ISS4PS

Information Systems Strategy for the Police Service

Volume 2

Implementing ISS4PS

Safeguarding the Citizen in The Age of Information

Home Office
BUILDING A SAFE, JUST AND TOLERANT SOCIETY

ACPO

Association of Police Authorities

PITO
SYSTEMS FOR POLICING

Foreword

Version 3 of The Information Systems Strategy for the Police Service
Volume 2 Implementing ISS4PS and Annexes.

Volume 1 of the Information Systems Strategy for the Police Service (ISS4PS) version 3 defines the vision and policies for ICT within the Police Service, while Volume 2 defines a target technical architecture and a practical approach to achieve the ISS4PS vision.

ICT Architecture is the technical foundation of an effective ICT strategy. Volume 2 version 3 contains technical detail describing the architecture and is supplemented by expansive annexes.

This version is for those readers who want to understand the key architectural messages at the highest level and those who need to understand the lower level technical direction and practicalities involved. The target audience is key stakeholders from the Home Office, Association of Chief Police Officers (ACPO), Association of Police Authorities (APA), the Forces, and Criminal Justice Information Technology (CJIT).

The central theme throughout the strategy is that the Police Service will develop more commonality, become more joined-up and work more corporately. A collaborative commitment is required to achieve the goals outlined in the strategy and produce tangible benefits throughout the Police Service.

Becoming joined-up is a start.
Remaining joined-up is progress.
Working together is success.

Contents

Page

Figures

Tables

Section 1 Introduction

1.1 Scope

The Information Systems Strategy for the Police Service (ISS4PS) version 3 is the overarching strategy for IS/ICT in policing. The context for Volume 2 is the legislative changes and government initiatives driving the Police Service to a more joined-up approach[2]. The ISS4PS is designed to assist in meeting many of the goals of government imperatives, such as, the National Policing Plan, the Police Science and Technology Strategy and the Bichard Inquiry.

The adopted approach to meeting the demands of these imperatives is to enable the Police Service to view itself as an enterprise operating at a national level. The ISS4PS is designed to achieve this and is based on much of the work already in progress within the Police Service.

The Strategy is constrained by both government policies and practicalities. It follows the e-GIF standards and principles, recognises the diversity of IS/ICT within the Police Service, and is cognisant of Criminal Justice System (CJS) technical architectures.

Volume 2 is based around the 14 ISS4PS policies outlined in Volume 1. Figure 1 summarises the policies of the ISS4PS.

Establishing the Foundations	Delivering Joined-up Services	Focusing on People	Making it Happen
1 Defining Governance 2 Securing Alignment across Forces 3 Making National Programmes Accountable 4 Creating an Assurance Function	5 Delivering National Initiatives 6 Engaging with Industry 7 Sharing Information and Services 8 Managing Information	9 Empowering Police Officers and Staff 10 Deploying Common Services to Citizens	11 Shaping the Future of Police ICT 12 Adopting a Common Architecture 13 Deploying Corporate Solutions 14 Coordinating Service Management

Figure 1 The 14 policies of the ISS4PS

Volume 2 is a practical guide aimed at police ICT Directors, their staff, central ICT coordinators, service providers, and suppliers of existing and future solutions. Volume 2 can be read in isolation; however it is recommended that Volume 1 is read in order to understand the rationale behind the ISS4PS policies.

The ISS4PS focuses on technology, data and application architecture. The business view is recognised as an important enabler for the ISS4PS but has less emphasis in Volume 2. The ISS4PS considers the business view to consist of business models, business processes, and a business architecture. There are a number of initiatives currently being progressed to define these artefacts, which are in different stages of their life cycle. A baseline of the business view needs to be agreed in the early stages of the ISS4PS implementation. This business view will be enhanced and further developed by a team with focus on the business and technology as the ISS4PS evolves during the lifetime of the implementation programme.

The key theme that runs throughout the ISS4PS is that the Police Service will develop more commonality and become more joined-up in its approach to IS/ICT services. This improved commonality and more joined-up approach will be reflected in national and local initiatives that develop and deliver the technical architecture for both infrastructure and applications to meet the overall National Policing Plan.

The Police Service is not the only body that is moving towards a unified approach to delivering IS/ICT solutions. Both the Public Sector and many commercial organisations have similar issues with legacy systems and have made considerable progress in overcoming them. It is to industry best practice that the Police Service must now look to unify its IS/ICT services, and it is industry best practice on which Volume 2 is based.

