NATO Communications and Information Agency
Agence OTAN d’information et de communication

ITM White Paper No. 1
NATO’s First Step to the Cloud: Overview and Business Drivers

Effective date: 31 August 2014
Revision No: 1.0
Issued by: Peter J. Lenk
Approved by: Dag Wilhelmsen
EXECUTIVE SUMMARY

Shortly after the coming to office Secretary General Anders Fogh Rasmussen commenced a programme of reform for the NATO Alliance, encompassing not only the re-alignment of the NATO Command Structure (NCS) to allow it to better deal with the current global geo-political realities, but also a consolidation of the NATO Agencies, reducing these to a fewer number in order to achieve efficiency and effectiveness benefits.

The newly created NATO Communication and Information Agency (NCI Agency) proceeded immediately to determine the current state of NATO’s IT capabilities and to identify a path for modernization that would contribute to the benefits and savings that were expected by the Alliance nations. This study effort, supported by the Network Centric Operations Industry Consortium (NCOIC), identified significant gains that could be made and as a result an ambitious programme to modernise NATO’s IT capabilities has been commenced.

Historically, investments in NATO’s IT have been made through various capability packages (CPs), through individual projects or programmes, and were often targeted at individual customers, user communities or facilities. These investments have had a very high aggregate cost due to the distributed architecture that was created and the resulting “replicate everything - everywhere” stove-piped approach. Implementations were carried out with an emphasis on the needs and wishes of the local site, instead of a global view towards standardization and global efficiency. As these decentralized capabilities continued to be proliferated to the sites, the number and complexity of these systems demanded additional manpower of a high level of expertise in order to continue to keep them operational. This has had consequent effects on the cost of maintaining the capabilities during the in-service phase of the life-cycle. Nevertheless, these capabilities have played an integral part of NATO’s success during this time.

With the advent of NATO reform, there is an opportunity to do things better. NATO can no longer afford to continue to implement capability with the complexity and waste associated with this decentralized approach. In a time of reducing investment and operations budgets, traditional approaches must be abandoned and smarter decisions must be made regarding how nations’ limited resources are used to provide services to the NATO users. A network centric approach, where capability is available primarily from fewer locations, with centralized expertise and support and use of automation is key. Such an approach is in line with industry and government best practice and has shown to reduce manpower levels needed, reduce the overall capacity of the IT infrastructure required and enable higher and more measurable levels of service.

This strategy requires changes to the way capabilities are acquired and designed. This coherent, centralized approach will reduce the complexity of these future systems and provide a foundation on which all systems are to be built. However, in order to achieve this, a level of standardisation of hardware and software solutions, beyond the level of functional needs, will be required. Thus the approach demands a long term, global partnering relationship with suppliers in order that by the end of the journey a level of uniformity of the hardware and software can be realised across the enterprise.

The IT Modernization project will increase the efficiency and effectiveness of NATO’s Information Technology (IT) infrastructure by:

1. Renewing obsolete IT infrastructure with standard solutions, reducing the heterogeneity of hardware and software assets;
2. Quantifying and increasing the availability of service levels;
3. Implementing NATO-wide Business Continuity and Disaster Recovery capabilities.
4. Enhancing the Information Security posture;
5. Increasing operational agility and flexibility by enabling reallocation of resources dynamically, as dictated by the operational situation;
6. Bringing new ways of working by enabling a mobile work force; and
7. Reducing the manpower and operations and maintenance costs required to provide and maintain services.

IT Modernization (ITM) is a journey; it will take half a decade to fully implement. It represents a fundamental shift from provision of bespoke services to the user community, independently at each user location, to the provision of commodity services in an efficient and standardised way, from only a few locations.
This is NATO’s first step towards adoption of ‘Cloud Computing’ by providing private, on-premises infrastructure as a service (IaaS). However, it is only the first step. The NCI Agency is committed to bringing beneficial change not only at the infrastructure layer but to all levels of the stack. Other initiatives will bring standardised platform components to the solution, in order to facilitate modular application development and software reuse, as well as enabling tighter integration of functional capabilities. The end-user applications will also be commoditised and made available as a service.

We believe that there is little choice other than to proceed on a path as has been defined by the IT Modernization project. Costs of the sustainment of the services, using the current distributed and stove-piped model, will continue to rise. They are already becoming prohibitively expensive, and hard choices will have to be made as to which services to terminate and which to sustain if changes are not introduced. The manpower shortages that the NCI Agency has experienced and continues to experience, particularly on the military side, mean that soon the point will be reached where services cannot be sustained according to the current model. Standing still is not an option.

The ITM journey is not a journey the Agency will take on its own. It is a journey that we will be accompanied on with the user community, other NATO stakeholders and industry. I ask that you join in this journey as active participants to help steer its course to a successful conclusion for all.

//signed//

Koen Gijsbers
# TABLE OF CONTENTS

1 OVERVIEW .......................................................................................................................... 5
   1.1 BACKGROUND ................................................................................................................ 5
   1.2 OBJECTIVES .................................................................................................................... 5
   1.3 THE CURRENT SITUATION ............................................................................................. 5
   1.4 THE FUTURE: ITM ........................................................................................................... 7
   1.5 PHYSICAL SCOPE ........................................................................................................... 10
   1.6 TECHNICAL SCOPE ........................................................................................................ 10
   1.7 PROJECT IMPLEMENTATION ......................................................................................... 12
   1.8 INTERDEPENDENCIES .................................................................................................... 13
   1.9 THE APPLICATION SPACE ............................................................................................. 14
1.10 THE CHALLENGES AND RISKS .................................................................................... 14
      1.10.1 Migration .................................................................................................................. 15
      1.10.2 Single Pane of Glass ............................................................................................... 15
      1.10.3 Balancing Costs Across the Lifecycle .................................................................... 15
      1.10.4 Dealing With Change and Imperfect Information .................................................. 15
   1.11 IMPLEMENTATION APPROACH .................................................................................. 16
2 OPERATIONAL BENEFITS ..................................................................................................... 16
   2.1 USER BENEFITS – EFFECTIVENESS ............................................................................. 17
      2.1.1 Resilience, Disaster Recovery and Sustainability ..................................................... 17
      2.1.2 Information Exchange ............................................................................................. 17
      2.1.3 Facilitate the Shared Service Concept ...................................................................... 18
      2.1.4 Support of Comprehensive Approach ...................................................................... 18
      2.1.5 Flexibility and Agility .............................................................................................. 18
      2.1.6 Security Posture ...................................................................................................... 18
      2.1.7 Mobility .................................................................................................................... 18
      2.1.8 Conformance with Agreed NATO Policy ................................................................. 18
      2.1.9 Metrics & Benchmarking: Customer Funding ......................................................... 19
   2.2 EFFICIENCY BENEFITS ................................................................................................ 19
      2.2.1 User Benefits .......................................................................................................... 19
         2.2.1.1 Continuity of Operations .................................................................................... 19
         2.2.1.2 Mobility / Productivity ...................................................................................... 19
      2.2.2 Service Provider (NCI Agency) Benefits ................................................................. 19
         2.2.2.1 Fewer Networks to Support .............................................................................. 19
         2.2.2.2 Fewer User Accounts ....................................................................................... 19
         2.2.2.3 Manpower Savings ........................................................................................... 19
         2.2.2.4 Supportability ................................................................................................... 20
   2.3 FINANCIAL AND MANPOWER BENEFITS ................................................................... 20
3 NEXT STEPS – BEYOND IAAS ............................................................................................ 20
   3.1 PLATFORM AS A SERVICE (PAAS) ................................................................................ 20
   3.2 SOFTWARE AS A SERVICE (SaaS) ................................................................................ 21
   3.3 HYBRID AND PUBLIC CLOUD OFFERINGS .............................................................. 21
   3.4 ROADMAP ....................................................................................................................... 22
OVERVIEW

