Australian Government
Department of Defence

Defence Information Management Strategic Framework

'First steps'

Information is a critical component of effective decision making and must be managed in such a way as to ensure that the right information gets to the right person at the right time.

Co-Sponsors: Deputy Secretary Strategy
Chief Information Officer

September 2010

Contents

EXECUTIVE SUMMARY

Information: a strategic Defence asset

Information sources are fast evolving and Defence must be able to fully exploit the use of information across our three distinct Information Management (IM) domains – war-fighting, intelligence and corporate.

Information is a strategic asset for Defence. IM is the capability that will bring that asset properly to bear on Defence's business and, in doing so, will improve decision making.

Defence has been using, saving and transmitting information for many years. Today, we have unprecedented technology to create, manipulate and use information. If we are to harness the use of this technology efficiently and effectively, then we need to identify and implement management systems to translate our information strategic asset into a Defence capability.

The need to manage information

Defence needs an IM Strategic Framework to address the serious risks posed to our activities and business through existing inefficient, unilateral and unaligned processes. Since the first introduction of electronic forms of IM in the mid to late 1980s, successive organisational change has progressively removed the previous uniform structures and procedures within Defence for managing information – albeit ones that were in place essentially for a paper-based system. Essential corporate knowledge and core personnel responsible for ensuring compliance and championing sound IM have been lost.

Defence no longer has a consistent approach to IM. This has resulted in a continuing challenge to comply with legislative requirements and an eroded confidence in the integrity of information provided to demonstrate evidence-based decision making. Defence personnel are severely constrained through an inability to easily search, access and share information. Similarly, existing Information Communication and Technology (ICT) solutions within Defence are not addressing user needs.

The vision

The vision for IM within Defence is the provision of a capability that is based on providing the right information at the right time to the right person to enable the right decision to be made.

This will depend upon:

- a single source of truth (the right information);
- information governance (the right time);
- a culture of information sharing between those who need to know (the right person).

With the adoption of the Strategic Framework, all decisions made throughout Defence that underpin IM will be aligned to a set of Defence's IM principles and objectives which, in turn, are linked to the Defence Business Model, thus aligning responsibility and accountability in achieving outputs within the context of the broader Defence governance regime.

Strategic alignment and consistency

In this paper, we describe mechanisms that will ensure strategic alignment and consistency within Defence by:

- enabling **superior decision making** by providing the right information to the right people at the right time;
- improving **information visibility** through a Defence Information Entity Model;
- allocating **information responsibility** to business process owners;
- improving the management of risk through assuring the **quality** of information;
- improving the **protection** of the information that we hold;
- **breaking down silos** within Defence through a program of cultural change; and
- **a**llocating adequate **resources** to make change happen.

Principles of information management

The following principles underpin this framework:

- Information is a valuable strategic and corporate resource.
- Information must be governed centrally, but easily shared across Defence.
- Information must be managed in accordance with security and legislative requirements.
- Information must have a single, authoritative source (a core record).
- Information is to be managed with a focus on meeting user requirements.

Objectives

The IM Strategic Framework has the following overriding objectives:

(a) Achieve the right information being available to the right person at the right time to support the conduct of Defence business.

(b) Achieve ICT solutions that are driven by user requirements.

(c) Achieve legislative compliance.

(d) Achieve resource efficiencies by being able to search for and locate the right information quickly and easily.

(e) Achieve effective and efficient ICT expenditure through ensuring visibility and use across Defence of existing software applications.

(f) Achieve a system of Corporate Governance which clearly defines responsibilities and accountabilities for the management of information.

(g) Achieve a set of common Business Rules to direct the appropriate handling of information and achieve the necessary integrity of information across Defence.

The successful achievement of these objectives will require sustained effort over several years. However, with appropriate resourcing and whole-of-Defence support, significant IM reforms can be realised progressively and an acceptable level of IM maturity could be realised in three years and IM could be well established in five years.

At the three-year mark, IM would be emerging as a capability in the organisation as its benefits became apparent. A single version of the truth would exist for information (the right information). There would be a set of standards for the description and definition of data and information (the right time) and an integration of information silos (the right person).