2 The legislative changes and government initiatives driving the Police Service are detailed in Volume 1.

1.2 Structure of Volume 2

Volume 2 is structured as follows:

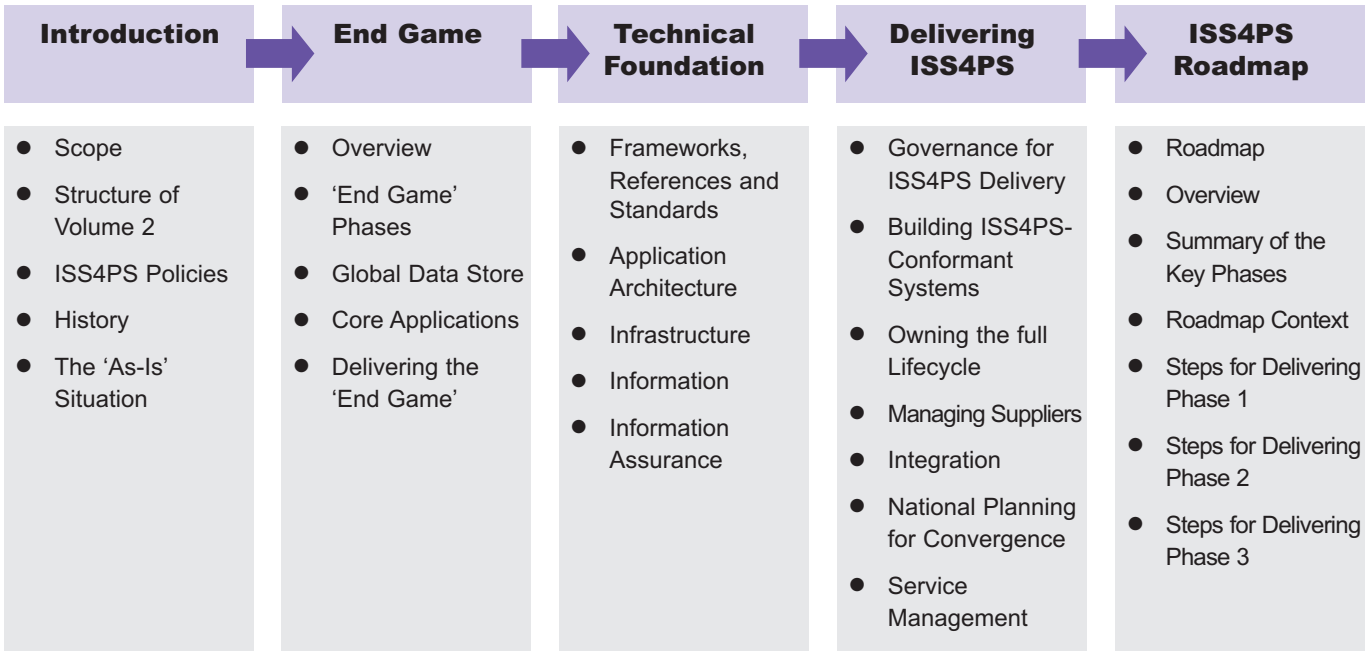

Figure 2 Volume 2 Document Structure

Section 1 – **Introduction** defines the scope of Volume 2, the constraints and context in which it sits, demonstrates how it achieves the policies defined in Volume 1, and provides a short summary of the background history.

Section 2 **The End-Game** describes the objectives of the technical architecture and a phased delivery approach. The architecture will be achieved in a series of stages described in the roadmap.

Section 3 **ISS4PS Technical Foundation** is focussed on applying ISS4PS standards within the Police Service.

Section 4 **Delivering ISS4PS** details how the 'End Game' will be delivered in a coordinated and controlled manner.

Section 5 **ISS4PS Roadmap** defines the ISS4PS steps over the coming years.

To support the main body of text in Volume 2 the following annexes have been included:

Annex A **Standards** provides a list of industry, government and police standards that are applicable to police IS/ICT.

Annex B **Actions and Guidance for IT Directors** is a set of actions and guidance for IT Directors and their staff for delivering Phase 1 of ISS4PS.

Annex C **ISS4PS Compliance** details the compliancy criteria for ISS4PS.