1.1 Background

With the creation of the NATO Communication and Information Agency (NCI Agency) the newly formed Agency inherited the IT asset holdings of NATO. One of the first initiatives launched by the Agency was to build an understanding of these assets, how they were used, what were the shortfalls and to develop a strategy for improving the infrastructure and the Agency’s ability to provide high quality, robust, standardised and cost effective IT services. This was done in conjunction with industry through the Network Centric Operations Industry Consortium (NCOIC). The study determined that the manpower levels enjoyed in the Agency far exceeded what might be expected to provide the IT services. It also made a number of recommendations regarding how the IT systems should be modernised in order to bring benefit to the NATO user community.

Based on the NCOIC recommendations, and working with the user community and other NATO stakeholders, the NCI Agency has defined a programme to modernise the NATO IT infrastructure. It is an ambitious programme that will see most of the IT assets replaced over a period of five years and will require significant manpower reorganisation. However, when completed will deliver a platform for more efficient, more effective and sustainable IT services for the user community.

1.2 Objectives

IT Modernization will transform the way in which IT services are provided in NATO. It will change the model from one where IT services are provided locally, using local resources, to one where resources are treated as global, pooled enterprise assets: it represents the first step of NATO’s journey to the cloud.

IT Modernization will increase the efficiency and effectiveness of NATO’s Information Technology by:

1. Renewing obsolete IT infrastructure and reducing the heterogeneity of hardware and software assets;
2. Quantifying and increasing the availability of service levels;
3. Implementing NATO-wide Business Continuity and Disaster Recovery capabilities.
4. Enhancing the Information Security posture;
5. Increasing operational agility and flexibility by enabling reallocation of resources as dictated by the operational situation;
6. Bringing new ways of working by enabling a mobile work force; and
7. Reducing the manpower and operations and maintenance costs required to provide and maintain services.

1.3 The Current Situation

The current IT infrastructure solution, as inherited by the NCI Agency, was implemented over many years, in a piecemeal fashion. Rather than being developed in accordance to any considered roadmap, overarching architecture or plan, it evolved, and was driven by local needs. The extant IT infrastructure has been procured at different times, from separate budgets, under separate contracts managed by a variety of different nations and NATO Agencies.

Three major funding mechanisms have been exploited to create the current situation: the Civil Budget responsible for the NATO HQ, the NATO Security Investment Programme (NSIP) providing capital for NATO Command Structure (NCS), and the Military Budget (BC) which has provided funds to maintain and in some cases replace equipment. In addition a variety of other funding mechanisms such as customer funding, Joint Funding, etc., have also contributed to the totality of IT systems deployed within NATO. This split in the funding models has led to a chasm in the coherence in the technical solutions, the management of the IT services, the definition of the service levels, etc.

Exacerbating the problem was the system approach adopted, where rather than looking at the problem holistically, each individual capability that was delivered was considered in isolation, and aspired to be as self-contained as possible in order to minimise implementation risk by reducing dependencies. Although steps have been taken in some communities to overcome this issue, today we have situations...
where we have a variety of technical solutions and technologies deployed even within single sites. As a result the infrastructure is locally focused, heterogeneous, difficult and costly to support and maintain, and offers little flexibility at an enterprise level.

This highly localized set of architectures leads to a highly redundant (but not necessarily highly resilient) service support situation where identical services are managed and supported in many locations using different hardware, different software, different processes and different people. The exact services being provided are not well understood, the levels to which the services are operated are ill defined and not measured, and the costs are not understood except at a very high level.

This heterogeneity also acts as a barrier to achieving a pooling of resources across the enterprise as it makes increased use of management automation difficult and prohibitively costly.

Figure 1 below captures the current situation.

![Figure 1: IT posture prior to IT Modernization](image)

As mentioned above, hardware is often dedicated to specific services and hence underutilized. An estimate of the server utilization conducted in August 2012 indicated that the average utilization was only around 9% across the enterprise; however, it was also concluded that the current architecture and implementation made it not feasible to exploit this excess capacity at an enterprise level.

Additionally the underlying hardware and software is ageing, leading to ever increasing costs of maintenance. The last major hardware updates conducted at some of the major NATO sites are indicted in Table 1. If one considers that the average lifetime of a server is around five years, then it becomes clear that much of the current infrastructure is obsolescent or obsolete. An estimate made in August 2012 was that by August 2014 65% of hardware in the enterprise would be beyond its normal supportable life and would begin to put an increasing pressure on the Operations and Maintenance (O&M) budgets.

<table>
<thead>
<tr>
<th>Command</th>
<th>Host Nation</th>
<th>NU Network</th>
<th>NS Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT</td>
<td>NC3A</td>
<td>Mar 2008</td>
<td>Sep 2006</td>
</tr>
<tr>
<td>MARCOM Northwood</td>
<td>NC3A</td>
<td>May 2009</td>
<td>Jul 2006</td>
</tr>
</tbody>
</table>
The prevailing local delivery model also means that Disaster Recovery (DR) capabilities are local in nature and scope. NATO sites do not currently support each other in disaster situations. Although backups are made, in the case of a major disaster at a site, such as a server room fire, it is not clear if and how long it would take to restore data and services. It is, however, fair to point out that some functional services cope with this at the application level, by replicating data across sites.

