Integrated ICT & Information Management Strategy 2012-2017

Date: 18th June 2012
Version: 1.0
DSTL/DOC65387

1. Table of Contents

		Page
1.	Table of Contents	2
2.	Executive Summary	3
3.	Introduction and Approach	4
4.	Dstl ICT Strategy Outcomes & Benefits Overview	8
5.	Dstl IM Strategy Outcomes & Benefits Overview	10
6.	Next Steps	12
7.	Annex A – Strategic Plans	13

2. Executive Summary

This strategy identifies the high level information and communications technology (ICT) and information management (IM) requirements of Dstl as a business and states how the organisation will satisfy them over the next five years in broad terms. It does not attempt to articulate the processes and technologies that will make this possible but the key decisions, ways of working and areas where technology solutions are required. It sets the direction for the future provision of IS and IM within Dstl whilst addressing a number of legacy challenges and ensuring that Dstl is aligned with wider government strategy and policy.

Core to this strategy is the need to understand the total through life cost of the information systems provision across Dstl, both corporately and departmentally provisioned and the benefits it brings to delivery for our customer base. This information can then be used to prioritise ICT and IM provision across the organisation and focus effort where it will provide most value for money. The period of austerity we are currently in merely highlights the urgency of developing this understanding.

The key business requirement is to extend Dstl's ability to collaborate effectively both internally and externally. External collaboration includes new groups of partners from non traditional allies through to more extensive collaboration with industry and academia at higher levels of classification than currently. This touches both on the ICT Dstl deploys and how it manages its' information emphasising the need to consider both elements together.

In terms of user experience the strategy's ICT focus is to consolidate the service that currently exists over the next two years so it is effective, efficient, reliable and repeatable. It will then be possible to move towards being more innovative in how it provides services and extending those services. Within the five year period covered by this strategy the intention is to go from reactive to proactive service provision.

Within the IM domain the strategy is to move Dstl towards managing and exploiting information effectively across all its operations in a consistent manner. Dstl can not afford to ignore the need for information management if it is to avoid substantial future costs or the need for information exploitation if it is to offer increased customer value year on year. With the current rate of global information growth and our own data growth this need is now critical.

Dstl also has the opportunity to become the repository for S&T research across the defence and security community which we will pursue. This complements Dstl's recently extended role and reduces potential duplication of S&T research for MOD.

3. Introduction and Approach

Purpose of this Document:

This document sets out Dstl's Information & Communications Technology (ICT) and Information Management (IM) strategy. It has been developed as an integrated strategy covering both ICT and IM due the inter-dependencies between the two areas. Within the context of IM, this document also includes a Knowledge Management & Exploitation (KM&E) component that is complimentary to the Dstl Knowledge Management strategy produced by the Chief Technology Officer.

Dstl's business is focused on the exploitation of global Science & Technology (S&T) and subsequent innovation in that arena to deliver advantage to HMG in pursuit of its objectives. The way Dstl manages and exploits the global S&T knowledge base especially its own information and knowledge is fundamental to its future success.

This strategy will be reviewed annually by the CIO to ensure that it remains aligned with Dstl's key strategic drivers and external influences.

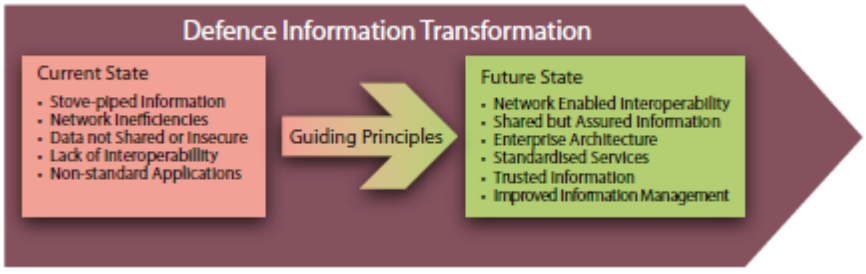
Changing ICT Investment Focus:

The Government are driving through the CIO Council a need to take a Pan-Government approach to ICT particularly focused on making Government expenditure in this area more effective and efficient in order to achieve greater Value for Money (VfM) for the public purse. This is reflected within Dstl's Corporate Plan and the Infrastructure Directorate strategy. The Government's ICT Strategy sets the framework for this approach and in developing Dstl's ICT & IM Strategy we have aligned and harmonised where appropriate with both the Government and MOD ICT Strategies and the MOD Information Strategy (MODIS).

