



# DE&S INFORMATION STRATEGY 2010

Defence Equipment & Support



MINISTRY OF DEFENCE

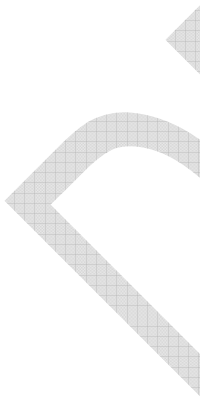
## ***DE&S Information Strategy – Foreword***



This DE&S Information Strategy (DE&SIS), which is consistent with the MOD Information Strategy (MODIS) issued in September 2009, sets the high-level context for DE&S to collectively transform the way we use and manage information. The emergence of Network Enabled Capability (NEC), and the significant investment in the Defence Information Infrastructure (DII) and other Information Systems, has prepared the ground for this transformation to provide *exploitable and trusted information at the right place, at the right time, to enable the right decision, in order to deliver the right effect and achieve the right outcome.*

DE&S needs strong and clear governance to ensure that *information is treated as a strategic asset* and is managed as such. To drive our information transformation this strategy provides the foundation from which the DE&S Chief Information Officer (DE&S CIO) will direct the development of more effective information processes and policy across DE&S. In doing so, I will require the full support and commitment of all in DE&S to create a holistic approach to the development of information capability.