The current Information Security posture is also not optimal. Because of the variety of software installed, and differences in software versions, it is difficult to ensure that all the latest security patches are applied consistently.

1.4 The Future: ITM

IT Modernization will provide private cloud-based Infrastructure as a Service (IaaS) services to support all of NATO’s business needs. The single, resilient, logically integrated but geographically dispersed, infrastructure will host all of NATO’s applications, negating the need for individual projects to provide hardware to support their capabilities.

The architecture to be implemented is based on that proposed by NCOIC in 2012. The study concluded that NATO’s fixed IT infrastructure needed to be modernized and transformed into a single enterprise, customer-funded service delivery system, with a common management and operations surveillance layer, limited operating system / hardware combinations, increased levels of virtualization, modern cloud technology, and include appropriate disaster-recovery / survivability considerations. Only through an enterprise approach of this sort would the NCI Agency be able to respond reliably, flexibly and rapidly to NATO customers’ demands, charge for its services in a transparent and predictable way, and be able to benchmark its services against outside organizations. With such an infrastructure in place, NCIA should be able to routinely measure its cost-efficiency, using industry benchmarks, and
optimize its infrastructure and processes in order to continually find improvement in cost and quality of the services provided.

![Diagram of IT posture following IT Modernization](image)

The words that characterize the IT posture NATO will have following IT Modernization are “POOLED” or “SHARED”. Resources will be pooled and available to the users according to priority. Excess capacity can be deployed as needed to satisfy mission demands. Sustainability will be enhanced due to standardization of software, hardware, process and thus also training and logistics needs. Resilience will be provided ‘out of the box’, with data and services being available at multiple points in the network at all times.

Pooling is an essential concept of cloud computing. It is the main driver for the adoption of the cloud business model. In NATO today we have processing, storage, etc., capacities at each site that are scaled to the worst case requirement at each site, on a functional service by functional service basis. As a result, during the NCOIC study in 2012, it was estimated that only about 9% of the resources were being used, on average. However, because the resources were geographically distributed and of varying technologies and eras, it was not practicable to consider them as a pool that could be shared. The unused 90% of the capacity could not be exploited as an enterprise resource. If a site was out of capacity or even a particular functional service within a site was short of storage or other resource, it was usually not possible to leverage excess capacity elsewhere to satisfy the shortfall. Pooling allows the sizing of the infrastructure to be reduced overall, while at the same time being able to deploy capacity to the users dynamically, according to the operationally assigned priorities.

An important aspect to this pooling is the scale and diversity of the user community. The easiest way to understand this is perhaps with an analogy. A common approach businesses and government organisations are adopting to save on office space costs is to size the space based on an estimate of the number of people that can be expected to be working from the building at any one time. For example, as people travel, have leave to take, are sick, etc., it is reasonable to assume that they only have to size the facilities to cater to the maximum number of simultaneous users of the facility, rather than the total number of employees. However, the space provided has to be flexible and a commodity that anyone can use when they do come to the office. It is a move from specialised offices, where everyone has their own furniture and photos on the wall, to standard flexible and functional offices that can be used by anyone, and can be assigned based on who shows up in the morning. This is essentially what cloud computing allows.
computing is about – it is the commoditisation of computing resources, providing them in a standardised way, that can support any service.

In a similar way, at the user end, as we create internet cafes and NATO SECRET (NS) cafes, we are essentially saying that the maximum simultaneous number of users we will have on these networks is less than the total number of users. Although users normally only see the front end, client-facing devices, there is a knock-on effect on the back-end as well. This approach can lead to considerable savings. If we have data centres that are used across time zones, the peak loads on the systems when users come in at 08:30 in Europe and check their emails will not correspond to the peaks when people in Norfolk come in to check theirs, five or six hours later. So we can reduce the overall scale of the resources needed. The more users with varying needs, the better the model works. This is the reason that large scale cloud computing providers, like Amazon, or SalesForce.Com, or Google can provide services at such reasonable costs; it is that they expect that the infrastructure they need to buy and operate is only a percentage of the total that might be needed should all users act simultaneously.

Three views of the future infrastructure are illustrated in Figure 3. At the extreme left is the User View of the service. Users are not interested in how the services are provided, only that they meet their requirements, such as: resiliency, performance, cost, etc. For example, a pilot might want to come in in the morning and operate their workstation to see the weather forecast for the next 24 hours. The pilot does not need to concern themselves with all of the activities that go on behind the scenes to collect data, enter it into databases, process it, analyse it, store it and produce finished graphics of the forecast; they are only concerned with the finished product and that it satisfies their needs in terms of timeliness, accuracy, and so on. That is the user view of the service.

A single ‘pane of glass’ view will be presented to the system administrators. The administrators will be able to manage all the pooled resources in the cloud in a transparent way, not having to worry about locations, the specifics of the hardware brand, etc., and will thus be able to focus on provisioning the assets to meet current priorities and optimise the performance of the services. Assets not in use can be powered down in order to save on energy usage. The measurement tools needed to understand the current status of the infrastructure and tools needed to manage the infrastructure in order to be able to provide the services to the user at the agreed service levels constitutes the Administrator View.
Of course underlying these abstract views is the reality of the physical configuration of the hardware; that is, the **Physical View**. What is important is that neither the users, nor the Operations Centre administrators need to be concerned with the Physical View – they can conduct their roles maintaining only their views which are tailored to their needs and abstracted from physical reality in a way that makes it easier for them to conduct their work. Of course at some level, further back in the organisation the physical view is necessary in order to maintain inventories, replace obsolescence, or conduct physical repairs to equipment, planned maintenance, etc., but this is not a level of detail that users or first or even second line administrators need concern themselves with.

### 1.5 Physical Scope

The physical scope of IT Modernization is the NATO Enterprise, defined to include the NATO Command Structure (NCS), NATO HQ (NHQ) and NATO Agencies. It will address two security domains: the Operational Network (ON) providing services at up to the NS level, and the Protected Business Network (PBN) providing services at up to the NATO RESTRICTED (NR) level, including access to the internet. Internet access will be provided through the Public Internet Access (PIA) Gateway project, due to deliver in the 3rd quarter 2014.