Annex D **Guidelines for National Programmes** provides a guideline for managing the enterprise portfolio[3] with a specific focus on how the enterprise architecture will be governed.

Annex E **Guidelines for Corporate Solutions** defines the criteria that provide guidance to Forces on whether they should adopt corporate solutions (referred to in policy 13).

Annex F **Principles and Actions** is a table containing all the principles and actions set out in Volume 2.

3 See Glossary for a definition of Enterprise Portfolio.

1.3 ISS4PS Policies

The 14 policies defined in Volume 1 (section 1.1) set out the necessary steps required to enable the successful delivery of the ISS4PS. Volume 2 focuses on policies 1 and 5 to 14. Policies 2 to 4 are touched on in Volume 2 and will need further consideration by the Association of Chief Police Officers, the Association of Police Authorities and the Home Office as part of the follow on work for ISS4PS. This sub-section explains how Volume 2 covers the policies defined in Volume 1.

1.3.1 Establishing the Foundations

Establishing the Foundations

1 **Defining Governance**
2 **Securing Alignment across Forces**
3 **Making National Programmes Accountable**
4 **Creating an Assurance Function**

"It is now widely accepted in the Police Service that to be successful, a national strategy for IS/ICT requires a clear mandate, and the authority and responsibility for realising it must be clearly assigned. To this end, police IS/ICT requires new governance arrangements so that it can best service the corporate needs of policing."[4]

Governance defines the accountability for the implementation of the ISS4PS, and outlines its relationship to the delivery of the business strategy for the Police Service (ACPO/NPIA as the responsible body for programmes that impact across Force boundaries, Chief Constables within Forces, and SROs within programmes). In addition, the governance defines the need for a Technical Authority role acting at all levels of the Police Service to provide the technical assurance for the ISS4PS.

Some of the key considerations for defining governance are covered in section 4, in particular the need for the role of the Technical Authority. It will be the responsibility of the governance body to manage the actions defined in the ISS4PS roadmap (section 5).

1.3.2 Delivering Joined-up Services

"The importance of a national approach to information sharing is now uppermost in current strategy for policing as reflected in the National Policing Plan. However, this is tempered by a realisation that IS/ICT programmes must substantially improve their track record for timely delivery, reliability and cost-effectiveness."[5]

Delivering Joined-up Services

5 **Delivering National Initiatives**
6 **Engaging with Industry**
7 **Sharing Information and Services**
8 **Managing Information**

The justification for the ISS4PS in the long term relies on the delivery of the enterprise portfolio of ICT programmes and achieving the associated business benefits. An enterprise-wide approach may introduce conflict in terms of short-term costs when considered alongside a silo based approach. However, this will be necessary for achieving the longer-term benefits of the ISS4PS End-Game.

In order to ensure that national initiatives deliver the necessary information sharing capability in a joined-up manner, Volume 2 defines guidelines for national initiatives (Annex D) and conformance requirements for achieving the ISS4PS compliance (Annex C). To achieve the technical architecture, at all levels, the Police Service must engage with industry. There is a need to establish a service-wide approach rather than one of engaging suppliers on a force-by-force basis. Volume 2 covers various aspects of design and development, including the involvement of suppliers of IS/ICT components and services (sections 4.2 and 4.4).

Part of the ISS4PS technical End-Game is providing a single view of core Police Service data to all Forces. This, along with common standards for data structures, provides the basis for the joined-up Police Service for information sharing (sections 2.3 and 3.3).

Managing information implies the need for common management processes. These processes will enable effective information sharing and maintain a common approach to presenting information to the public (section 3.4).

4 ISS4PS, Volume 1, Establishing the Foundations.
5 ISS4PS, Volume 1, Delivering Joined-up Services.

1.3.3 Focusing on People

Focusing on People

9 Empowering Police Officers and Staff
10 Deploying Common Services to Citizens

"The needs of two particular groups are prominent in many of the recent inquiries and reports initiated by government and need to be at the heart of future initiatives: Police Officers and staff, and the law-abiding citizen."[6]

The level of consistency in IS/ICT proposed by the ISS4PS will enable the delivery of appropriate training for police officers and staff. This will provide a level of competence across the Police Service that will foster closer working practices, providing a level of consistency to the citizen, irrespective of location.

These policies are not covered directly by any particular section in Volume 2, but form part of the business benefits that will emerge in each phase of the delivery of the ISS4PS Roadmap.