Over the next 10 years HMG and consequently Defence will increasingly use common ICT and only in cases where there are unique requirements (ie; Operational imperative, Security or Intelligence) will differentiated ICT solutions be authorised. The challenge for Defence and therefore Dstl is to understand better where ICT investment should be aligned with wider Government initiatives and to support these activities, whilst preserving those capabilities that are unique because they have to be. Regardless of approach ICT provision must become more efficient than it is currently in order to achieve year on year cost savings and reduce its overall through life cost.

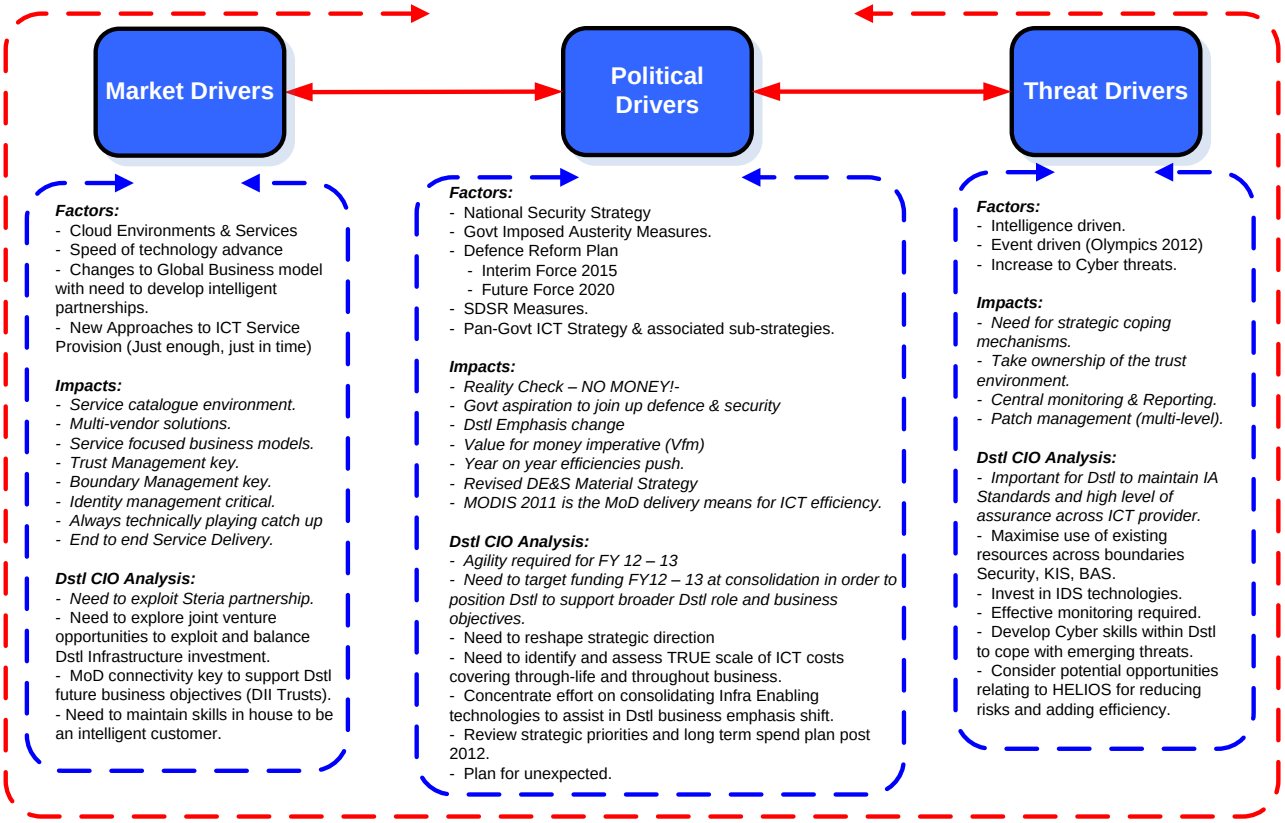
Within Defence there is recognition of the need to become more effective at translating technology innovation into tactical and strategic advantage for the UK and a drive to achieve this largely through improved collaborative working with Allies, OGDs, Industry and academia. In this way HMG will efficiently access the global knowledge base and get closer to the sources of technology innovation. Significant elements of the tooling required to enable effective collaboration are ICT based and require good IM practices.