***Major General Tim Inshaw***  
***Chief Information Officer, DE&S***

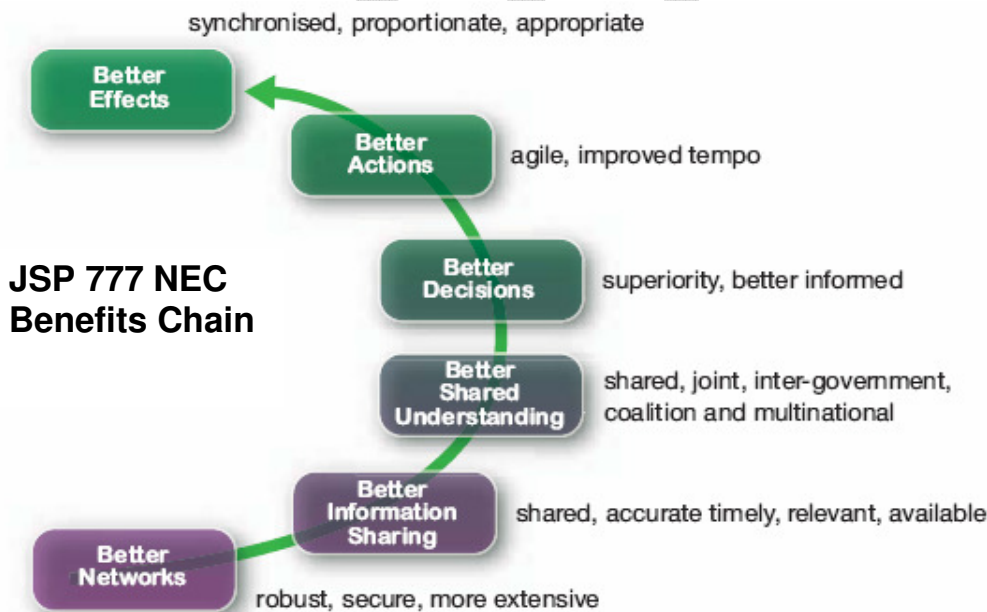


## INTRODUCTION

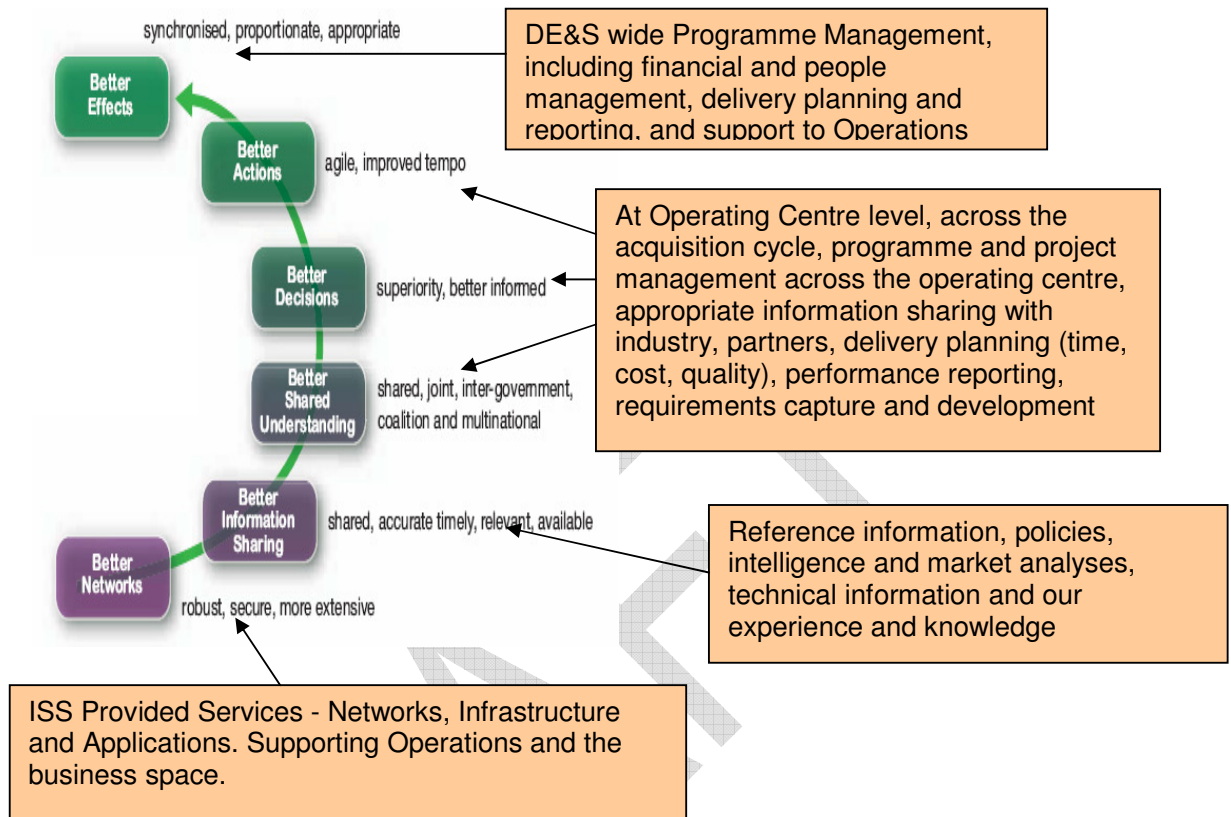
1. DE&S shares the same information vision as that of Defence, which is to achieve **“Agile exploitation of our information capabilities to improve effectiveness and efficiency on operations and in support areas through access to, and sharing of, timely, accurate and trusted information”**. Achieving this will enable better decision making in DE&S, which will improve acquisition processes and through resulting greater efficiencies in the support chain deliver increasingly better support to the front line.
2. The DE&S Business Strategy 2010-11 states that “Improving our access to and use of robust, timely and accurate information is critical to improving agility, efficiency and performance.” This strategy defines what that means for DE&S business and provides a means to achieve it.
3. This information transformation will move DE&S from an environment characterised by both information overload and lack of access to, or knowledge of, relevant information sources, to a structured approach to information assurance, management and exploitation. It will provide the ability to securely work collaboratively using technologies that reduce the burden of administration and provide high quality information sharing. Investing in our people will ensure they have the necessary information Skills, culture and capability they will be able to exploit information for business benefit.
4. This strategy is based on the MOD Information Strategy (MODIS) published in 2009, and it describes what DE&S information needs are, and the governance regime required to ensure these needs are met. It also describes a strategic approach to fully deliver DE&S information needs and then links to the DE&S CIO Business Plan for 2010 – 2014 which details how the strategy will be delivered. It also commits DE&S to meeting targets set in MODIS for Information Assurance, Information Management and Information Skills.