### 1.6 Technical Scope

The technical scope includes the consolidation of IT infrastructure to three central Enterprise Data Centres (EDC), as well as deployment of distributed *standard or enhanced* nodes (SN or EN) to the local sites. The data centres will provide high levels of resilience, including automatic failover between geographic locations for the highest availability services. Disaster recovery capability will be centrally provided, with data being available in at least three locations at all times allowing for restoration of services in predictable timeframes and predictable limits on data loss. *Standard* nodes will provide only a minimum set of processing and storage services locally, while *enhanced* nodes will include some level of local processing and storage to provide additional levels of resiliency as well as to deal with a few legacy applications that are not yet ready for the new architecture. Existing and future applications will be centralized and consolidated across this redesigned infrastructure to provide the efficient and effective IT services which NATO needs.

The ITM solution has the following characteristics:

- a. It will deliver private, on-premises cloud-based Infrastructure as a Service (IaaS), capable of hosting any of NATO’s applications, in order to provide a service to the users;
- b. It will establish three Enterprise Data Centres (EDC’s) at Mons, Brussels, and Lago Patria;
- c. It will include local branch offices, or nodes, of two types: *standard nodes* offering very limited or no local provision of user facing services and *enhanced nodes* allowing for limited local provision of user facing services for additional resiliency or in order to deal with legacy;
d. A centralised Operations Centre (OpsCen) in Mons, with a back-up located elsewhere within the BENELUX (TBD), providing centralised management of all IT services including the management of the local nodes;

e. A workforce that will be adjusted to the new architecture, in both skills and location, with the local Customer Support Units (CSU) providing 1st line maintenance, the OpsCen providing 1st and elements of 2nd line, and the Service Lines providing 2nd and 3rd line support. The types of skills and levels of skills are envisaged to be significantly different than what is in existence today; and

f. A set of process, and the tools to support them, that will allow the efficient provision of IaaS to the enterprise.

Three nodes from the existing NATO network (SHAPE Mons, NATO HQ Brussels and JFC Naples HQ) will be renewed and upgraded to function as Enterprise Data Centres (EDCs) and will serve the entire NATO Enterprise. All data will be mirrored across the three data centres so that it is maintained in at least three locations at all times, one being a hardened facility. It will be possible to restore and run services from any EDC or enhanced node, and services can be moved seamlessly between these. The two EDCs at Mons and Brussels will also provide real-time mirroring of data and service state between them in order to have seamless geographic failover for the services with the highest availability needs.

To complement the creation of EDCs, equipment at all remaining nodes will be renewed within the scope of the project, creating either Standard or Enhanced nodes, which although distributed will function in the centrally managed service provision environment. A consistent baseline of hardware and software will be established across the entire Enterprise to facilitate the management and increase supportability. A move towards common funding of the common elements of the infrastructure, and the use of framework contracts will contribute to enhanced commonality and thus supportability. Client devices, peripherals and local network infrastructure will also be renewed as necessary.

It is envisioned that around 80% of all existing services will be centralised to the new EDCs by the end of the project. The remaining 20% of applications are considered unsuitable for centralization in their current form, or are close to the end of their life cycle, and will continue to be run and supported at the

**Definitions**

**Virtualisation** – the abstraction of the characteristics of a hardware element, via a software layer. Such an abstraction allows for more than one virtual instance of the hardware to be used simultaneously on the same physical hardware, allows the software running on the virtual hardware to be isolated from changes to the physical characteristics of the hardware and allows for the seamless movement of services across physical hardware instances. In the case of ITM we will deal mainly with the concept of server virtualisation where we create multiple virtual copies of the CPU, memory, IO and other elements such that each application running on the single physical device is isolated from other applications, and each is presented with the illusion that it has its own physical server available for its sole use.

**Service Migration** – the process of relocating services from one hosting infrastructure to another hosting infrastructure. In the case of ITM this will be the relocation of the hosting of the services from the old infrastructure to the new ITM provided infrastructure.

**Centralisation** – A particular type of service migration, involving the movement of the service hosting and responsibility for the management of the service from a remote location to a central Data Centre.

**Data Centre Consolidation** – the reduction of the number of locations from which services are hosted.

**Service Consolidation** – the reduction of the number of separate instances of the same service that are being run in parallel. For example, rather than running three instances of a functional service, each supporting a user community at a different geographical location, through consolidation of the service all locations could be served from a single instance of the service running in a single location.
local level for the time being. As the applications undergo future upgrades or replacement they will be mandated to run in a centralised mode. The goal is to reach 100% centralisation as quickly as possible.

Initially, and within the scope of this project, all core services will be consolidated into a single version serving all users. In those cases where centralisation is possible but not service consolidation, services will be centralised to the new EDCs, but multiple instances may remain for some transition period of time, until the functional service teams responsible for the applications have affected the application changes needed.

The project will also renew the client devices, providing mobile solutions for the PBN and new devices on the ON, for common-funded users. It will also renew the local area infrastructure at NCS sites and provide widely accessible wireless access to PBN services.

In concert with these hardware and software changes the embryonic Operations Centres that are being currently established under the internal NCI Agency transition activities at SHAPE HQ, with a backup facility at a location in the BENELUX area, will be upgraded. Only first level support functions will remain at the local sites; second and third level support plus all management functions will be centralized. The new Operations Centres will need tools and training (to be provided under the IT Modernization project) in order to take on the complete scope of their new role.

1.7 Project Implementation

The execution of this project will be undertaken in an incremental fashion in four stages referred to as Waves. The first Wave, which will establish two of the EDC’s, the Operations Centre and alternate, and upgrade those nodes most in need of hardware renewal. It is anticipated that the Invitation for Bid (IFB) for the main work will be released before the end of the fourth quarter 2014. It will then take c. 12-16 months to achieve contract award, hence implementation in earnest can only begin in early 2016. Allowing for a six month start-up and design phase, the first two EDCs will be established early 2017. The work will then turn to the renewal of nodes where equipment is oldest, identified to be Norfolk, MARCOM, LANDCOM and to implement the new site at Sigonella that will host the main operating base (MOB) for the Alliance Ground Surveillance fleet. Following that, the subsequent Waves will be 12 months in duration and will incrementally migrate additional sites into the nascent NATO cloud. The third EDC will be added in Wave 3, following hand over and full occupation of the new NATO HQ building in late 2016.