The MOD will implement the Defence Information Transformation moving from the current state to the desired future state through MODIS:



Dstl Approach:

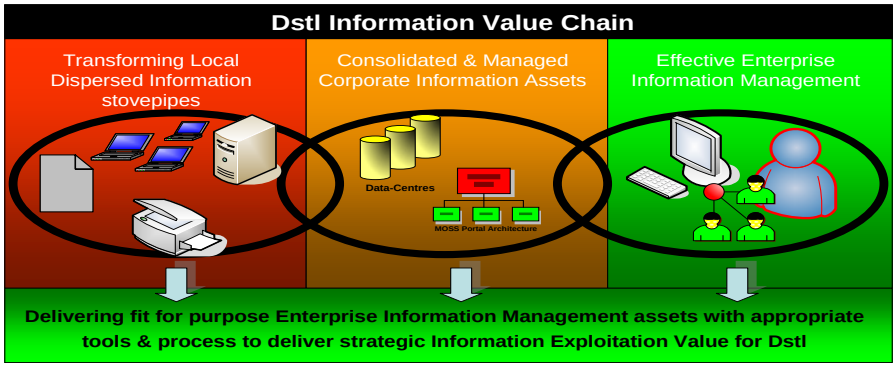
Dstl recognise the ICT landscape issues and future challenges facing the Defence and Security Sectors and is committed to aligning its ICT & IM Strategy as appropriate to ensure cohesion. In addition, Dstl are well positioned to assist the MOD and OGDs in facing these challenges, both in its advisory role and in developing and applying innovation in a small controlled defence and security focused environment which can later be more widely exploited. The following landscape factors have been assessed and built into this strategy:



Strategic ICT Landscape

Dstl has embarked on a new ICT Service contract with a new Strategic Delivery Partner (Steria) with a contract that is based around a managed service approach comprising a range of well defined ***Delivered Services***. Dstl will continue to develop its ICT within this managed service context. This provides Dstl with full visibility of through-life ICT costs and provides agility to develop the scope or scale of managed services to meet our business need within a robust Governance framework. This is linked to a commercial enabling contract with sufficient flexibility built in to facilitate, not hinder, Dstl's agility in the rapidly changing environment in which it operates.

Dstl will progressively move from current state where information is managed in multiple stovepipe environments/system, through to consolidating information under an effective managed service in order to reach our desired end state of developing and delivering an Enterprise Information Management environment based on planned co-ordinated projects.



Information has significant value to Dstl, it represents a vital component of Dstl's core business and supports the businesses core asset, the knowledge of its staff. The responsible management of information, including the retention, disposal, and preservation of information/records will enable Dstl to make best use of its corporate memory. This must be enabled by effective use of trusted and assured infrastructure, systems and services and aligned to the wider knowledge management activities within the lab.

Dstl's approach is harmonised with the broader Defence Information Vision and MODIS 2011 which describes the following:

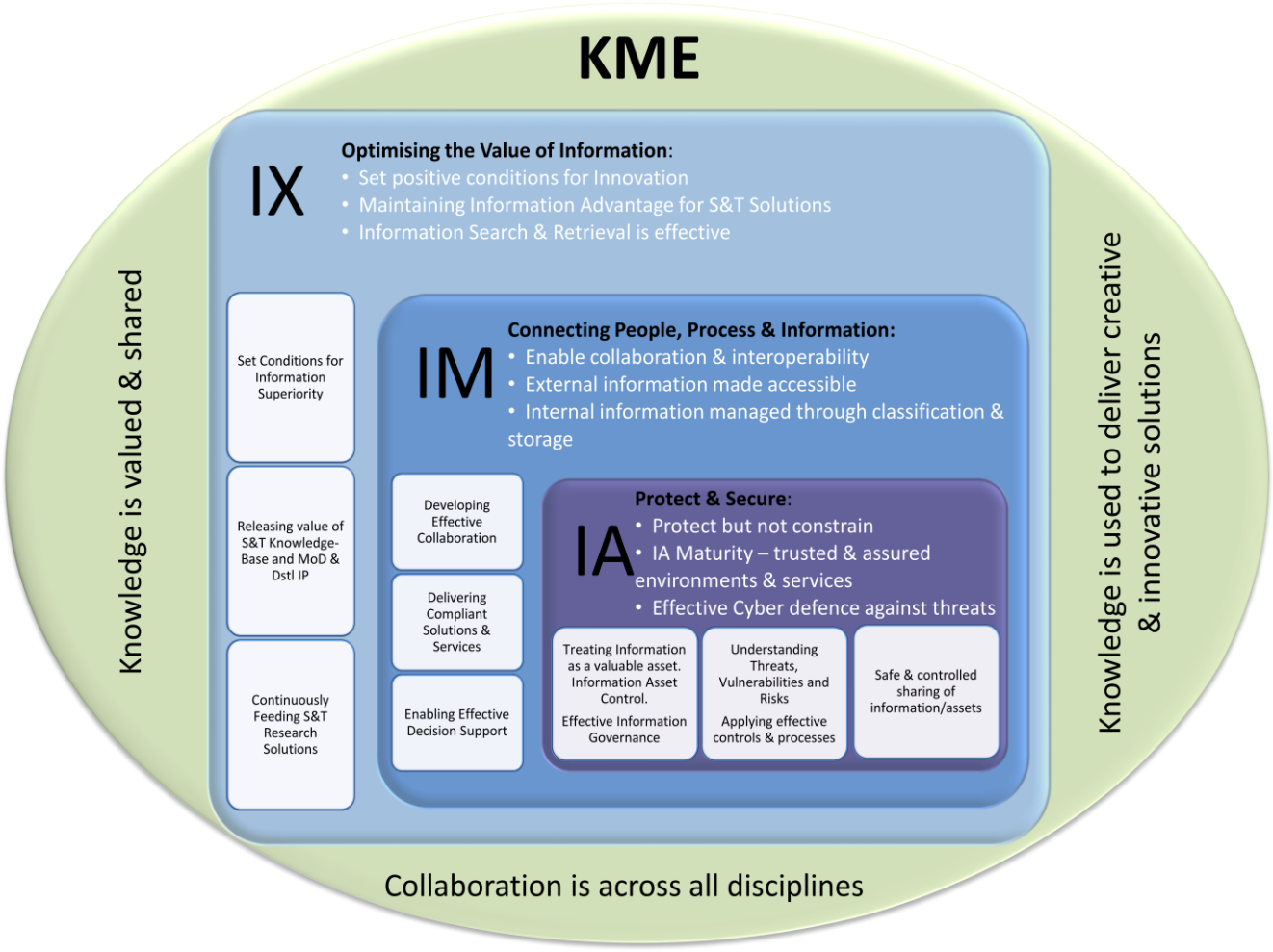
- Information Assurance (IA) acts as a foundation through which we put in place the appropriate controls and assurance to manage our information risk and deliver effective trust and accessibility to our information assets and host environments.