## WHAT INFORMATION DOES DE&S NEED?

5. Information is needed above all to enable decision making. The NEC Benefits Chain process described in JSP 777 illustrates this well:



6. In DE&S specifically information is required to support decision making in the following areas:



7. As part of the approvals process, to assure that DE&S is planning to deliver “information-smart” acquisition programmes.
8. Risk management is critical to all that DE&S does in delivering equipment and support. Effective risk management needs information support to assess, quantify and mitigate risks to DE&S outputs.
9. Furthermore, information sources in these areas have to be secure, reliable and up to date and we have to be able to access them easily and quickly.
10. Finally, people within DE&S need to be trained in managing information, and in how to effectively use that information.

## INFORMATION GOVERNANCE

11. This DE&S Information Governance structure will seek to ensure that good information management becomes the norm throughout the organisation and enables DE&S to exploit its information assets for battle-winning effect. The Governance structure is at Annex A, which also shows the relationship between DE&S governance and the wider Defence information governance picture.

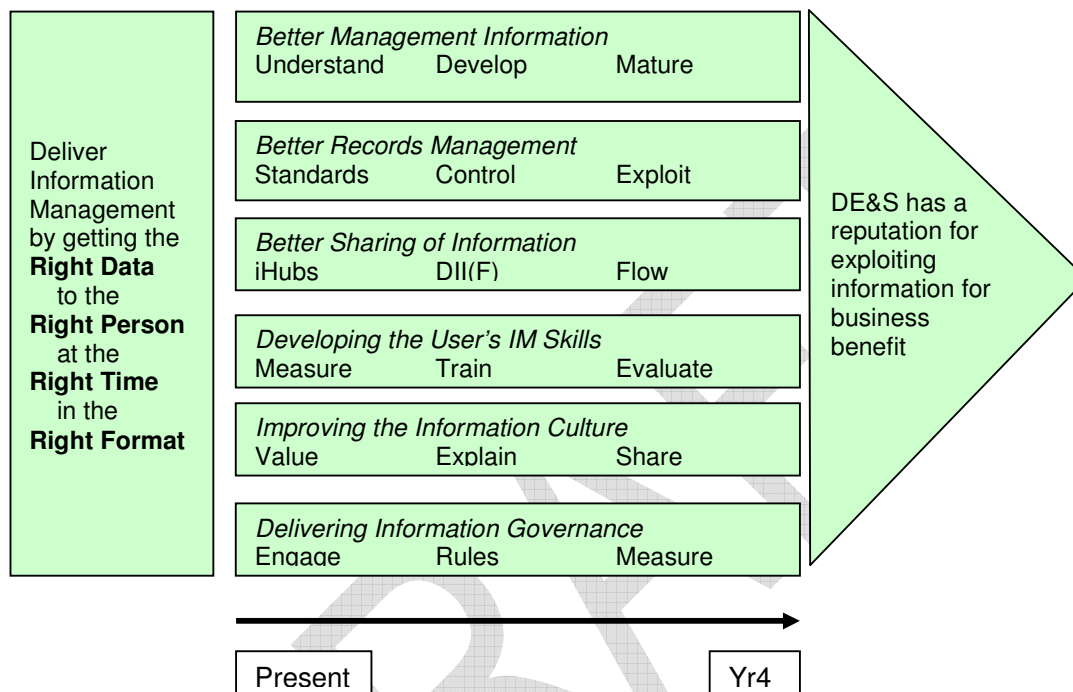
12. A key role for the Governance structure is to ensure that information risks are captured, understood and managed. The current programme & projects Board will oversee a programme of work to ensure that effective Information Risk Management (IRM) processes and procedures are adopted pan-DE&S and monitor progress against the targets set. The DE&S PPB will provide the direction to deliver Information Assurance and Information Management and ensure that DE&S is meeting its legal and Departmental responsibilities.
13. The current 1-star chaired Information Transformation Programme Board (ITPB) will be retitled the DE&S Information Transformation Forum and supporting ad hoc Information Working Groups (IWGs) will report directly to it. Information Asset Owners and Senior Information Officers across DE&S will be supported by DE&S CIO, and trained information management professionals formed into iHubs and supported by DE&S CIO will drive forward exploitation of information assets.