At the five-year mark, IM would be established as a critical capability. Information would be available as a service to processes thus enabling rapid process improvement in response to environmental changes.

Following endorsement of the Strategic Framework, we will develop an Implementation Roadmap which will include a program of work and detail resource requirements for the remainder of the program, as well as progress a number of initiatives as Quick Wins. Specific initiatives to be undertaken in the first six months include:

- developing an approach to cultural change, to prepare a communication strategy and to begin implementing that strategy through a dynamic communication plan;
- further developing the overarching IM governance arrangements through initiation and progression of elements of the IM Project;
- relating the processes described in the Defence Business Model to high-level information groupings, thus aligning responsibility and accountability in achieving outputs within the context of the broader Defence governance regime; and
- identifying the Defence key performance indicators (KPIs) from the Defence Business Model (outputs) and to identify the primary sources of information that would be used to populate these KPIs. We will work closely with the Strategic Reform Group Executive to progress this.

We will report to the Defence Committee in March 2011 on the Implementation Roadmap and the Quick Wins achieved over the next six months.

Purpose of paper

The purpose of this paper is to describe a Strategic Framework that will improve the management of information within Defence. The consequence of improved information management (IM) will be enhanced decision making by all staff, both military and civilian, within Defence. The Strategic Framework describes a vision and a set of steps that need to be taken to achieve that vision.

The analysis and recommendations contained in this paper are based on consultations both inside and outside Defence together, with a comparison with private sector practices.

Introduction

The Defence IM Strategic Framework will ensure that all personnel, both military and civilian, have the ability to provide, consume and require timely, open and effective information, when it is needed and where it is needed.

The following philosophy underpins the IM strategies and approach:

To ensure that the right information gets to the right person at the right time to make the right decision.

The development of the IM Strategic Framework, the first for Defence, follows the Defence Committee's consideration and agreement on 26 November 2009 that Defence requires a structured, user focused and effective system to manage information, and to mitigate current, significant risks. However, Defence's IM practices can only improve if the requirements of our personnel are met and the Strategic Framework is aligned with the stakeholder advice provided.

At the outset, it is critical to note that IM is not Information and Communications Technology (ICT). The principles in the Strategic Framework will be used to derive a set of supporting ICT requirements which, in turn, will inform the deployment of ICT systems. Ensuring that Defence has the necessary ICT systems is an important component of IM. However, fundamental to achieving effective IM is the recognition that it is the user requirements which drive IM and when linked to these requirements, the specific ICT systems and solutions will enable IM to occur in an effective and efficient way.

Additionally, the Defence ICT Strategy is to be informed by the IM Strategic Framework. The ICT Strategic Plan's approach and objectives should be consistent with ICT enabling improved IM and Defence achieving its overall IM objectives.

Defence maintains a highly skilled and professional workforce. However, even with the organisation's best endeavours, its full potential remains unrealised due to inefficient and disparate IM practices. Currently, information is not being managed across Defence in a consistent manner, the integrity of information often cannot be verified (there is not a single identifiable source) and evidence for key decision making is not readily available.

Several IM initiatives are already underway within Defence. Whole-of-Defence initiatives include upgrading and rolling out the Defence Records Management System, streamlining the System of Defence Instructions and developing a governance regime for our Defence internet and intranet sites, as well as specific and separate IM initiatives in Groups and Services such as Navy and Air Force. It is not the purpose of this document to delay these initiatives. Rather its purpose is to improve alignment between them through a corporate approach that will have the effect of establishing unity of approach across Defence and accelerating progress. Annex A lists these initiatives. Individual Groups and Services will be responsible for ensuring that their initiatives align with Defence-wide standards for IM being developed by Strategy Executive and CIOG.

Defence will also soon be subject to significantly more rigorous legislative requirements that will result in substantially more information being required to be made publicly available. If Defence does not reform and establish a leading practice IM operating environment, the organisation's reputation will continue to be jeopardised and any potential information 'advantage' will not be realised.

The absolute imperative to transform from a stove-piped information paradigm to a networked, agile, information-adaptable Defence organisation is unquestioned. This Defence IM Strategic Framework will establish the vision, goals and approaches that will guide the required IM initiatives and investments for the Whole of Defence enterprise.