- Information Management (IM) provides the collaborative framework through which we bring together people, process and technology to manage our information assets effectively.

- Information Exploitation (IX) is the state where we are optimising the information assets we own, manage or process in order to feed into S&T innovation and enable defence to achieve and maintain its critical strategic goal of Information Superiority.

Dstl use a single term of "***Information Management***" (**IM**) to describe the entire spectrum of descriptive terms used elsewhere across MOD/OGD. This is to ensure that Dstl staff focus on managing information responsibly which incorporates elements of IA, IM and IX.

The diagram below demonstrates how Dstl bring all component parts of IM together to deliver our operational output to customers using Knowledge Management & Exploitation as the enabler to service Dstl operational outputs for S&T innovation:



Strategic Alignment of ICT & IM Strategy

Defence ICT Vision:

Defence shall strive to align its ICT across Government where possible, recognising that the achievement of the Defence objectives is our highest priority.

Defence Information Vision:

Agile exploitation of our information to improve effectiveness and efficiency on operations and in support areas through access to, and sharing of, timely, accurate and trusted information.

Dstl Strategic ICT & IM Vision:

The Vision

To be a leader in the provision of knowledge and information services within Government.

Dstl interpret this vision as the efficient and effective implementation of ICT capability to meet business needs which has particular resonance at this time of Government austerity. Dstl will be a fast follower of ICT changes that add significant benefit to the organisation seizing opportunities that will contribute to the long term success of Dstl. We will simultaneously rationalise our ICT estate (hardware and software) and streamline processes and practises to minimise the support burden and effect efficiencies.

The Mission

To ensure that Dstl has ready access to all necessary information and has a set of processes and tools with which to exploit this information in support of Dstl's business goals and the wider Defence vision.

Dstl will operate in a manner that enables the effective and progressive development of Dstl ICT Infrastructure and IM capabilities so that they are:

- Capable of managing the challenges of today.
- Prepared to take on the requirements of tomorrow.
- Capable of building fit for purpose capabilities to meet the challenges of the future.

This will be achieved by combining the value of people, process and technology in order to; provide an effective, resilient and affordable infrastructure that is based on pragmatic and strategically focused investment.

Dstl will exploit its ICT Strategic Partnership with Steria in the future in order to achieve broader ICT efficiencies/goals through developing a range of Infrastructure Capabilities and Services that address emerging needs.