## **RISK MANAGEMENT**

14. There is currently no single risk management tool in use across the business; consequently DE&S CIO are working with the change team to move forward to a single risk management capability. This will define the business requirement for a coherent DE&S solution, and it is intended that the capability could be used in other Lines Of Development so as to support programme management of Through Life Capability Management.
15. Defence CIO has now issued a Information Risk Management Policy, this refers to information risk “appetite”, and sets out a framework for determining information risk appetite. DE&S CIO will ensure consistency between this defence requirement and the DE&S activity mentioned above.
16. Information risks must be recognised, recorded and managed effectively at all levels in DE&S, and the DE&S CIO team will review DE&S information risks to ensure this takes place. At the same time, the business led governance structure will ensure these risks are managed and mitigated effectively.
17. The DE&S Senior Information Risk Owner (SIRO), will use DE&S CIO to aid in understanding corporate level information risks, determining the DE&S risk appetite and in creating the appropriate mitigation plans. DE&S CIO will manage those risks on behalf of the SIRO, acting within a business driven governance framework, and will work with business areas who will be the owners of the majority of the risk mitigation work. DE&S CIO will ensure that the DE&S appetite for information risk is fully understood and put in place controls to ensure it is appropriately managed. Proper protection of information is fundamental in achieving this, but this has to be balanced against achieving business benefit through wider information exploitation, IAOs will be supported in achieving this by the DE&S CIO office. For example, Defence must reduce the possibility of compromise or loss of personal information to the absolute minimum, therefore the information risk appetite in this case would be low.

## STRATEGIC DIRECTION

18. The strategic direction for DE&S is described in the figure below. This shows how through continuous delivery of capability and development of skills and ways of working, DE&S can reach it's strategic objective.



### DE&S Programme Management

19. DE&S does not have a management information capability that can automatically extract information from Operating Centres and present it in a format that can assist programme level decision making. An easy to use and reliable way to extract essential underpinning performance, financial, commercial and other information is essential to speed up management processes and enable clearer and more up to date analyses.
20. The DE&S CIO team is working together with the Change Team, under the sponsorship of DE&S COS, and ISS Application Services to clarify the requirement for and enable delivery of an initial Management Information System (MIS) for DE&S. Alignment with the PACE IKM agenda will help to reveal decision making requirements within DE&S; in turn this will help derive the precise Management Information System (MIS) requirements. This work will continue, alongside defining the requirement and then seek funding for a full DE&S MIS capability. Importantly, this will not be an "additional" capability, but will become a coherent DE&S Corporate MIS.
21. This MIS programme will be supported by a development and procurement approach which will allow early delivery, and maximise flexibility in how the solution is delivered. Simultaneously, work will be undertaken to drive coherence across all DE&S information processes.

22. At Operating Centre level the same applies as to the Programme level, with the added complication of having to draw together information manually from process owners and front line commands. Within the operating centre, there is a clear requirement to share information between projects and with industry partners.
23. Information sharing across operating centres will be enabled using team sites, and these will be upgraded to new capability in-line with the DII programme.
24. The DE&S CIO team will also work with Front Line Commands (FLCs) and business process owners to drive further commonality in information management to develop a fully coherent solution.

### **Records Management and Reference Information**

25. DE&S CIO has already published policy and guidance on records management. This will continue to evolve as the capability of DII improves, particularly with delivery of Electronic Document and Record Management.
26. Reference information will include information used as part of day to day business; records of decisions previously taken, that enable audit but can also improve future decision making. Importantly, policies, rules and guidance and public domain information such as standards are also important sources of reference information.
27. DE&S CIO is also capturing in one place on the DE&S Intranet extant guidance and policy on information policy, rules and guidance.
28. Operating Centres have also now set up team sites to enable information sharing, and this will continue to be supported by DE&S CIO, particularly as the delivery of the DII Alamein, Blenheim and Cambrai releases will allow improved and consistent team site capability across DE&S.
29. Further work is also in-hand to look at how best DE&S can use information technologies to improve the way in which DE&S store and use reference information and how this can be shared. This would also include what information DE&S needs from and shares with the public domain, and what relationship will be required with MOD Information and library services.