How information is managed is an integral part of strategic planning across Defence. The establishment of robust corporate governance, clear and common business rules and appropriate resourcing will ensure that the best value of this fundamental organisational asset can be realised.

High level information requirements must also be aligned with the enterprise strategic and business drivers.

What is information management?

Definition

IM in this context is defined to be getting the right information to the right person at the right time to enable him/her to make the right decision.

The purpose of IM is to enable effective and efficient performance management and decision making through the provision of timely, accurate and up-to-date information. Its scope covers the complete breadth of Defence's business: war-fighting, intelligence and corporate administration.

Data management

IM should not be confused with data management. Data management relates to organisational and technical tasks concerning the planning, storage, and provision of data, both for computer personnel and end-users.

Structured and unstructured information

We tend to regard information as being structured or formatted data that is held in a computer. Increasingly and with the advent of the Internet, most information (some estimates suggest as much as 99%) of information is unstructured. The Internet has not changed the existence of this information but it has changed our ability to access it. It is worth pointing out that the information that Defence needs to make decisions affecting its business is not necessarily owned or created by Defence. The focus of information systems provision has shifted from storage to access or retrieval.

It is the need to cope with the accessibility of this unstructured information, together with the (relatively) small amounts of structured information that today challenges the decision maker. To a significant degree, network centric warfare (NCW) depends upon information superiority. This superiority is achieved through enabling access to the optimum amount of information to facilitate a timely decision.

Information as a strategic asset

Information is critical to the business of Defence both for operational and administrative purposes. Defence's war-fighting capability depends upon a commander's ability to seamlessly access intelligence, logistical and personnel information in order to make strategic or tactical decisions.

The Strategic Reform Program[1] describes a significant program of administrative reform to address what has been referred to as the "broken backbone" of Defence. The management, monitoring and ultimate success of this program will depend upon access to information.

The importance of information as a strategic asset has been recognised by Defence papers in other countries. In the United Kingdom, the Ministry of Defence's Information Strategy 2009[2] states that "information … [must be] … treated as a strategic asset". It says that "Defence information is a strategic asset, which needs to be managed in a structured way, made accessible to those who need it, and protected in accordance with security, legal and commercial requirements."

The United States Department of Defense Information Enterprise Strategic Plan, 2010-2012[3] highlights the "importance of information sharing to national security". The document paints a vision of "mission success" which, it says, means "treating information as a strategic asset".

The benefits of IM

There are several benefits to effective IM within any organisation and Defence is no exception:

- improved decision making;
- improved data quality and accuracy;
- improved organisational integration;
- increased productivity; and
- enhanced reputation.

Current situation

Information collection

The current situation was derived by talking to staff within Defence, drawing comparisons with IM practices outside Defence and through an independent

[1] The Strategic Reform Program 2009; Delivering Force 2030

[2] UK MOD, 2009, http://www.mod.uk/NR/rdonlyres/530403AF-FC89-41E0-852F-4D2934C15001/0/2009_MODIS.pdf

[3] US DoD, http://cio-nii.defense.gov/docs/DodIESP-r16.pdf

consultancy[4] aimed at assessing the degree of IM maturity within Defence.

Information maturity

A recent consultancy assessed the existing maturity of Defence IM ability along a number of dimensions:

Strategy: the degree to which there exists a plan of action, a strategy, for delivering business value.

Organisation information use/users: the degree of user sophistication at transactional, operational and analytical levels and covers internal business users, business partners and customers.

Information process: the degree to which information processes support the capture, storage, transformation, delivery and use of information in operational, reporting and analytic business processes.

Data: the degree to which data and information is standardised, granular, and readily available as a service.

Governance: the degree to which there exists governance to deal with the management of priorities, plans, business processes, applications and data.

Information technology: the degree to which ICT is ready to support the concept of information on demand.

IM in Defence: current maturity level

Based on interviews and external comparators, Defence maturity was assessed[5] on a scale of five levels (see Table 1 below), with five being the highest level of maturity.