4. Dstl ICT Strategy Outcomes & Benefits Overview

ICT Outcomes & Benefits:

Dstl's ICT Strategy enables the following outcomes in relation to Dstl's corporate strategy and the broader MOD and Cabinet Office ICT Strategies:

Dstl Desired Outcomes	Dstl Envisaged Benefits	What Success Looks Like
Improved Operational Effectiveness	• Dstl's Business Delivery Output is more effective, having been enabled and/or enhanced rather than constrained by technologies and information tools. • Year on year reduction in cost for the delivered service or improved delivered service for same capital outlay. • ICT provision is flexible and agile	• Establishment of a network trust with the Defence Information Infrastructure (DII) at restricted and secret. • Provision of UKIMN across the Dstl Estate for above secret working. • Dstl processes and requirements are matched to the application removing the need to configure applications. • The delivered service achieves a like for like 5% year on year saving over the period of the Steria contract.
An understanding of the business benefit of ICT investment	• ICT is viewed as a business enabler rather than a cost centre by Dstl • Clear linkage of services and projects to business goals • Improved decision making in support of future ICT investments for Dstl.	• ICT projects within Dstl will deliver 80% of their proposed benefits and be delivered on time and budget. • The publication of an ICT service and technology roadmap traceable to business goals. • ICT projects are prioritised based on value to the business.
Increased re-use and exploitation of Dstl ICT Services and capabilities	• Achieve cost savings and year on year efficiencies. • The proposed benefits of ICT investment are exceeded	• The establishment and use of standard architectural building blocks across all networks. • Leasing of excess ICT capability to other parts of government
A continuous and measured approach to Risk Balanced Technology Innovation to meet Dstl and Defence & Security current and emerging requirements & challenges.	• Improve the use of ICT to enhance the delivery of Dstl's output and support to military capability and customer delivery. • Maximise potential return on investment. • Exploit Dstl innovation and ICT Infrastructure and Services to assist MOD and OGD in facing future challenges.	• Dstl system & process innovations used in other areas of government. • Use of virtualised environments to provision bespoke application environments.
New, existing and legacy software & systems are managed and exploited effectively.	• Maintain current & future service delivery to Dstl business requirements. • To reduce solution delivery time & development costs. • To optimise ICT investment return.	• The number of applications is significantly reduced. • The majority of applications are in vendor support and are managed through life. • Old models are retired. • Dstl will buy in non core services where it offers business advantage.

Governance of non-corporate systems	• Non-corporate systems present no greater risk to Dstl operation than corporate systems. • Departmental systems provide focussed provision of capability that cannot be provided corporately • The number of IS systems present in Dstl reduces minimising risk and promoting value for money	• Provision of non corporate systems occurs only when the corporate provision cannot meet the business need. • Dstl has full visibility and control of all non corporate IS. All these systems will be accredited and maintained based on a risk management approach. • The overhead of accreditation will be reduced.

5. Dstl IM Strategy Outcomes & Benefits Overview

IM Outcomes & Benefits:

Dstl's IM Strategy enables the following outcomes in relation to Dstl's corporate strategy and the broader MOD and Cabinet Office ICT Strategies:

Dstl Desired Outcomes	Dstl Envisaged Benefits	What Success Looks Like
Effective Collaboration	• Achieve improved collaboration across Dstl and between Dstl and relevant communities. • Collaboration is facilitated not tolerated.	• Establishment of a network trust with the Defence Information Infrastructure (DII) at restricted and secret. • Provision of UKIMN across the Dstl Estate for above secret working. • The provision of a collaborative toolset based around Sharepoint that operates across the organisational structure and the research programme.

Effective Information Exploitation	• To optimise Dstl's ability to release the value of the MOD/Dstl S&T IP for knowledge & innovation.
	• Ability to reduce future research costs through information/innovation re-use.
	• Faster and more efficient delivery of information to business endpoints (S&T Departments) through new Information Services and Self Service tools.
		• The ability to search across information stores receiving comprehensive and accurate results. Effective enterprise search
		• Storage growth slows as a "store once, use many" philosophy is adopted.
		• A single records management process is adopted across the organisation using a common file plan and file naming convention.
		• Information not part of the formal record is captured and available through collaborative mechanisms.
		  ○ A lab wide technical Wiki
		  ○ Communities of interest
		  ○ Trials data and model repositories.

Improved Operational Efficiency	• Accurate, up to date information reduces wasted effort & costs.	• Information sources are easy to search through a single search engine. • Dstl will operate a culture of information sharing and adopt good information management processes. • The business will define and publish its business information requirements in order that they can be delivered. • S&T information will be made more widely available to the Govt. customer community through the MOD funded Athena programme and improved collaboration mechanisms.