This implementation plan is illustrated in Figure 4, below.
1.8 Interdependencies

The IT Modernization project does not stand alone; a number of other NATO projects in the pipeline are critical enablers of ITM. Still other projects will contribute or be affected by ITM.

The NCI Agency has established, under the Director of Infrastructure Services (DIS), an implementation office for Infrastructure Services that is overseeing the programmatic coherence across all the different lines of development. These all form part of the larger ITM programme and vision.

It is best to consider this mosaic from a service stack point of view, according to the NATO C3 Taxonomy. This is illustrated in Figure 5. In Figure 5, the following projects are identified:

- ITM = IT Modernization
- ANWI = New NATO HQ Active Network Infrastructure
- NIP = NATO Information Portal
- UCC = Universal Communication and Collaboration
- NCI = NATO Communication Infrastructure
- VOSIP = Voice Over Secure IP
- LTX = Communications Bandwidth provision
- PIA Gateway = Public Internet Access Gateway
- Studio VTC = Studio Video Teleconferencing
- NCIRC = NATO Cyber Incident Response Centre
- NPKI = NATO Public Key Infrastructure
- COI = Community of Interest
As part of the preparation for the implementation of IT Modernization, considerable effort has been expended in order to understand the applications that are running on the NATO networks, and conduct a detailed data gathering exercise. The data gathering has addressed two aspects: gathering of exact information regarding what applications are installed on the network and where, and a profiling of the applications so that their requirements and baseline behaviours are well understood.

The base-lining effort has resulted in the cataloguing of some 550 ‘significant applications’. Analysis of these is indicating that there are perhaps 400 that can be eliminated from the inventory as either there are newer versions of the same applications already installed elsewhere on the networks, or there are alternative applications providing similar functionality available and it is not considered cost effective to support several applications which provide equivalent features.

Of the remaining 150 applications, perhaps 40 are NATO-specific bespoke applications that support NATO operational military processes. Detailed and realistic profiling of these applications has been conducted in order to understand the requirements of these applications in terms of processing, storage and bandwidth. As most of these have been designed to operate in the old architecture, where client and servers are all located on the same local area network (LAN), testing was conducted in a simulated target architecture, including realistic representations of the latencies introduced by the wide area network (WAN) and cryptographic equipment, to understand options for centralising these applications. This information will be essential in order for industrial bidders competing for the work to be able to understand the scope of the effort.

Bringing the applications under control, reducing the number of applications, and converging to a common baseline of applications will save considerable effort during the migration stage of IT Modernization. It is also predicted to save considerable operational costs in terms of licence costs and manpower support costs. This is an essential enabler to ITM.

1.10 The Challenges and Risks

As part of the project, a detailed risk management plan is under development that will quantify the risks to the project. This will take into account both the risks at the individual work package level, that is, the risks that affect the work packages delivering their outputs, as well as the risks that the overall ITM
project will deliver the benefits and savings that have been articulated. Management of these risks throughout the project lifetime is seen as one of the critical activities of the ITM project team.

The four main challenges that have been identified for industry to solve are:

1.10.1 Migration

IT Modernization will be implemented in Waves, in an incremental fashion, as described earlier. As each site is implemented, it will be necessary to migrate all of the existing applications and data to the new infrastructure without interrupting the users’ ability to conduct their work. This has been compared to changing the engines on an aircraft while the aircraft is in flight. The solution will entail a rigorous methodology being applied in an uncompromising way, and detailed planning and rehearsals to that all aspects are understood and accounted for before touching the live systems. The scale of the migration is large, involving some 44 sites across the four Waves, each with some unique needs and constraints. This is seen as a major challenge and will be a key differentiator that will be assessed when scoring industries’ bids for the work.

1.10.2 Single Pane of Glass

Many of the benefits and savings predicted stem from the ability to centralise the management of the infrastructure and from the centralisation of the applications. The efficiencies lie in the fact that similar functions will only be carried out once, from a single location, rather than replicated everywhere across the networks. This means that the people conducting the tasks in the future from the centralised location need a robust and capable ability to monitor the assets and services across the enterprise, and to manage them in a seamless way, regardless of the geographic location or underlying technological differences. The completeness of the toolset provided, and the level of automation implemented, will dictate the numbers of people needed in the central location, as well as the skill levels required to conduct first, second and elements of third line maintenance.

Although the intention and strategy of ITM is to minimise the heterogeneity of the technological solutions provided, given the five-year implementation timelines set out, there will be evolution in the technology and solutions implemented in Wave 1 are likely to be somewhat different than what is implemented in Wave 4. Therefore the service management and control (SMC) solutions will have to evolve with the evolution of the technology while at the same time minimising the change seen by the administrators that are ensuring the systems continue to operate and provide the services needed by the users. The SMC cannot be seen as a point solution, delivered once at a certain time in the project, but must continue to evolve, adapting in lock-step with the deployment and evolution of the ITM project as a whole.

1.10.3 Balancing Costs Across the Lifecycle

NATO is expecting significant efficiencies to be brought through the implementation of ITM. Most, but not all of these stem from reductions in the manpower levels that will occur at the local sites. Another way of viewing this is that ITM must enable NATO to deal with the manpower reductions that will occur as nations reduce the manning levels they are willing to support in the Agency, while users still expect the same or higher levels of service. This is a major ask.

So the costs need to be balanced across the CAPEX and OPEX portions of the life-cycle. It is no good to minimise CAPEX costs if the investments being made do not enable the ability to operate the services with the reduced levels of manpower that is expected in the future. Industry will be asked to find the right balance across the life-cycle so that the totality of CAPEX and OPEX costs are minimised, even though NATO is not asking industry to participate in all of the service operations activities. A bidder that minimised CAPEX costs but does not consider how their proposed solution will positively affect the manpower and other life-cycle cost factors, will not be assessed very highly during the bid evaluation phase of the project and should not expect to be awarded any work.

1.10.4 Dealing With Change and Imperfect Information

One of the realities that exist in NATO is the constant change. This manifests itself in many ways. NATO has chosen to reorganise the NATO Command Structure, reducing the number of headquarters and the
locations and functions of some of them. This is unlikely to be the final word and it can be expected that in the future additional changes will occur or at least refinements will be implemented.