Level	Description
1	Data is available to run the business but there is considerable *ad hoc* and manual dependence. There is often no single version of the truth. Data availability is an **embryonic** form of IM.
2	There is some degree of information availability and a degree of integration across the business. Work environments tend to be disparate or siloed with limited end-to-end process visibility.
3	A single version of the truth exists for information. There is integration of silos and a set of standards for the description and definition of data and information. At this level IM is **emerging** as a capability in the organisation as its benefits become apparent.
4	Information is available as a service to processes thus enabling rapid process improvement in response to environmental changes. At this level IM is **established** as a critical capability.
5	Information is a competitive differentiator. Processes can be adapted in real-time. IM is **embedded** in the culture of Defence and is self sustaining and self-optimising.

Table 1: Maturity levels for IM

An assessment of the current maturity of IM in Defence is illustrated in Figure 1 at page 10. The left side of the figure shows (in red) a band of maturity to reflect the

[4] Assessment of Information Management Maturity at Department of Defence, IBM, 2009

[5] The maturity levels were assessed based on a detailed questionnaire completed during an extensive interview process with a number of Senior leaders in Defence

fact that different parts of Defence are at different levels. The line within the band illustrates the current average maturity across Defence.

IM and ICT

In analysing the current situation it is important to draw a distinction between:

- the identification of information needs and the use to which information is put; and
- the systems and technology that facilitate the storage, manipulation and retrieval of information.

Desired situation

IM as a Defence Capability

The desired state for IM in Defence is that information should be recognised as a critical component of effective decision making and should be managed in such a way as to ensure that the right information gets to the right person at the right time.

In three years' time:

- IM will be regarded as a rapidly emerging Defence capability in line with its acceptance as a strategic asset *(we will have confidence in the information we provide);*
- information owners will have been identified for the main groupings of information *(we will be clear about who is responsible and accountable for specific information)*;
- information owners will actively contribute to the development of processes and systems that facilitate access to that information *(we will have access to all the information we need to make a decision);*
- there will be consistent mechanisms for assuring and managing the quality and provision of information across Defence *(we will have common business rules to support quality business processes);*
- there will be a single source of truth for all significant data *(we will know where to find the right data*); and
- the linkage between information systems and the information required to measure performance will be transparent *(we will be able to report quickly and accurately).*

Achieving this would mean that IM becomes a Defence Capability within the meaning of the *Defence Capability Development Manual, 2006*. "...In ordinary usage, 'capability' means the capacity to be or do or affect something. The term can refer to a quality, capacity or ability… 'Capability' in the Defence context is the combined effect of multiple inputs. It is not the sum of those inputs, but the synergy that arises from the way those inputs are combined and applied that determines the level of capability in a particular context…"

In order to maximise Defence's IM capability, its IM maturity needs to increase in line with Figure 1 below to move from the red band to the green band in three years.

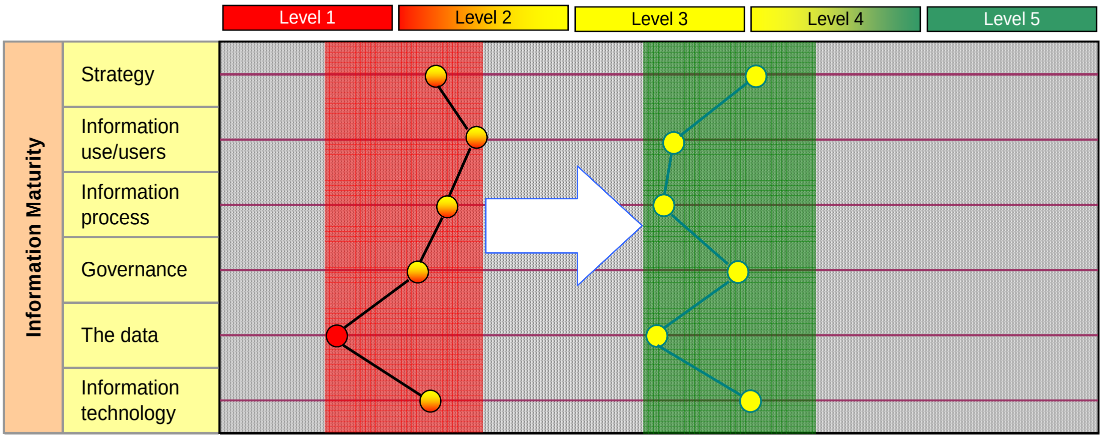

Figure 1: Desired Defence IM maturity

A realistic, measured vision

It is important not to be over ambitious. This document proposes work that can be reasonably achieved in three years at an affordable cost and an acceptable risk, both in terms of the financial and personnel commitment required. It is important also to recognise that the defence environment will continue to change rapidly, as it has over recent years. Figure 1 shows that Defence needs to:

- develop a strategic approach to IM to the degree that information enables innovation based on its acceptance as a strategic asset;
- describe the configuration of the information that it uses to run its business in the same way that it would configure any other asset;
- relate information to the business processes that create it and are responsible for it;
- establish governance processes that encourage the right culture, attitudes and behaviour in relation to information sharing and protection;
- ensure that the data that supports IM is created and stored only once; and
- establish an suitable ICT infrastructure to support a new, consistent and coherent approach to IM.

This is a realistic description of where Defence could be in three years. Within five years, we would expect to be at about level 4 although some areas such as Intelligence will need to be (and for some dimensions already are) at level 5.

The reason for not seeking to reach level 5 in all areas of the IM Maturity is that, in assessing progress made at the five year point, it may be that the levels reached are deemed adequate for most of Defence's requirements then and for the foreseeable future. To attempt to achieve level 5 across the board may not be cost effective or significantly value adding.

Enhancing IM in Defence

The risk of doing nothing

There are a number of risks associated with doing nothing: that is, in assuming that existing initiatives are capable of addressing Defence's low IM maturity:

- It will continue to be difficult to ensure that the right information is being used in decision-making processes, through the lack of having a single source of verifiable information.
- In particular, it will be difficult to measure the progress or pace of reform in Defence which will limit the effectiveness of that reform.
- Defence will be unable to comply with legislative requirements, such as the *Archives Act 1983, Freedom of Information Act 1982* and the Information Publication Scheme.
- Wastage and inefficient use of financial and personnel resources will continue with the duplication of information creation and processing.
- The imbalance will increase between Defence's use of and reliance on electronic information with inconsistent, ineffective and misaligned practices resulting from a lack of central guidance, structure or defined responsibilities.
- There will continue to be limited assurance that the right systems are being used for particular business needs.

Principles for IM

The following set of Defence IM principles will underpin the IM Strategic Framework:

- Information is a valuable strategic and corporate resource;
- Information must be governed centrally, but be easily shared across Defence;
- Information must be managed in accordance with security and legislative requirements;
- Information must have a single, authoritative source (a core record); and
- Information is to be managed with a focus on meeting user requirements.

Areas of focus

In order to bridge the gap between the current and target states several areas of focus require attention to improve IM maturity. Resourcing is discussed later in the paper. The following are the areas requiring focus:

- Governance
- Cultural Change
- Visibility
- User Requirements
- Compliance

Governance

An examination of the Strategic Reform Program shows that both the savings streams and non-savings streams depend upon information that is consistent, timely, accurate and up-to-date. This information is required both to base-line a starting position and then for monitoring the progress of reform.

Progress has already been made in establishing elements of a governance regime. The responsibility for IM is in the remit of Deputy Secretary Strategy. The role of CIOG is to provide user-driven systems, technology and communication capacity and capability to the business to enable decision making.

To improve the integrity of Defence's information, a robust corporate governance framework for IM must be consolidated, and directly linked to this will be the establishment of common Business Rules that clearly articulate how information is to be managed, stored and made accessible.

The Governance structure must ensure the full engagement of stakeholders, an understanding of accountabilities and responsibilities throughout Defence, and allow for effective feedback to ensure IM is driven by user requirements.

Other governance initiatives in the form of Information Manager champions in each Group and Service, the Defence Corporate Information Management Improvement Committee (DCIMIC) and the Information Management Steering Committee (IMSC) also contribute important management functions to move the IM agenda forward.

Additional governance arrangements are likely to be established to oversee other aspects of the IM agenda and work has commenced to capture and further develop the overall governance model.

Cultural change

The backbone of IM is culture. It is often the case that, with perhaps good intentions, information is power. If information is power then the likelihood that it will be readily shared is not high.