Increased Agility	• Trusted information can be accessed and manipulated by authorised users, whenever and wherever required, limited only by affordability and security factors. • Timely, accurate and relevant Information enables Dstl's Executive & Business planning & decision-making.	• Access to the Internet and RNet is available globally through secure means both wired and wirelessly.
Positive Reputational Impact and Sustained Customer Confidence	• Dstl's reputation with customers remains positive and impressive and provides customers with high confidence in Dstl to manage IM in a compliant and effective manner. • Ability to reinforce and strengthen Dstl's brand by setting and maintaining a clear perception that Dstl are seen as a "safe partner" for managing S&T information/innovation. • Dstl are recognised for contributing to success rather than introducing another form of risk to customers.	• Information is managed rather than collected. Evidenced by proactive records / information management regardless of media. • All information in Dstl is owned by and the responsibility of an Information Asset Owner • Dstl will look to become the UK focus for defence and security S&T information.

6. Next Steps

This strategy has set out the future direction for ICT and IM in Dstl over the next five years. It proposes a number of measures that are necessary if Dstl is going to continue to offer increasing value to its customer base and meet the growing need across the business for collaboration and agility. Delivery of this strategy will not be easy due to the large amount of work involved, the financial constraints on Dstl over the next few years and the discipline required by some of the proposed changes in how we should manage our information. However Dstl is not alone in facing these challenges and will work with others to overcome them, adopting solutions that are proven to work elsewhere wherever possible.

This strategy will be reviewed at least annually in order to keep it current in what will be a dynamic and challenging period for ICT provision in UK Government. Given the overarching nature of this strategy a number of roadmaps, sub strategies and plans tackling specific issues such as storage and maintenance of Dstl's information assurance maturity level will be published in the coming months. These will be aligned not only to this strategy but the evolving Infrastructure Directorate wide approach to prioritisation, planning and delivery of its programme of work..

7. Annex A – Strategic Plans

Dstl Strategic Plan for ICT:

The following strategic plan for ICT covering the period 2012 - 2017 will be used to focus and influence ICT delivery and innovation. The plan has been broken down into Strategic Lines of Activity (SLoA):

SLoA 1 - Maximising value for money

Dstl will maximise value for money from its existing and new investments by:

- Understanding the current full cost of its IS provision across the organisation including the investments made at a departmental and project level where they will become tools of the trade for the business. It will then use this information to identify areas where efficiencies can be made and potential gaps in the corporate provision.

- Adopting a benefits' realisation approach to new projects – each proposed project must articulate measurable benefits up front and upon completion these will be compared to the delivered benefits.

- Dstl will prioritise its IS spend across the organisation based on value to the overall operation but not limited purely to cost / financial return.

- KIS will derive a charging policy/model to sustain high cost facilities within the IS provision such as trials data storage and high performance computing.

- Dstl will measure the through life cost and value to the business of the non STEM applications it runs on corporate systems and remove those that do not provide a suitable return on investment.

- Dstl will look to buy in non core services such as Finance and HR support (currently provided via iCAS) where it offers business advantage but will retain core scientific IS provision such as models in house. It will obtain service from and supply capability to common government platforms as appropriate.

- Dstl will explore opportunities to capitalise on its investments with other parts of government for the public good. Initially we will explore opportunities to exploit latent data centre capability but later look to develop and deliver common services for government communities with similar requirements to Dstl. This includes both technology based services and consultative services such as architecture looking to extend the current IMD customer base and service offering.

SLoA 2 - Agile service provision

Dstl requires the ability to be able to provide agile services in terms of its ability to modify and bring new services into being quickly. Enabling activities will include:

- Dstl will adopt a risk balanced approached to future system/application provision based on the perceived return on investment, the information risk and business need. For example the use of virtualised environments to provide bespoke application environments will be investigated particularly for STEM provision.

- For STEM applications KIS will provide environments in which a user maintained application can run that can be provisioned through automated workflow such that once approved by the budget holder environments are provisioned and available within minutes.

- Where corporate provision cannot meet a business need in a timely or efficient manner non-corporately maintained systems will be implemented and appropriate governance applied.

SLoA 3 - Collaboration

Dstl's expanded remit to manage all S&T research for MOD requires a greater degree of collaboration than ever before with a more diverse series of partners at all classifications. Enabling activities will include:

- Dstl will establish links with other networks at all classifications prioritised by business need and opportunity. These will be established with boundary protection that is appropriate to the perceived information risk. Specifically Dstl will extend the capability to communicate at a high classification through the UK Intelligence Messaging Network (UKIMN) and take advantage of the future collaboration opportunities this community offers.

- Dstl will establish network trusts and employ encryption as required to facilitate collaborative arrangements. Specifically it will achieve a full DII trust to MOD at restricted and secret and enable greater communication/collaboration with Industry and Academia through the use of commercial encryption.

- Dstl will focus its use of collaborative tools around Sharepoint and the Office suite to capitalise upon its investment to date. However it is recognised that this is an area of rapid development and so KIS will maintain a technology watch activity in this area through KM&E with a view to adopting those tools that offer significant business advantage.