NATO’s IT systems will not stand still over the time period planned for ITM. Additional systems currently in the pipeline will deliver and will need to be accommodated within ITM, even though today not all the details of what and when things will be delivered are not fully understood. Timelines in NATO are always difficult to predict accurately. Local changes will occur as equipment needs to be updated due to obsolescence or failure. Operational missions often call for rapid and unpredicted change to occur in order to respond to evolving situations.

The project team and the industrial partner selected for ITM will need to be able to deal with the constantly changing set of realities and demonstrate the agility needed to adapt, without impacting the overall costs of ITM or the ITM timelines themselves. Flexibility, pragmatism and experience will all play a role in the success of achieving the ambitions of the ITM project. There will be many ‘unknown unknowns’ over the course of the five years of ITM.

### 1.11 Implementation Approach

NATO will issue five main contracts that will address different aspects of the Implementation of IT Modernization across the entire project (all four waves). The five contracts will have the following scopes:

- **Contract No 1:** Establishment of Data Centres, renewal of local nodes including local area networks (LANs), set up of Management Centres including training and tools, implementation of client service provisioning, integration, consolidation, centralization and transition.
- **Contract No 2:** Renewal of client devices.
- **Contract No 3:** Provision of Consultancy Support to NCI Agency.
- **Contract No 4:** Upgrade of the ANWI data centre to the IT Modernization scope.
- **Contract No 5:** Adaptation of the NCIRC capability in order to deal with the new modernised IT infrastructure.

Industry partners will be selected for Contracts No.s 1, 2 and 3 using NATO International Competitive Bidding (ICB) procedures. For Contracts No 1 and No 2, bids will be evaluated against the entire project scope but initial contract award will only cover Wave 1. Subsequent waves will be the subject of costed options awarded annually following authorization by the NATO Investment Committee, and demonstration of successful progress.

In order to deliver a coherent IT infrastructure, the intent is that all hardware purchases for front or back end equipment would be procured through contracts No’s 1 or 2, from the moment the contracts are issued, until following Wave 4. This means that if a Functional Service (FS) application needs hardware it should not be looking to buying its own; rather it should be asking the ITM project to provision capacity. If this necessitates a procurement, this is the business of the ITM project, not the FS project. This is a critical aspect of the overall strategy and the only way that coherence can be achieved and maintained.

A separate 4th contract will be placed for works to be carried out in the New NATO HQ in Brussels in order to upgrade the datacentre to be delivered under the ANWI project from a local DC to an EDC.

A 5th contractor will be needed in order to adapt the NATO Cyber Defence Incident Response Centre (NCIRC) capability to the reality of the new IT architecture following modernization.

### 2 OPERATIONAL BENEFITS

ITM is not primarily about savings; it is far more about bringing benefit to the user community by enabling the delivery of enhanced operational services, enhanced in a number of key ways.

Two significant factors regarding NATO IT service provision need to be recognised. First, the IT equipment NATO has in-service today is getting old. It has to be replaced. Doing nothing is not an option. Serendipitously, money has already been foreseen for the replacement of the IT equipment across large segments of NATO. So, ITM is not necessitating ‘new money’; rather, it is utilising money
that was already programmed to be spent to replace aging equipment and spending it in a smarter way to achieve a range of benefits.

Second, it should be recognised that the skilled military manpower on which NATO relies to operate the IT systems in NATO, in order to provide services to users, is a scarce resource. The levels of manpower the current situation demands is unsustainable. Nations have reduced and are expecting to be able to continue to reduce the numbers of their military staff that they dedicate to support NATO IT services. Again, doing nothing is not an option. NATO needs to change the way services are provided in order to deal with this reduction of military staff. ITM is a key enabler in order to achieve this.

The benefits ITM will bring can be grouped into several categories: those that contribute to the effectiveness of the organisation, and those that contribute to the efficiency. In the case of efficiency, this can be further broken down into the efficiencies that are brought to the user community, which are difficult to measure in purely financial terms, and those that it brings to the service provision organisation, that is, the NCI Agency.

2.1 User Benefits – Effectiveness

Specific benefits that the operational user should expect of the proposed implementation include:

2.1.1 Resilience, Disaster Recovery and Sustainability

There is a perception today that the levels of resilience provided are quite high because of the local nature of the hardware and data; however, the truth is likely different. Loss of a data centre can well mean the loss of an element’s ability to operate for some time or the inability of the Organisation to conduct its mission.

Currently Disaster Recovery (DR) is locally provided with no enterprise view and in many cases unclear requirements and unknown achieved levels. Although all locations have provision for back-up today, it is handled locally. It is not clear that in all cases in the event of a major disaster that services could be restored in a reasonable time frame. Besides disaster recovery, there is today limited capability to provide continuity of services critical to the business, in an uninterrupted manner.

ITM will enable these capabilities in an enterprise way. Three copies of data will be available at all times, so complete data loss in the event of even multiple disasters will be prevented. For critical services, data will be mirrored in real-time so that automatic geographic failover will ensure continuity of these services. These are capabilities that do not exist today. The architecture will support a variety of BC and DR levels, according to agreed targets.

Sustainability will also be enhanced. The current architecture is what is best described as ‘accidental’. It is the result of a replacement approach that relies on periodic block replacements of obsolescent equipment, with the purchasing conducted under the leadership of many organisations and through many different projects. The delays in obtaining funding and the fracturing of the activities into many locally controlled projects has had significant negative impacts on the infrastructure: much of the equipment exceeds end of life before the next round of replacement occurs, and the numbers, makes and models of equipment across sites, and even within single sites are large. As a result some locations are running on equipment that was installed in 2006. Some locations are operating two and three different makes of storage area network and many types and brands of servers. This presents a constant challenge from a logistics, training and management point of view. By reducing the numbers and types of components, both hardware and software, in accordance with the proposed architecture, the capability will be more sustainable. By adopting a strategy that sees replacement of equipment on a defined, periodic basis, the big bang obsolescence will be avoided.

2.1.2 Information Exchange

The PBN is a key enabler of information exchange. By creating a single network from all of the disparate NU and NR domains extant in NATO, the ability to seamlessly exchange information at up to the NR classification would be greatly facilitated. The PBN will also be connected with the NATO SECRET network, for a one way exchange of information to the higher classification, facilitating bringing information from the internet to the NS and in general facilitating sharing of information with C2
systems. Notification on the low-side of high-side mail having been received will also be implemented, to facilitate quick response to urgent high-side issues.