It is also the case that executives and managers ask for information just in case it is needed. Senior leaders need to know that information is available (should it be required). Adjusting executive behaviour in this way will result in significant savings in time and effort but it does depend upon trust in the information resource.

Issues associated with the consistency of IM arise for two related reasons:

(a) the difficulty of managing the business of Defence as a single operation entity means that its objectives must be met through the inter-operation of a number of different Services and business units; and

(b) the managers of each of these business units need specific information to achieve their business objectives.

Over the years, a culture has arisen whereby there is a tendency not to share information readily. Defence will need to pursue proactively significant organisational cultural change to instil the consciousness that IM is everyone's responsibility. Through ensuring Defence personnel are engaged and embrace the need for IM change, it will be understood that along with direct responsibility comes clear benefits.

Improvements to searching and retrieving information will lead to improved confidence in the integrity of information. A change in culture will also be linked to training and to developing accountability and responsibility for information.

Cultural change is long and arduous, but a vital, process. It depends upon having a clear vision, which this document proposes, and will then require some specific interventions:

- a baseline of current behaviours and a means of tracking cultural and attitudinal change;

- the identification and tracking of staff's information roles and dependencies;
- extensive consultation to understand barriers and enablers for change;
- a clear, consistent and coherent communication plan that gives messages through channels that reach the greatest number of people;
- the identification of IM skills and the embedding of those skills in the workforce, including at the most senior levels, through suitable training and development;
- the modification and use of formal performance based tools, such as the Performance Feedback Assessment and Development Scheme.

Visibility

Defence must cease the practice of unilateral decision making for IM processes and ICT solutions. This practice is the result of a widespread lack of visibility of endorsed Defence policy, as well as of existing technology solutions, which manifests itself in high levels of wastage, duplication and inefficient allocation of scarce resources.

CIOG is establishing a whole-of-organisation database of the existing ICT software and applications and how these can be applied to Defence business. Licensing and use of ICT solutions for IM are now centrally governed to ensure an end to the current practice of duplicate purchasing of the same or similar equipment and software. This work will assist in improving IM.

Effective IM also depends upon the timely visibility of the information that is needed and, to a degree, the relationship between each group of information. There is no Defence Information Entity Model (DIEM). The DIEM is essentially a diagram that identifies logical groupings of information used by Defence, whether structured or unstructured and whether owned by Defence or not. It may also show the relationships between those information groups.

The DIEM is different to a Corporate Data Model which defines structured data and its relationships and is required for systems purposes. The DIEM, on the other hand, will assist in the allocation of responsibility for information to business owners.

User Requirements

The achievement of Defence's business outputs and outcomes depends upon a clearly defined set of business processes. Every business process consumes information and many create information. The process owner should be responsible for describing and defining the information requirements for the process. The DIEM will enable Defence to allocate responsibility for each information group to the business process owner of the process that creates it. Where there is more than one creating process an informed decision can be made about the allocation of responsibility.

Ownership of information is important for several reasons:

(a) the relationship between information and key performance indicators (KPIs) can be made explicit;

(b) responsibility for the requirements for systems that create, store and manipulate information can be allocated; and

(c) it is clear where responsibility for the protection of that information rests.

Compliance

The protection of information is critical to Defence's operational capability. Defence has excellent policies in place for the protection of structured and unstructured information. But the context within which information should be protected changes with time.

The current situation is that Defence's information is protected by default; in the future Defence's information will be unprotected by default implying the need for a tightening of governance and compliance processes.

Defence must ensure it is compliant with current and potential future legislative requirements. Defence is about to see significantly more onerous public disclosure requirements for its information than hitherto, and will need significantly to reform current processes to meet this challenge.

These requirements represent an enormous change to the way Defence has traditionally managed the public release of its information. This includes through the amended Freedom of Information Act including the Information Publication Scheme (IPS), as well as Govt 2.0 initiatives that will require Defence, as a normal part of our business, to make publicly available substantially more information.

As part of the new IPS, Defence will need to ensure that the information published is accurate, up to date and complete. Defence will cease its current inconsistent approach to IM and will put in place uniform and sophisticated (but clear) business processes to support these requirements.