- Dstl will add voice over IP support to its existing networks to support secure voice communications between sites and with external partners to the user desktop it will initially focus on the SNet and TSNet.

- Dstl will review its telephony provision in FY 2012 to ensure that it is fit for purpose, value for money and meets Dstl's future desktop strategy.

SLoA 4 - Efficient, safe delivery

Dstl as a business requires efficient delivery of its IS services to support obtaining value for money and agility. The delivery must also protect the information it holds complying with statute and wider government policy. Enabling activities will include:

- Dstl will optimise its current and future ICT estate including the processes and procedures surrounding the service provision. It will automate workflow where possible, maximise the number of first line incident request fixes and minimise desk side visits.

- Having optimised its current ICT estate Dstl will look to provide innovative technology and procedural solutions to its business problems based on a risk balanced, pragmatic approach.

- Dstl will improve its planning process particularly around renewal of services to ensure the technology elements are updated based on a roadmap and schedule derived from business criticality. The roadmaps and schedule will form part of the Infrastructure directorate roadmap which will be co-ordinated through the iPMO. Dstl will aim to have all its technology elements within the vendor support window or have consciously assessed and accepted the risk of allowing them to fall outside the support window. Dstl will use this mechanism to pragmatically access the constantly changing ICT technology environment and determine how and when a service moves forwards based on business benefit.

- Dstl will continue to develop and adopt an Enterprise Architecture (EA) approach to its' IS provision which is compatible with the broader MOD and Government EA approach. We will develop this architectural capability across KIS, IMD and Steria to meet Dstl's own architectural requirements, maintain sufficient in-house capability for Dstl to be an intelligent customer and to support wider security and defence needs.

- Dstl will use standardised architectural building blocks where possible across all its networks adopting a "design once, use many" approach which will consequently migrate

all networks to a similar core design. This will reduce overall network design costs and simplify network support.

- Dstl will apply an efficient lightweight governance framework across its management of IT. Existing non corporate systems will have appropriate governance applied retrospectively where it does not currently exist.

- Dstl will put in place application management for off the shelf applications. This will rationalise the number of applications we support across the networks which is currently excessive. We will also remove those that are no longer in the vendor support window and those that present an unacceptable security risk. Where two or more applications perform similar functionality Dstl will standardise on one, removing the others.

- Dstl will investigate the use of virtualisation for the delivery of STEM applications / models and supporting in-house code development to remove the need for testing prior to deployment and to make the provision of small networked environments an automated workflow.

Dstl Strategic Plan for IM:

The following is the strategic planning for Dstl's information management over the period 2012-2017. It supports the broader MOD MODIS objectives of shared information across trusted environments delivered through new innovative and standardised services. Dstl will move towards this goal progressively and pragmatically. Where information is mentioned it refers to all forms of media including but not limited to; paper, electronic records, tapes, film/slides and video

Key to the approach is to champion a culture which values and exploits knowledge and information for the benefit of the work of the laboratory and its customers. Information is a strategic asset to Dstl with a lifecycle from creation through to disposal. We must ensure the full lifecycle is managed to ensure quality, integrity and effective exploitation.

This element of the strategy is complementary to the Knowledge Management Strategy which is produced by the Chief Technology Officer.

SLoA 5 - Understanding what information we have and where it is stored - Information Management

Dstl requires efficient management of its information both to reduce its operating costs (store once, use many) but also to enable the information to be exploited. All data in Dstl will be owned by an Information Asset Owner and be managed through life from creation to disposal.

- Dstl will implement "single sources of truth" for all formal records as a minimum with an aspiration to extend this to all business critical information.

- Dstl will ensure appropriate infrastructure, tools, processes and training in information management is available to allow staff to undertake their role. We will look at developing an information management skill / maturity framework as this has been effective at improving our information assurance. Any framework adopted will align where appropriate with broader MOD or Government practice. Dstl will look to apply an innovative approach to its' information management activities.

- Dstl will move towards applying appropriate metadata to all its information and providing an Enterprise wide search capability.

- A strategy will be developed through the JCC for managing Dstl's legacy holdings and be pragmatically implemented. The strategy will look to move all records onto electronic storage or disposal. Legacy data will be electronically represented so it can be searched efficiently. The strategy will ensure that the effect on the business is minimised. Ring fencing legacy data will be considered an acceptable option if other options are deemed too expensive. Long term legacy stores such as the TNT archive will be accessed as part of this exercise. The strategy will also look to the future making proposals to avoid digital obsolescence.

- In accordance with HMG policy Dstl will migrate from a 30 year rule to a 20 year rule. This will be complete by 2017, three years ahead of the legal requirement. In the course of this work a compliance check will be conducted to ensure Dstl has the correct Lord Chancellor's Instruments or has passed historically important information to The National Archive.