### **Information Sharing with Industry**

30. Our industry partners now reach very close, and indeed into, the front line. Information is shared between DE&S and industry, this capability must be enhanced wherever necessary and wider sharing, where appropriate, made possible. Effective information sharing between DE&S and industry partners is critical to successful operations, balanced with the need to protect national security and the commercial interests of those partners.
31. DE&S project teams already use many methods to share information with industry partners. It is important that these relationships are designed to meet capability delivery expectations, and so business leaders must have flexibility to select appropriate tools and facilities. Agility and flexibility in communicating in a secure and timely fashion will be coupled with a simple affordable capability that can be delivered quickly to meet the business needs. This will be built on common services and resource-light maintenance of shared and trustworthy information.
32. To achieve our ambitions in this area will require a more agile and flexible procurement model, DE&S CIO will work with delivery partners to ensure a fully supported core capability is made available to business users, underpinned by reliable and coherent information sources. Business users will be able to tailor how this information is shared, and how it is presented.
33. DE&S CIO will establish the requirements for shared working with industry, and then work with delivery partners under business sponsorship to ensure the capability is made available.

## **Approvals Process**

34. As projects come up to their approval points they need to be assessed so DE&S can be assured that best value for money is being achieved. There is a need to make sure projects have built in the most effective and secure approach to information use, sharing, and exploitation.
35. Although it is important that project approvals processes include assuring information processes, it is equally important to offer an information coherence service to projects throughout their lifecycle. DE&S CIO will develop and deliver this process, to assure conformance with DE&S information architectures, information management and security rules and processes, and Network Enabled Capability joining rules.
36. A specialist team within DE&S CIO will assist in the gateway review process for the information aspects of projects by providing timely and effective guidance. This will aid DE&S to deliver equipment and support with coherent information underpinning. Capturing tangible and non-tangible benefits will help articulate, measure and demonstrate the benefits of better management of information and strengthen value for money arguments.

## **Process Information**

37. Delivery of capability requires integration across different information processes, such as those that deliver personnel, commercial or finance information, and also integration with front-line command requirements and demands, and with industry.
38. Work is already under way to understand the requirement for integration of coherent process information within a DE&S MIS. This will be further enhanced by working with Defence CIO on their emerging Management Information work, and through collaboration with process leads.
39. It is intended to build on the information relationships that Defence CIO are clarifying, to understand the required information flows between process owners, FLCs and DE&S. Opportunities will be seized to adopt consistent solutions, processes, tools and standards to expand the ability for exchange of information between applications, stakeholders and interested parties. The opportunity to reduce costs, for example through reduction of legacy applications, fostering partnerships, increasing interoperability and reducing manual overheads by automation of exchange within a known and controlled environment, will also be identified.

## **Knowledge**

40. Knowledge is about how DE&S makes sense of information, by linking it together, and helps provide an understand of the business world in which DE&S operates. DE&S has long sought to share knowledge, through learning from experience, but often this is locked away in people's heads. The challenge is to share and exploit that knowledge.
41. DE&S CIO are looking to build on work being undertaken by Defence CIO, and examples of good practice across MOD to try to develop knowledge management for DE&S.

## **Security and Reliability of Information Sources**

42. Information must be stored securely, it must be available when it is needed, and it must be up to date and reliable. This requires well managed data with appropriate applications to access that information.

Information Assurance within DE&S will be developed in line with MOD CIO expectations as expressed through the Information Assurance maturity Model.