1.3.4 Making it Happen

Making it Happen

11 Shaping the Future of Police ICT
12 Adopting a Common Architecture
13 Deploying Corporate Solutions
14 Coordinating Service Management

"The Police Service needs a more coherent approach if it is to overcome the barriers to interoperability, adopt technologies in a responsive way, and achieve cost savings."[7]

The Police Service must go through a process of harmonising business processes. When core business processes and technical solutions in different areas of the business unify, it will become possible to reap the full benefits of the ISS4PS. The harmonisation of the services provided to meet the business needs is the ultimate goal. Volume 2 does not specify how this will happen, but rather it removes any technical barriers to the harmonisation of business processes throughout the Police Service.

The ISS4PS service-based architecture is considered to be the industry best practice. Service-based architectures capture business logic through a set of loosely coupled services using common standards. The Police Service already has many products in operational use. Inclusion of common products in the technical architecture will only be made where there is a business benefit in standardisation (sections 2 and 3).

Corporate solutions are those solutions that all Forces will use. These include any application, item of infrastructure, outsourced service or other element of ICT where it is beneficial for all Forces to use the same thing. Deploying corporate solutions may be difficult for some Forces where doing so clashes with their current IS/ICT technical architecture and strategy. Over time, the Police Service will find that it is increasingly beneficial to adopt a corporate approach as the set of solutions work together seamlessly, both within and between Forces (section 2.4).

The IT Infrastructure Library (ITIL) captures industry best practice for managing IS/ICT. Adopting ITIL disciplines generally allows organisations to reduce operational risk and increase the level of IS/ICT service to the business (section 4.7).

1.4 History

The ISS4PS has been developed to assist in meeting many of the goals of government imperatives, such as the National Policing Plan (NPP), the Police Science and Technology Strategy, and the Bichard Inquiry, specifically in the sharing and coordination of technology and data.

In 2002 Programme Valiant[8] prepared a comprehensive overview of the way ICT was being used within the Police Service and proposed a number of strategic changes. The study surmised that in order to respond to the

6 ISS4PS Volume 1, Focusing on People.
7 ISS4PS Volume 1, Making it Happen.
8 Programme Valiant used the work of the earlier COLIN project, which explored using software components for designing, building and deploying business 'capabilities' (applications).

increasing demands for business change, ICT within the Forces had to become more responsive and efficient. Programme Valiant identified that the only feasible way of achieving these efficiencies in ICT was for the Police Service to view itself as an 'enterprise' operating at a national level rather than a collection of disparate operations.

ACPO and Central Customer adopted Programme Valiant and refined the approach into a set of projects known collectively as the Information Systems Strategy for the Police Service (ISS4PS). Ongoing initiatives within the ISS4PS are the Enterprise Architecture Framework for the Police Service (EAF4PS), the Corporate Data Model (CorDM) and the Unified Police Security Architecture (UPSA).

In January 2005 ACPO commenced the ISS4PS refresh project to ensure that the technical direction remains consistent with police business strategy. In addition, to represent the arguments for adopting an enterprise approach in a clear manner, reflecting the direction of current government initiatives.

1.5 The 'As-Is' Situation

There are a number of issues with the 'As-Is' situation that must be addressed if the ISS4PS is to be a success. The highest priority issues are:

- **Application Silos**

  In evolving a process to meet immediate requirements, both force level and national application silos have been developed.

  At the force level, many forces have architectures consisting of mixed supplier application silos. Most Forces do not have integrated application suites; each application maintains its own database duplicating data held by other applications.

  Many Forces have been obliged to develop local data warehouses to obtain an integrated view of their data. These typically take data feeds, through local Extract Transform and Load (ETL) interfaces, from the application suites. Using an ETL is limited; it provides a one-way data transfer with no way to provide feedback of a change in the information stored in one system back to another.

  At the national level there has been a move towards greater commonality for more recent procurements. However, central applications such as the Violent Offender and Sex Offender Register (ViSOR) and the National Firearms Licensing Management System (NFLMS) still maintain their own database of data. For both of these applications there is work underway to expose services for integration.

- **Increasing Diversity**

  Diversity at the Force level has increased through use of Commercial Off-The-Shelf (COTS) and Police Off-The-Shelf (COTS) applications from a variety of different suppliers and through the existence of unique Force bespoke developments. There are a number of suppliers in the market, giving rise to a variety of products in use. Many of the Forces customise versions of these products to meet local requirements that further complicate the picture.