- We will consider the adoption of dedicated repositories for certain information types such as trials and model data.

SLoA 6 - Using information to generate knowledge and improve delivery - Information Exploitation

Unless the information Dstl holds is exploited it has no value to the organisation and should be disposed of. Exploitation requires information to be managed properly so that it is accurate and can searched efficiently and effectively and consequently accessed in a timely manner. Exploitation of information enables Dstl to build knowledge in its staff and provide the most cost effective solutions to customer requests.

- Dstl will actively promote a culture of information sharing in order to create an effective collaborative working environment.

- Dstl will ensure appropriate infrastructure, tools, processes and training in information exploitation is available to allow staff to undertake their role. Dstl will look to innovate in this area.

- Dstl will look to become the UK focus for defence and security research information from all sources. This would complement the overall role of Dstl and provide a more cost effective service for MOD by reducing duplication and introducing efficiency into the information management of research outputs across the defence and security arena. This builds upon the work carried out by the Athena project[1] which manages the research output of MOD sponsored programmes. Athena is already reaching out to other Governments and UK industry to make their information accessible as part of the collection and this strategic objective is the logical extension of that initiative.

- We will improve our ability to exploit business information to support Dstl Executive and Business focused decision making. This will require progressively improving connections between business process, information flows and enabling ICT systems/applications/tools.

SLoA 7 - Looking after our information - Information Assurance

Dstl must appropriately protect its ICT infrastructure, systems and data proactively managing against the increased Cyber threat and emerging/new forms of attack.

- Dstl will adopt a risk managed approach to information assurance

- Dstl will introduce a single effective identity management system that operates across all its environments.

- Dstl will ensure that its infrastructure, processes, systems and network environments are robust by design and subject to effective information assurance controls to manage any threats/risks. This will be applied to all information stores across all media types. For example Dstl will introduce intruder defence systems and extend the monitoring on all its networks to strengthen its defence in depth.

- Dstl will build resilience into business critical ICT systems. It will ensure that resilience measures are appropriately balanced and scaleable such that it can manage resilience challenges with agility. Dstl will review and propose a strategy for resilience of information stored in non electronic formats.

[1] The Athena project is a MOD funded activity within Dstl to collate and make available all defence S&T research output available to MOD along with an ability to search the collection. Within MOD this is known as The Science Gateway and is available over DII at both restricted and secret. Within Dstl it can be found as a link off the main Nexus page.

- Dstl will increase its capability in the cyber arena to meet customer demand and will cross fertilise skills between its operational (customer focused) business and its internal (corporate IS provision) function.

- Dstl will place emphasis on maintaining effective defensive cyber measures to reduce risk exposure to Dstl. This will include focus on and investment in effective Information Assurance relating to boundary management, network monitoring and incident response capabilities.

SLoA 8 - Doing the right thing - Information Governance

Dstl is required to fully comply with all Legal, Regulatory and Statutory obligations in order to maintain effective assurance across the IA compliance spectrum.

- Dstl will maintain a robust approach to IAMM as it becomes business as usual and will operate under a continuous improvement regime. We will expect this approach to be adopted by our service partners and third party suppliers as part of their continuous service improvement to Dstl.

- We will continue to monitor and review our information governance structure and adjust as required to meet business need. This structure will be used across all the areas of information management within Dstl for example it will be used to implement the current records management initiative lead from MOD CIO Office.

- In 2012 we will carry out a capability fit gap against the Cabinet Office IAMM level 4 criteria and determine if it is in Dstl's business interests to try to obtain this level or if sustaining the current level 3 is the best fit for the organisation.

SLoA 9 - Making information accessible - Information Access

Dstl has a largely mobile workforce that requires flexibility in its ability to access information and uses this additionally to support Dstl's flexible working arrangements. Dstl currently makes RNet access available globally through broadband and 3G connections from which access to UNet can also be obtained.

Other Dstl networks are only available through the wide area network which is distributed between core sites and out stations through dedicated links. The establishment of a trust with DII at restricted and secret will facilitate access from third party locations within the MOD Estate where broadband and/or wireless access is not universally available.

- Dstl will provide access to external information sources which support the work of the laboratory.

- Dstl will devise a method to allow its partners and third parties to connect securely via UNet to their internal networks. No other methods will be permitted.

- Dstl will provide one or more approved end user devices in each major category to facilitate its mobile workforce. At the time of writing these categories are desktop, laptop, tablet and Blackberry/mobile device. Other devices will be permitted only with an approved risk balance case.

- Dstl will investigate the need for and possible solutions to individual remote working at secret.