Next steps

Communication

The IM Strategic Framework must be communicated in a structured way to all stakeholders, keeping them informed, engaged and up-to-date on project activities, and to provide a mechanism for stakeholder's feedback for their concerns, issues and new or additional requirements.

The next six months – quick wins

There are several opportunities to make early progress in the area of IM reform and to demonstrate early benefits. A preliminary plan for achieving these, based on 5 work streams, is illustrated in Figure 4. Following endorsement of this Strategic Framework, Deputy Secretary Strategy, in partnership with the Chief Information Officer, will lead the work described in Figure 4 and report progress back to the Defence Committee.

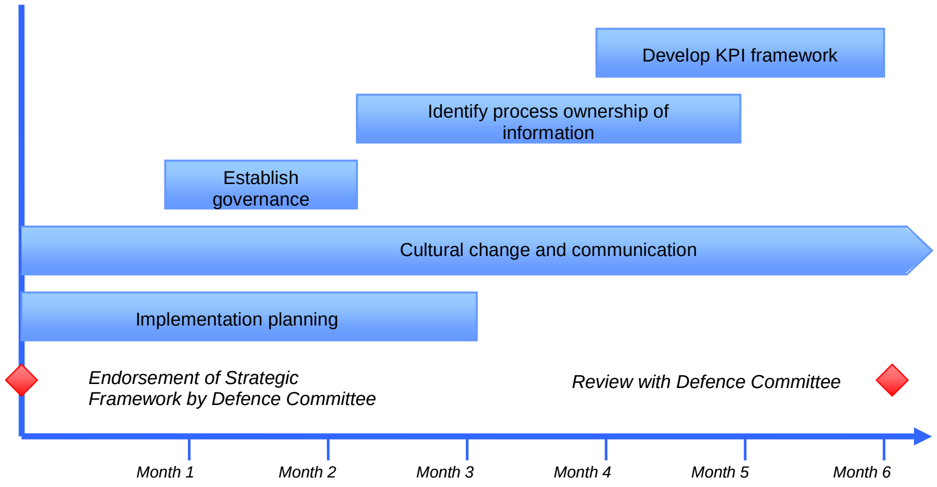
Develop KPI framework
Identify process ownership of information
Establish governance
Cultural change and communication
Implementation planning
Endorsement of Strategic Framework by Defence Committee
Review with Defence Committee
Month 1
Month 2
Month 3
Month 4
Month 5
Month 6

Figure 2: The next six months – Quick Wins

Implementation planning

The purpose of this work stream is to build an implementation roadmap, which will include a program of work and detail resource requirements for the remainder of the program. This planning will inform the IM Project currently being conducted under the Strategic Reform Program.

Output: Implementation roadmap and associated resource requirements.

Cultural change and communication

The purpose of this work stream is to develop an approach to cultural change, to describe a communication strategy and to begin implementing that strategy through a dynamic communication plan.

Output: Cultural change assessment, preliminary communication, communication strategy (by the start of month 4).

Establish governance

The purpose of this work stream is to further develop the overarching IM governance arrangements.

Output: Charter, terms of reference and plan of implementation for any new governance arrangements.

Identify process ownership of information

The purpose of this work stream is to relate the processes described in the Defence Business Model to high-level information groupings, thus aligning responsibility and accountability in achieving outputs within the context of the broader Defence governance regime.

Output: allocation of information ownership to process owners, Development of an initial Defence Information Entity Model (DIEM) to link process and information ownership together.

Develop KPI framework for IM

The purpose of this work stream is to identify the Defence key performance indicators (KPIs) from the Defence Business Model (outputs) and

(a) to identify the primary sources of information that would be used to populate these KPIs; and

(b) to identify any gaps or issues.

Output: a Defence KPI framework, developed in conjunction with the SRG Executive.