- **Piecemeal Approach**

  National initiatives have targeted tactical business needs, for example, Custody and Firearms, rather than taking a holistic view and this has tended to further fragment rather than unify the Force technical architectures[9]. The Police Service has a Police Performance Accountability Framework but lacks a clear mandatory national strategy. This has meant that Forces tend to focus on local rather than national priorities. This has led to a diversity of approaches.

Application silos, the lack of a holistic view, and a wide diversity of approaches are three key issues that the ISS4PS tackles.

9 The focus here is on national initiatives, such as, the NSPIS programme.

Section 2 The End-Game

This section describes the technical blueprint of the End-Game architecture for the Police Service and a phased path for achieving it. The End-Game describes a modern ICT context different to the situation today. Migrating to this technology is a long-term target requiring coordinated action by the Forces to achieve success.

The End-Game supports the achievement of policies 1 and 5 to 14 described in Volume 1 'Understanding ISS4PS'.

Contents

2.1 Overview

The End-Game blueprint describes the goal for Police Service information systems and technology. It covers: technical architecture; service delivery; infrastructure; information sharing, legacy integration; information assurance and standards. It describes a phased approach to meet this goal, aimed at achieving business benefits within each phase.

The key aspects of the blueprint are:

- **Business-led and Responsive to Change**

  The ISS4PS architecture will be based on specific business services and will be sufficiently agile to allow solutions to evolve to meet changing business needs. This will be achieved through the use of a service-based architecture.

- **Integrated Solutions**

  Solutions will be fully integrated, recognising the inherent inter-dependence of police business processes and will avoid the temptation to produce silo-based solutions to individual business problems. This approach will be achieved through the use of an Enterprise Service Bus (ESB). An ESB will provide scalable message-based integration of the business services to be implemented in the technical solutions. Interfaces to data and business services will be based on common open standards, which support interoperability between suppliers solutions.

- **A Single Source of Data**

  The data that underpins the business will be integrated, rather than being held in a set of incompatible data silos. This will be provided through the development of federated data stores at Force level and a Global Data Store/Service (GDS) at the national level. The GDS will be viewed as a single logical database storing information for a number of business areas. It will provide a standard interface to all business data that is of national interest.

- **Harmonised Business Processes**

  Business processes will be harmonised across the Police Service. Corporate solutions will be built or procured to support core business processes, that is, processes that are a core function of the Police Service. There will be a process for deciding which solutions need a corporate approach, and whether one or more alternative corporate solutions are required. Corporate solutions could be approved Commercial Off-The Shelf (COTS), Police Off-The Shelf (POTS) or bespoke products.

- **Implement Once – Use Many Times**

  A Business Service is a technical implementation of a business task which forms part of one or more business processes. Where it is economically and technically feasible, common business services will be implemented once and then used within the corporate solutions, wherever that service is required. This will give rise to a set of core business applications.

- **User Access Through a Variety of Channels**

  Solutions will be designed to provide access through a range of different devices and delivery channels, including desktop and mobile devices. This will be achieved through the use of an SOA combined with XML.

- **Common Security Policy**

  A common approach to security will be provided through the ACPO/ACPO(S) Common Security Policy (CSP). The Unified Police Security Architecture (UPSA) will provide a federated approach for user authentication, authorisation and directory services.

	Non-ISS4PS Solutions	ISS4PS Solutions
Business	• Different Processes • Minimum Reuse	• Similar Processes • Maximum Reuse
Applications	• Local Applications • Legacy Applications	• Core Applications • Central Applications • Services
Information	• Local Data Stores • Police National Computer	• Global Data Store • Global Data Cache
Sharing	• Enterprise Application Integration • Point-to-Point	• Enterprise Service Bus
Security	• Various	• Common Security Policy

Figure 3 The Evolution from Non-ISS4PS to ISS4PS Solutions

Figure 3 highlights how non-ISS4PS solutions, which are prevalent today, will migrate to work within the principles of the ISS4PS.

The ISS4PS architecture is agile and fully supports closer 'joined-up' working in the wider Criminal Justice Information Technology (CJIT) community and other government agencies.

The architecture removes the barriers to sharing up-to-date information by applying data standards, using extensible technologies such as, XML and providing shared services.