2.1.3 Facilitate the Shared Service Concept

The instantiation of the PBN will create a single business domain, with all users able to share information across the domain. This will facilitate the shared services concept. As it is today, the shared service concept will be hampered by the barriers created across the enterprise due to the different organisations using different business domains to conduct their administrative work.

2.1.4 Support of Comprehensive Approach

Engagement with partners, civil authorities, NGO’s will always be problematic from the NS domain. The ability to conduct some operational processes at the lower classification level, which allows access to the Internet and would facilitate this broader engagement, in line with the vision of the Strategic Concept.

2.1.5 Flexibility and Agility

Today, as each of the locations is locally managed and operates autonomously, there is excess capacity in some locations and a shortage in others. These imbalances cannot be corrected in real time, as it would involve the physical movement of equipment between sites. Today, a commander at a location has at his disposal only the CIS assets that he currently has in his facilities. This issue is exacerbated as the current implementation relies on many applications running on their own dedicated hardware. By virtualising the processing, storage and network elements, these IT resources can be flexibly managed and reallocated to satisfy the various needs. ITM will facilitate the pooling of resources, such that capacity allocation can be made in real-time, based on current operational priorities no matter their location.

2.1.6 Security Posture

The achievement and maintenance of high levels of information security is challenging today. The numbers of different software with different patch levels makes it hard to ensure all are secure. Having over 30 locations with major data holdings, also makes it difficult and costly to ensure all are equally well protected. ITM will reduce the attack surface, ensure a higher level of standardisation, and thus facilitate higher levels of cyber security.

Today, as many administrative processes are carried out on the NS network, people need to have access to NS, even though their role would otherwise not necessitate such access. This violates the ‘need to know’ principle.

By reducing the number of principle sites and centralising the management, limiting access to critical administrative interfaces, the posture for IA/CD will be enhanced.

2.1.7 Mobility

ITM will bring with it increased possibilities for mobility and newer ways of working. If a headquarters is ‘shut down’ due to weather or other cause, work can still continue as users will have remote access to data up to NR. While on travel, data and services will be accessible from anywhere potentially increasing the efficiency of the staff utilization.

The ability to access data and services from locations other than a fixed office is now the norm in the civilian world. With the PBN this will be enabled, allowing work to continue while on travel, when at home, and when facilities are inaccessible due to inclement weather or natural disaster. Mobility allows for flexible working, provides an added degree of resilience, and can increase productivity. Having a single mobility solution will also bring benefits in terms of seamless access from around the enterprise, and outside of the enterprise, with a single service desk to contact to resolve issues.

2.1.8 Conformance with Agreed NATO Policy

‘The NATO Policy For the Rationalisation of Information Infrastructures based on Their Classification Levels’, dated 18 July 2008, articulates the policy that NATO shall operate two networks, one allowing the processing and storage of data at up to the NS level, and the other at up to the NR level. Establishment of the PBN will create the second of these two information domains.
2.1.9 **Metrics & Benchmarking: Customer Funding**

Currently no, or at least very few, metrics exist that measure to what quality and at what cost services are provided. By achieving a consolidated infrastructure that enables centralised provision of highly standardised services, it will be possible to measure both the quality of the services the NCI Agency provides, as well as capturing their complete cost. These are key enablers for a transparent customer funding model.

2.2 **Efficiency Benefits**

2.2.1 **User Benefits**

2.2.1.1 **Continuity of Operations**

Currently most services on the NU and in many cases on the NR networks are provided locally. If the local site goes down then services are interrupted. The PBN concept will decouple the location of the user from the point of service provision, allowing for continuity of operations across data centres, and improved resiliency. This in turn can increase user efficiency as it decreases the probability that the user will experience service interruption.

2.2.1.2 **Mobility / Productivity**

Mobility enhances productivity. The ability to access data and services while on the move, means that users can continue to work even when out of the office. It is difficult to quantify the savings, but if one conservatively assumes one extra work day per year is gained by travelling personnel in airports, on trains, etc., then it could be expected that about 15,000 man days could be gained. It may also be possible to reduce office space to take account of the fact that on any given day not all staff members are present (but continue to be productive).

2.2.2 **Service Provider (NCI Agency) Benefits**

2.2.2.1 **Fewer Networks to Support**

From a service provision point of view, fewer networks means that fewer systems need to be supported, fewer management solutions need to be implemented and maintained, and fewer application instances need to be supported. This can lead to significant savings overall as common solutions can be implemented; standardisation can be increased, thus reducing the total number of applications to be supported. The cost savings that this brings are difficult to quantify at this time, but estimates are reflected in the NCI Agency savings and benefits plan.

2.2.2.2 **Fewer User Accounts**

The cost of the provision of IT services scales as the number of user accounts: more accounts, more storage, processing, bandwidth, etc. So a key factor to achieving savings is a reduction in the total number of user accounts. Currently many users have accounts on the NS, but only because they need to access administrative processes that only exist in this domain. Many of these people already have accounts on one of the lower classification networks that will be merged to create the PBN. If the high side accounts can be closed, then savings should result.

2.2.2.3 **Manpower Savings**

The NCI Agency is facing significant manpower shortages as military billets are not being filled at the required level. This trend is expected to continue and in fact get worse over time. There will come a point where if we do not implement ITM it will no longer be possible to provide CIS services at their current levels. ITM is not being implemented to drive savings; it is being implemented to deal with this reality. We have to change how we provide services or face increasing costs to hire more civilian or consultant staff or reduce services or service levels. There is no choice.

The overall manpower savings that are predicted from IT Modernization amount to 515 people, 385 of which are military posts. This has not been broken down across the two networks, as many of the final positions will be common across both. However, as a rough guide, most of the savings on the NS will be a result of centralisation of capabilities. For the PBN this is also true; however, there is the added benefit of reducing the number of networks supported. So as both networks support roughly the same number of users (today), the overall savings attributable to the creation of the PBN might be considered to be in excess of half the identified posts.
2.2.2.4 Supportability
Creation of the PBN by merging many NU and NR networks into a single network will bring with it the possibility to standardise on software versions and choices in general, thus allowing fewer different licences to be bought. It will also reduce the overall hardware footprint and variation, again reducing the support costs, the supplier support relationships that must be maintained and managed, and the training that must be given to the system administrators.

