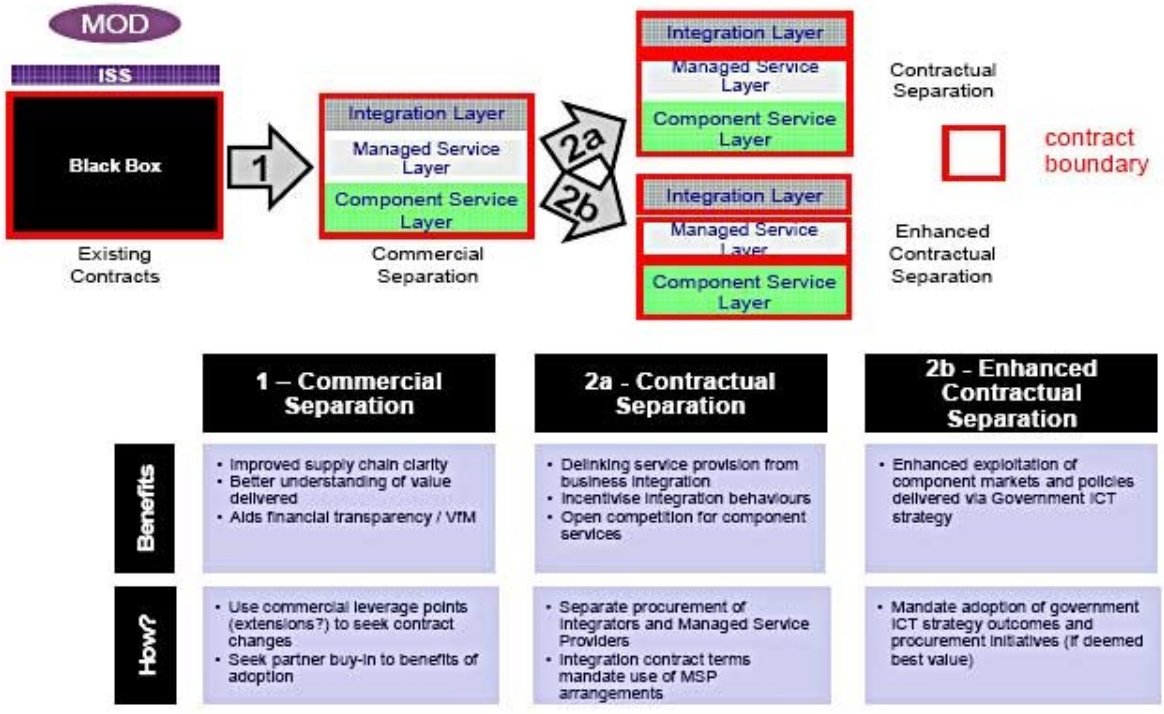


Figure 4 – Transition to DCNS Target Supply Chain Model

The DCNS acquisition approach will be introduced progressively as commercial arrangements require replacement, new requirements are generated or opportunities arise to achieve rationalisation. DCNS plans to deliver a number of outcomes:

- Maximise the efficiencies the Department obtains from its supply base by exploiting the TSCM, by benefiting from a competitive and dynamic supply base and building sound supplier relationships where the emphasis is on risk sharing and reward for improved performance.
- More controlled and focussed engagement with Industry that promotes open and frank dialogue.
- Financial transparency of all elements of the supply chain and each service.
- Supplier behaviours that are driven through good Relationship Management and appropriate commercial incentives which reward good performance through payment, recognition and gainshare, thereby incentivising for success and risk sharing alliances.
- Contracts that are of shorter duration, more agile, 'plan for flexibility' and include a strong change management mechanism that will facilitate this flexibility.
- Liaison with pan-Government procurement projects to identify and agree opportunities for greater collaboration, rationalisation and other best practice approaches.
- Aligns with the OGC portfolio management approach.
- Greater Systems of Systems architecture and safety control.
- The ability to make value based informed decisions, including the use of outsourcing.

7 WAY FORWARD

In this Strategy we have explained how Defence will use ICT to enable achievement of the Defence objectives, while delivering efficiencies and savings across Defence and pan-Government where appropriate. We have described the technological and behavioural principles that will provide the capability and agility required, and the policy and governance that will ensure the VfM rightly expected by Government.

The Strategy has described how Defence will:

- Take an Architectural Approach to its ICT, allowing the Operational and Business needs to be planned, understood and coherently delivered.