43. The protection of information has been highlighted recently, the education of staff and adoption of best practices led by iHubs and other governance and support areas will be continued to ensure that DE&S improves its performance against Defence measurement processes.
44. Conducting Information Audits will give DE&S a better understanding of the realities of Information Assurance and will help generate more meaningful and accurate impact assessments of the information risks facing the business. In turn this will help identify areas requiring improvement and targeted solutions can be created and deployed. Use of the Defence standard review tools will ensure a consistent record of performance against department targets and the ability to compare performance pan-TLB.
45. DE&S CIO is working to continuously improve, streamline and rationalise information delivery mechanisms. This includes working with DII and Atlas to drive down legacy systems, and working with ISS AST to improve data quality, through a renewed MIS capability. This will deliver reliable and up-to-date information from the underlying data sources. At the same time, work is underway to specify the required minimum application set, and to develop a fast delivery method for generating applications for business use.
46. Following on from the initial Modernising Government agenda that helped deliver access to information through Freedom of Information and the Data Protection Act, DE&S will ensure that it has a robust structure in place to handle requests for information and make the most of the available tools to deliver replies efficiently.

### **Training to Manage and Exploit our Information**

47. DE&S personnel need to be trained in how to properly store information and in new ways of working to allow us to manipulate that information.
48. The MOD Information Skills Strategy will underpin a training and development programme for all DE&S users. DE&S CIO participation in the iMOSS project will provide lessons in the preparation requirements for business use of new DII capabilities. Lessons learned will be written into information exploitation guidance for DE&S users by DE&S CIO.
49. DE&S CIO will use the Defence maturity models to assess Information Management and Information Assurance performance. DE&S CIO will engage with and support Defence CIO to ensure the models capture and assess the unique requirements of DE&S wherever this is possible. The potential to exploit information across traditional system boundaries will be explored and where activities offer significant savings these will be accelerated to drive out hard-cost savings. Involving industry partners as well as identifying cross-department collaborative working opportunities will demonstrate DE&S commitment to delivering better business outcomes through engagement and better use of existing and emerging technologies.
50. Building on the "Protecting Information" training, staff will refresh their awareness of their obligations to protect and manage access to information whilst ensuring the need to share is fully complied with.

### **Next Steps for the CIO**

51. The DE&S CIO has issued its Business Plan for 2010-14 which describes the actions it will take to transform the way we in DE&S will manage, share, present and exploit our information to achieve our