2.2 End-Game Phases

The ISS4PS Roadmap has been designed to deliver benefits over three overlapping phases, with each phase delivering business benefits. This allows the Police Service to benefit from any investment made throughout the implementation. The benefits will accrue rather than all being delivered at the end. The phases for delivery will be:

- **Phase 1** will provide an improved local view of data and a greater ability to share information nationally through the implementation of local 'federated data stores';
- **Phase 2** will deliver increasing improvements in the ability to view national data via a national Global Data Store/Service (GDS);
- **Phase 3** will provide a consistent national architecture to access the national data including a suite of corporate solutions.

It is recognised that Forces are at different stages of technology enablement and will join the progression to the End-Game at different points. The progression to the 'End Game' is flexible enough so that Forces have the freedom to continue to deploy tactical solutions in order to meet immediate business needs, as well as moving towards the overall alignment with shared common standards and solutions.

The End-Game describes an IT architecture that is different from what is in place today. However, the approach and technology underpinning the End-Game is not a new concept. A number of Forces have already built or procured integrated systems that support several different business processes. At a Force-level the 'integrated application set' is a suite of interoperable applications built from common services that share an integrated data store (database).

Each of the phases is discussed in the remainder of this section. Further details of two cornerstones of the End-Game, the GDS and the core business applications are discussed in sections 2.3 and 2.4 respectively.

2.2.1 Phase 1 – Federating the Data

Goal

To deliver improved infrastructure, data visibility, exchange capabilities and service management and meet the immediate requirement of making data held by Forces available to other Forces.

Description

There will be a database within each Force containing all core Force data, which is accessible to officers and staff within the Force and other Forces (subject to security controls). This is called the federated data store. It will have a standard interface based on the Corporate Data Model[10] (CorDM) and the existing implementation of CRISP. Forces will develop Extract, Transform and Load (ETL) procedures to load data into the federated data store from existing databases.

The federated data stores will provide an outward facing service that will allow other Forces, and potentially external organisations, to query the data. Access control will be implemented at a local level. This will meet the requirement of making data held by Forces available to other Forces and organisations.

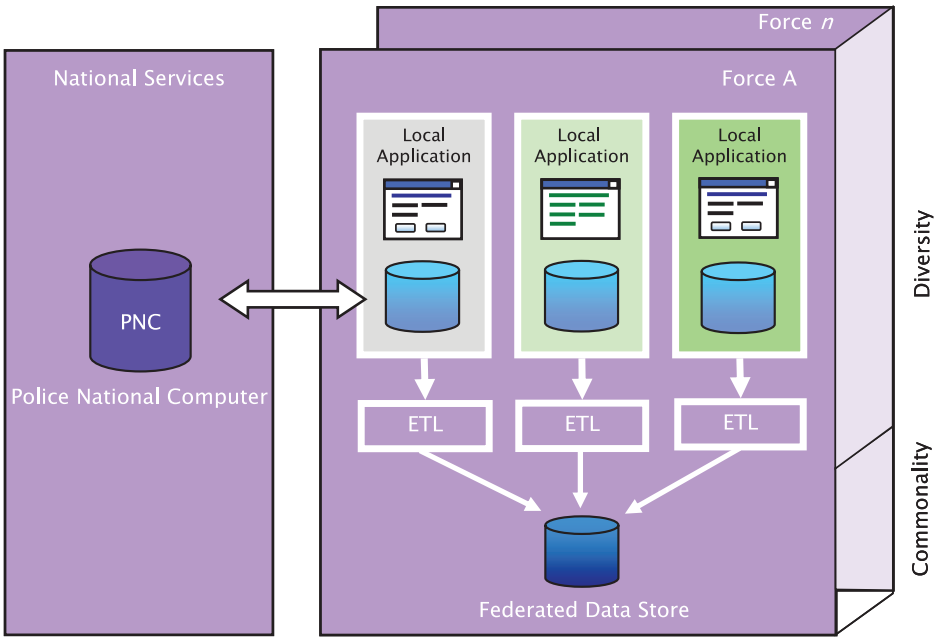

Figure 4 Federating the Data

Within Phase 1, it will be necessary to make some improvements in data quality at a Force level. This will arise from the need to map to standard data objects within the federated data store. However, national standards that define the way in which data is captured, stored, and managed will not have been fully implemented at the start of phase 1, therefore this will be a gradual improvement process.