Longer Term Program of Work

The following table describes a program of work:

Project	Objective	Key outputs
Governance	To describe a set of governance arrangements for the management of information as a defence capability.	An assessment of the effectiveness of the IM Strategic Framework against the KPIs defined by the IM Implementation Plan.
IM Implementation Roadmap (Resources)	See below.	See below.
Cultural Change	To describe a program of activities designed to change behaviours and attitudes toward the ownership, sharing and protection of information as a strategic asset for Defence.	Assessment of the degree to which silos are broken down and information is visible as an end-to-end resource.
Visibility	To develop a DIEM that will be used to maintain ownership of information by process owners.	Assessment of the extent to which groupings of information used by Defence are described and understood.
User Requirements	To identify business process owners' responsibility for particular information groups within the DIEM.	Assessment of the effectiveness of business process owners in expressing requirements to CIOG.
Compliance	To review and update policies relating to the protection of information within Defence.	Assessment of the effectiveness of the protection of Defence's information resource.

Table 2: IM Projects

Commitment

The realisation of the vision described in this strategic framework will require the continued commitment of all levels within Defence. This commitment will need to start at the top and senior officers and managers will need to lead by example, particularly in the area of information sharing.

Resourcing

The program of work described above will need to be adequately resourced. This depends upon the resourcing requirements being identified and justified against expected longer term benefits.

Defence currently has sufficient financial allocations to support critical ICT solutions which enable the IM requirements to be implemented. However, Defence's personnel resources are a critical challenge to achieving IM reforms.

The immediate action, therefore, is to develop an IM Implementation Roadmap.

This work will produce six key outputs and should be completed within 12 weeks:

- the constitution and terms of reference of the governance arrangements for IM and the relationship between it and existing governance. Where it needs to recommend changes to existing governance arrangements it should do so;
- such expansion of the IM vision that it considers necessary;
- a detailed IM Project plan that describes the activities to take place over the next 36 months and beyond. In particular it will produce project briefs for each of the projects identified, including records management (including visual), a web content management system, IM governance, an enterprise search engine, business intelligence and data warehousing. This project is already identified under SRP for funding ;
- the resources, both skills and financial, necessary to achieve success;
- an expansion of the benefits to be achieved through effective IM; and
- the communication plan that needs to be established associated with the implementation of the Strategic Framework and its associated projects.

We will report progress to the Defence Committee on the IM Implementation Roadmap and its associated Quick Wins six months after the date of this paper.

ANNEX A

Current Information Management Initiatives

Records Management

A Strategy was agreed by the DC in November 2009 and is being progressively implemented. The major initiative is the adoption of the DRMS as the mandated records management system for Defence. EDMS/DRMS will be upgraded in late September and mid October respectively and rollout out to proposed new users (approx 30,000) will occur progressively over about 24 months commencing early 2011.

Visual Information Records Management Project (VIRM)

A Strategic Plan is being developed to enable the corporate management of Defence's Visual Information Records (imagery and video). Processes for determining the user requirements for the upload, storage and management components of the project are in train. Currently VIRM is expected to be implemented in 2011-12.

Internet/Intranet Compliance Project (IICP)

A project to develop a compliance regime for internet and intranet usage has commenced. Currently work is being undertaken to develop governance and reporting frameworks and Chapter one of the Internet/Intranet Compliance Manual has been circulated for comment. The project also includes action to ensure minimum compliance with the government's requirements under the amended FOI Act and the Information Publications Scheme. The project is due for completion by mid 2011.

Web Content Management System (WCMS)

Acquisition of a WCMS is proposed as an initiative under the IM project. Work is currently being undertaken to audit the web estate and to develop use requirements for the system. It is envisaged that the acquisition and implementation of the WCMS will occur at the end of 2012 for the Defence Internet.

System of Defence Instructions (SoDI)

A Strategy was agreed by the DC in March 2010. Three of seven projects have commenced starting with the review of the DI(G) and Defence Manual business processes. Action to update the out-of-date DI(G)s/Manuals has commenced and is scheduled for completion by end 2012. Single Service Instructions are also in the process of being updated and this exercise should be completed by end 2011. A review of the SoDI framework has commenced and a paper is scheduled to be presented to the DC in Feb 11.

Information Management Project

A CIOG initiative that covers a collection of projects including DRMS upgrade and rollout; WCMS; Information Governance; date warehousing; enterprise search facility and business intelligence. The scheduling of projects and their phasings are currently being discussed with a view to all initiatives being delivered over the next five to ten year period.