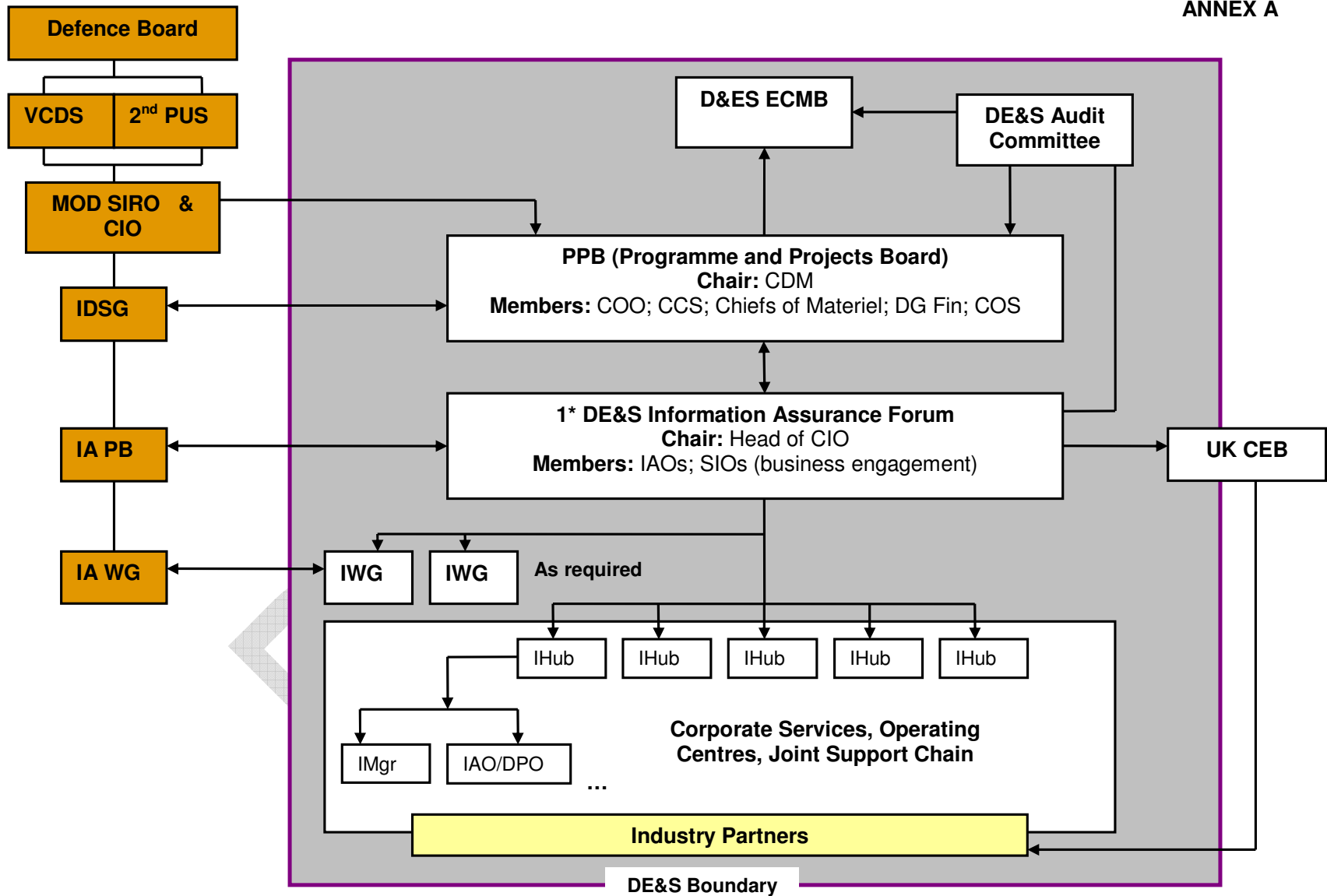
outputs. An immediate priority is to get approval for this Strategy; this will be done through the ECMB in June 2010 providing the authority to drive the Information Agenda forward.

52. DE&S CIO is already engaged on three fronts. First, it is planning the preparation and rollout of the DII Release 2B "Alamein" capability enhancement. This release of DII will provide teams with improved information storage and sharing capability (MOSS), an improved e-Search capability, an upgraded directory (e-Directory) and a new Defence Intranet platform, also based on MOSS.
53. Second, DE&S is delivering an improved Information Capability Assurance service through the Information Capability Assurance Team (ICAT). ICAT will provide teams with clearer guidance to ensure new project gateway submissions fully consider how the information elements of new capabilities co-ordinate with other emerging and existing systems.
54. Third, DE&S CIO is improving the organisation's standards of Information Management and Skills to meet our Defence Information Management and Skills Maturity Model (DIMSMM) targets. We are committed to achieve Level 2 of DIMSMM by February 2011, and we cannot do this without the full co-operation and participation of the DE&S Business teams.
55. To prepare for the rollout of Alamein and to advance DE&S towards Level 2 of the DIMSMM, teams must undertake a number of actions. As a pre-requisite to Alamein rollout, teams must appoint Senior Information Officers (SIO) and Information Managers (IMgr), and they must undertake the appropriate training. Information Hubs (iHubs) must be created, the iHubs roles must be filled and the appropriate training undertaken. In addition, teams must develop their Fileplans, consistent with the MOD fileplan and split their current information into Work-In-Progress (WIP) and Records. Individual users must adopt new ways of working, such as those detailed in the JSP747 IM Protocols<sup>1</sup>.