2.3 Financial and Manpower Benefits
As well as achieving these business and performance benefits, the recommended approach has been determined to be able to deliver substantial savings, as described in the Agency’s Benefits and Savings Plan, 23 October 2013. It is estimated that it will lead to a savings of 515 posts, of which 120 are NATO International Civilian posts, and 385 are military posts. The savings come primarily at the edge of the network, that is, at the local CIS Support Units, where centralisation of service provision means that their role becomes primarily first line maintenance. Specifically, the manpower savings are predicted as shown in Table 2:

<table>
<thead>
<tr>
<th>Organisational Element</th>
<th>Savings (Total Posts)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Civilian</td>
</tr>
<tr>
<td>HQ Functions and Enabling Functions</td>
<td>0</td>
</tr>
<tr>
<td>Service Lines</td>
<td>59</td>
</tr>
<tr>
<td>CIS Service Support Centre</td>
<td>0</td>
</tr>
<tr>
<td>Operations Centre</td>
<td>0</td>
</tr>
<tr>
<td>CIS Support Units</td>
<td>61</td>
</tr>
<tr>
<td>Totals</td>
<td>120</td>
</tr>
</tbody>
</table>

Table 2: Predicted manpower savings as a result of the implementation of IT Modernization

In addition to the manpower savings predicted, there are also predicted direct savings in terms of hardware and software costs. Together the manpower and O&M savings amount to 24.5 M EUR per year in steady state.

3 NEXT STEPS – BEYOND IAAS
In this section is provided a vision of where and how the NCI Agency intends to take the next steps to the cloud, beyond IaaS. While IT Modernization is on firm footing having passed a number of critical hurdles in terms of fund and scope authorisation, the other aspects of the cloud, Platform and Software as a Service (PaaS and SaaS) are at a slightly earlier stage.

This section also explores the concepts of hybrid cloud and public clouds and how these might apply and be leveraged by NATO.

3.1 Platform as a Service (PaaS)
In parallel to the implementation of IT Modernization, NATO is embarking on the development of a Service Oriented Architecture (SOA) layer, in order to standardise and provide as a central service the core platform services that all applications require. This will be implemented as a series of projects, in some cases building on what is already available today in NATO. The SOA layer will provide the following services:

- Mediation
- Orchestration and choreography
- Message oriented middleware
- Information access
ITM: NATO’s First Step to the Cloud

- Information aggregation
- Information annotation
- Information discovery
- Metadata repository
- Registry
- Web hosting
- Policy decision point
- Security token services
- Policy enforcement point
- Identity Management
- Policy administration point
- Core data management capabilities
- Geographic
- Portal
- Unified Communication and Collaboration (UCC)
- Document management

There is today not a common understanding of what constitutes PaaS across the community. What NATO is implementing falls short of some concepts that also include the development environment and features such as big data analytics, and so on. What NATO is creating should be seen as the first step towards a more complete platform. Nevertheless, it is sufficient to allow the abstraction of the essential Community of Interest (COI) business process away from the underlying platform logic, and provide this logic only once, in a standardised way. This will open the possibilities to savings in future application development and life-cycle costs, as well as facilitate tighter integration of capabilities, information sharing and software and information reuse.

3.2 **Software as a Service (SaaS)**

Software as a service will partially be implemented under ITM, and partially through other means. Under ITM, NATO expects that most software will be centralised to run from the EDCs. Facilities will need to be provided for automated and self-service application provisioning. With ITM, NATO will adopt an ‘app store’ approach, allowing users to access the applications they require to do their jobs, based on their user roles and appropriate credentials. Application virtualisation technologies are seen as an essential contributor to the solution, at least for an interim period, until such time that all applications have been redesigned and rebuilt to operate in a centralised cloud mode. Over time, applications will evolve to be ‘cloud-ready’ and client access will be based predominantly on technologies such as HTML 5, that allow for a rich user experience from a browser interface. NATO is some years away from achieving this ambition, and it is not within the scope of the IT Modernization project to transform all of the applications and make them cloud-ready. Nevertheless, with the deployment ITM, users will experience rich software services with many of the characteristics of SaaS.

3.3 **Hybrid and Public Cloud offerings**

Public cloud offerings will continue to be difficult to leverage for any services that deal with information above the NATO UNCLASSIFIED (NU) level because of security concerns. This will hamper NATO’s ability to take full advantage of some of the benefits that these service offerings promise. Nevertheless, NATO will continue to follow the evolution of these services and it is reasonable to expect that progress will be made at the PBN level in the coming 3-8 years.

At the NATO UNCLASSIFIED level some public cloud offerings are already being leveraged in several areas, most notably, HR and web hosting. This is expected to grow in the coming years to take advantage of the savings and the rich functionality offered.

Similarly, a hybrid cloud, which includes one or more public clouds, is unlikely to gain much traction except at the NU level in the near to mid-term. Where the concept of the hybrid cloud has the biggest potential impact in NATO is at the classified level, in deployed or multinational situations, where all members of the hybrid cloud are providing and consuming services at the same security level.
In Afghanistan NATO hosted many services that were used across the coalition. NATO as an alliance made the common investment to make these services available, which then meant that not all services would need to be brought independently by each coalition partner. In the future this concept can be built upon where NATO could act as a cloud broker, brokering services between the entities offering services, be they NATO, a NATO nation, a non-NATO coalition partner nation or a supporting industry, and the consumers, according to priorities. The role of the cloud broker needs to be further developed and understood in this context in NATO and the ability and appropriate standards needed in order to federate clouds need to be agreed. Nevertheless, this concept appears to offer a significant positive impact for any future operations NATO may decide to support. This concept is illustrated in Figure 5.

![Figure 5: The NCI as a cloud broker in a coalition hybrid cloud](image)

### 3.4 Roadmap

An overall conceptual roadmap for NATO’s journey to a full set of cloud services is illustrated in Figure 6. In order to achieve the IaaS and PaaS capabilities, NATO will commit in excess of €300M. The total cost of SaaS implementation, moving Functional Services (FSs) to the self-service cloud, is not as well defined as it will be implemented incrementally, as parts of other programmes. IT Modernization will enable many of these, largely via application virtualisation; however, these will continue to evolve and be transformed according to other road maps, incrementally over time. IT Modernization is not an event but rather a trip that is part of a larger journey to the cloud that will transform how IT services are provided to the NATO user community.
Figure 6: NATO’s roadmap to the cloud