10 The Corporate Data Model provides the Police Service with the controlled and consistent data environment needed for improved information sharing. The logical data model represents the structure and standards for all data of interest to the Police Service.

To support the increased load from exchanging data, the national network will be upgraded through the provision of the Police National Network 3 (PNN3). Compared with the existing National Network, PNN3 will support a more advanced capability with higher speeds and greater capacity[11]. Force network and infrastructure will be improved to meet minimum standards that will be defined.

The initial phase of implementing a common approach to service management will be in place at local and national levels providing improved quality of service management to the Police Service.

Benefits
A summary of the benefits realised in this phase are:

Policy	Benefits Realised in Phase	
7 Sharing Information and Service	Data visibility within a force Data visibility across forces Data visibility with other organisations	Partial Partial Partial
8 Managing Information	Data equivalence Data integration and simplification Data security	- Partial -
9 Empowering Police Officers & Staff	Data quality Improved Infrastructure capability	Partial Partial
10 Deploying Common Services to Citizens	Data consistency at a national level Increased consistency for the public	Partial -
11 Shaping the Future of Police IS/IT	Minimising dependencies Enabling regional re-organisation Enabling agility	- Partial -
12 Adopting a Common Architecture	Simplicity of Design Increased use of new technology	- -
13 Deploying Corporate Solutions	Increasing economies of scale	-
14 Coordinating Service Management	Improved quality of service	Partial

Table 1 Summary of Phase 1 Benefits

Timetable
Phase 1 is expected to complete in year 2 of the implementation roadmap.

2.2.2 Phase 2 – Globalising the Data

Goal

To deliver a national view on core data, through the implementation of a central data repository known as the Global Data Store/Service (GDS), which will improve the visibility, quality, uniformity and scope of national data.

Description

The GDS will be a national integrated data store that will allow the Police Service to perform searches on the totality of police data (or at least that data which is deemed to be of national interest). The GDS will be populated from the federated data stores delivered in Phase 1. As in Phase 1 Forces will continue to run their own legacy applications and systems that will feed the federated data store through an ETL tool. The legacy applications will still hold the master data.

11 Asynchronous Transfer Mode (ATM) with Multi-Protocol Label Switching (MPLS) are practical technologies capable of supporting the net work improvements required.

The GDS will provide a comprehensive set of interfaces for accessing data including an application to provide query facilities for users. Unlike Phase 1, Phase 2 will encompass both structured, semi-structured and unstructured data and the ability to link them. Duplicate data from the federated data stores will be minimised and the data cleansed using business rules, which support national data sharing. Data cleansing will occur prior to feeding the GDS, thus improving the overall quality of national data. Manual processes will need to be used to improve data quality both locally and nationally, for example, checking whether a data item exists on the GDS before creating a new one.

The GDS will allow persistent associations and links to be created between data items, for example, people and vehicles. This will enhance the value of the information held, especially for intelligence purposes. This facility offers a considerable advantage over phase 1. In Phase 1, although local Force data is available for querying through the federated data store, there is no facility to add association and link information between data items at a national level.

The GDS will become the data store for all new applications that work with core data. For new business services the GDS, rather than the local application's data store, will hold the master data. The GDS will provide an interface for creating, updating, deleting and querying the data to be used by developers of core business applications.

There will be an option to use a Global Data Cache (GDC) alongside the GDS. This is a local copy of the GDS (or an appropriate part of it) supporting the ICT operational needs of a Force. The GDC, hosted regionally or locally, allows the Force to transact directly with the data. The data will be synchronised with the GDS ensuring any data of national interest is immediately available.

Although similar in concept to the PNC, the GDS has a number of major advantages over the current PNC. Specifically, the scope of data held will cover all major business processes, the currency and quality of the data will be significantly improved. It will offer a service-oriented data access interface and there will be formal data quality and ownership rules. The GDS will use the services available from the Unified Police Security Architecture (UPSA) to implement security to a data item level. PNC will be run in parallel with the GDS and will be the source of some of its data.

The design of the GDS supports the concept of the mixed ICT economy, with Forces operating both legacy and new applications and being able to gradually transfer their data to the GDS. The timing for the change from legacy to new applications will be dependent on their individual situations enabling them to join at different points.

Further technical details of the GDS are discussed in Section 2.3.