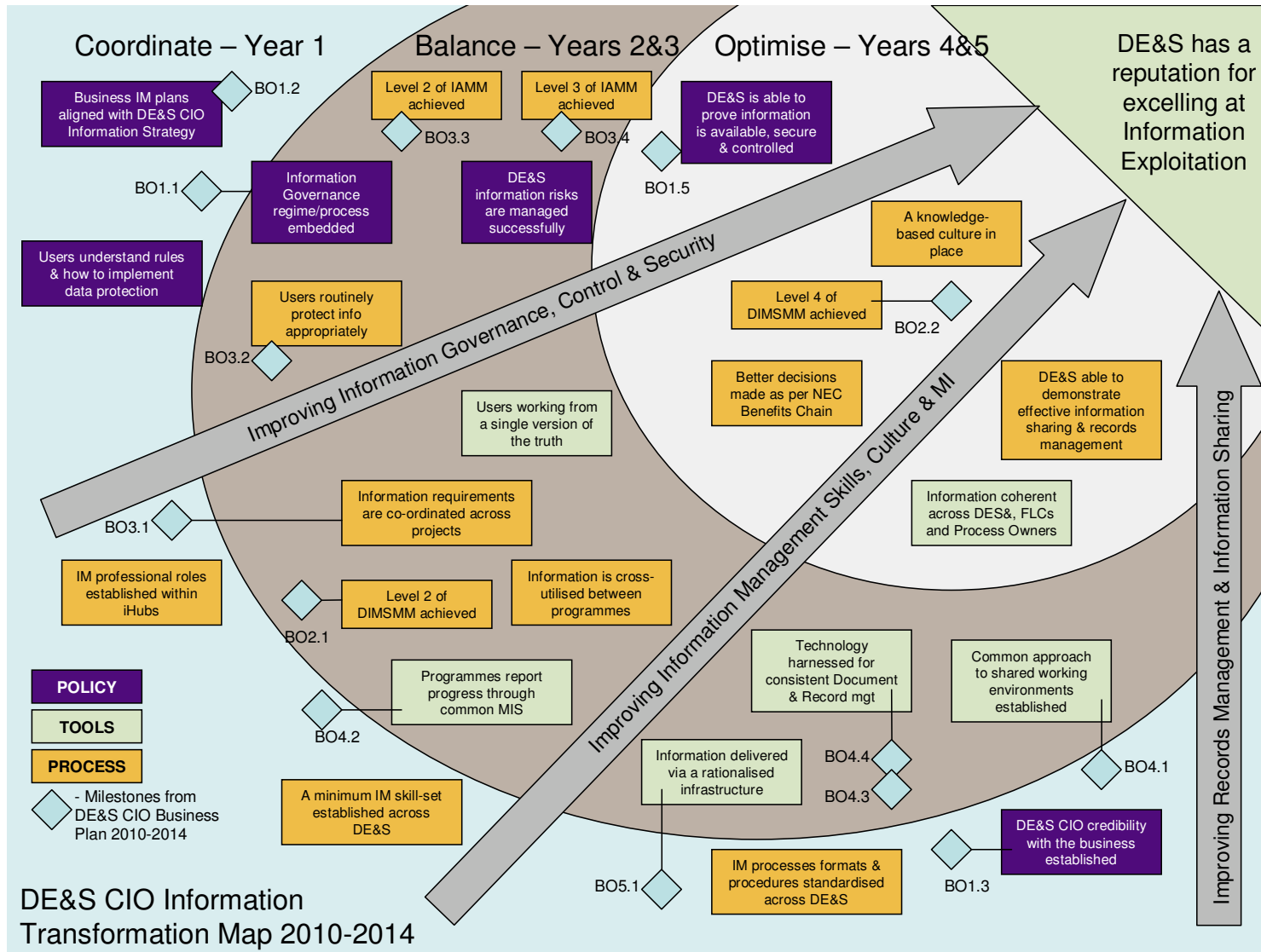
DRAFT

---

<sup>1</sup> More information can be found on the DE&S CIO Defence Intranet pages.



# DE&S CIO Information Transformation Map



**DRAFT**

**INTENTIONALLY BLANK**