- Use common standards in that architecture to make delivery and re-use simple and better enable interoperability.

- Use common services and processes, aligned across Defence and Government and fully integrated with the enabling application to increase effectiveness and efficiency.

- Provide common applications from a managed portfolio that maximises reuse, fully exploits OTS solutions and minimises the reliance on bespoke solutions.

- Manage an effective network and infrastructure that is secure and sustainable and common across Defence, Government and Allies where appropriate.

- Provide staff with the skills needed to fully exploit the capabilities provided and do their job.

- Be effectively structured to govern, acquire and manage the ICT to meet Defence needs such that costs are reduced, effects are maximised and operational risk is minimised.

Following SDSR publication, Defence will seek to implement its recommendations through the Strategy for Defence, Defence Strategic Direction, Defence Plan and a set of Defence sub-strategies. The sub-strategies are the principal means of achieving the SDSR outcomes and will provide a clear line of sight linking Defence objectives to delivery priorities. Defence CIO will determine the Information Management and ICT elements required through MODIS and the Defence ICT Strategy. Both are living documents, regularly reviewed and updated with the next issues expected by March 2011.

The Cabinet Office is due to release a revised Government ICT Strategy in Autumn 2010 and Defence will respond to this through pro-active engagement with the CIO Council and Industry. This engagement will shape how we acquire new capability to ensure we use the right ICT to meet the needs of Defence and the Government.

Definition and Acronyms:

AMO	Air Movements Operations
AOF	Acquisition Operating Framework
BT	British Telecommunications
CADMID/T	Concept, Assessment, Demonstration, Manufacture, in-Service, Disposal/Termination
CAP ISTAR	Capability: Intelligence, Surveillance, Target Acquisition & Reconnaissance
CDM	Chief of Defence Materiel
CESG	Communications-Electronics Security Group
CIO	Chief Information Officer
COIs	Communities of Interest
COTS	Commercial Off The Shelf
CTOs	Chief Technology Officers
CVR	Controlled Values Repository
CWE	Collaborative Working Environment
DCDS (Cap)	Deputy Chief of Defence Staff (Capability)
DCNS	Defence Core Network Services
DDA	Defence Disposal Authority
DE&S ISS	Defence Equipment and Support, Information Systems and Services
DFMS	Departmental Financial Management System
DII	Defence Information Infrastructure
DIMSMM	Defence Information Management Skills Maturity Model
DSAS	Defence Security and Assurance Services
DTA	Deployed Technical Architecture
DWP	Department for Work and Pensions
EA	Enterprise Architecture
EAS	Employee Authentication Service
ECDL	European Computer Driving Licence
e-GIF	Electronic-Government Interoperability Framework
EP	Equipment Programme
FLC	Front Line Command
FLIS	Future Logistics Information Systems
HMT	Her Majesty's Treasury
HR	Human Resources
HRMS	Human Resources Management System
IA	Information Assurance
IAB	Investment Approvals Board
IASS	Internet Access Shared Services
IATP	Information Assurance Technical Programme
ICT	'Information and Communications' Technology
IdAM	Identity and Access Management
IM	Information Management
JPA	Joint Personnel Administration
Log NEC	Logistics Network Enabled Capability
MJDI	Management of the Joint Deployed Inventory
MODIS	Ministry of Defence Information Strategy
MOSS	Microsoft Office Sharepoint Server
NATO	North Atlantic Treaty Organisation
NCA	Network Capability Authority
NEIP	Non-Equipment Investment Programme
NGOs	Non Governmental Organisations

NOA	Network Operations Authority
NTA	Network Technical Authority
OGDs	Other Government Departments
OTS	Off The Shelf
PO	Process Owners
PSG	Professional Skills for Government
PSN	Public Sector Network
SDG	Systems Direction Group
SDiG	Sustainable Development in Government
SDSR	Strategic Defence and Security Review
SEIG	Systems Engineering and Integration Group
SIRO	Senior Information Risk Owner
SOGE	Sustainable Operations on the Government Estate
SOSA	Systems of Systems Approach
SSM	Single Source Maintenance
TLB	Top Level Budget-holder
TSCM	Target Supply Chain Model
TSCP	Transglobal Secure Collaboration Programme
TTP	Tactics Techniques and Procedures
UAD	User Access Device
UORs	Urgent Operational Requirements
UOT	Urgent Operational Tasking
US	United States
VfM	Value for Money