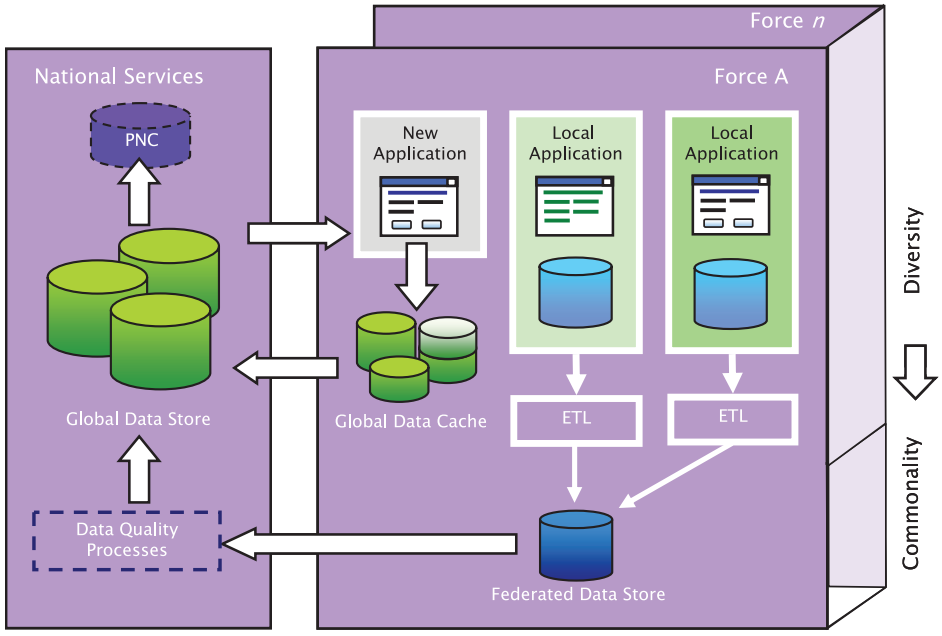

Figure 5 Globalising the Data

Benefits
A summary of the benefits realised in this phase are:

Policy		Benefits Realised in Phase	
7	Sharing Information and Services	Data visibility within a force Data visibility across forces Data visibility with other organisations	Partial Partial Partial
8	Managing Information	Data equivalence Data integration and simplification Data security	Partial Full Partial
9	Empowering Police Officers & Staff	Data quality Improved Infrastructure capability	Partial Full
10	Common Services to Citizens	Data consistency at a national level Increased consistency for the public	Partial Partial
11	Shaping the Future of Police IS/IT	Minimising dependencies Enabling regional reorganisation Enabling agility	Partial Partial Partial
12	Adopting a Common Architecture	Simplicity of design Increased use of new technology	Partial Partial
13	Deploying Corporate Solutions	Increasing economies of scale	-
14	Coordinating Service Management	Improved quality of service	Partial

Table 2 Summary of Phase 2 Benefits

Timescales
Phase 2 is expected to complete in year 4 of the implementation roadmap.

2.2.3 Phase 3 – Globalising the Architecture

Goal

To deliver a common architecture with central and core applications supporting a national view of data and provide a single national approach to ICT.

Description

During the third phase, Forces will migrate towards a common architecture, harmonise their infrastructure, implement a common suite of core applications, and complete the implementation of the common approach to service management.

The implementation of a set of core applications is a cornerstone of the strategy. A core application supports a common Police Service business process, such as, Crime or Custody, within a Force and manages data that is of national interest. The development of core applications will use industry, government and police standards, and will use modern design and development methods. They will exploit modern technologies, such as, portal technologies to support a number of delivery channels including mobile devices.

Applications will be either core, central or local:
- **Core Applications** will write directly to the GDS using the GDS data access services. They can be deployed centrally or from within a Force infrastructure.
- **Central Applications** will be deployed and offer a national service. Existing examples are the Violent Offender and Sex Offender Register (ViSOR) and the National Firearms Management System. These will write directly to the GDS using the GDS data access services and will migrate towards the ISS4PS End-Game.

- **Local Applications** will be deployed to meet local requirements. Where local applications work with data of national interest, they will share this data either through the GDS or through a service interface.

Integration will be achieved through an Enterprise Service Bus (ESB). This will provide the enabling mechanism for reliable message transfer and to 'build' local, central and core applications from the range of available services.

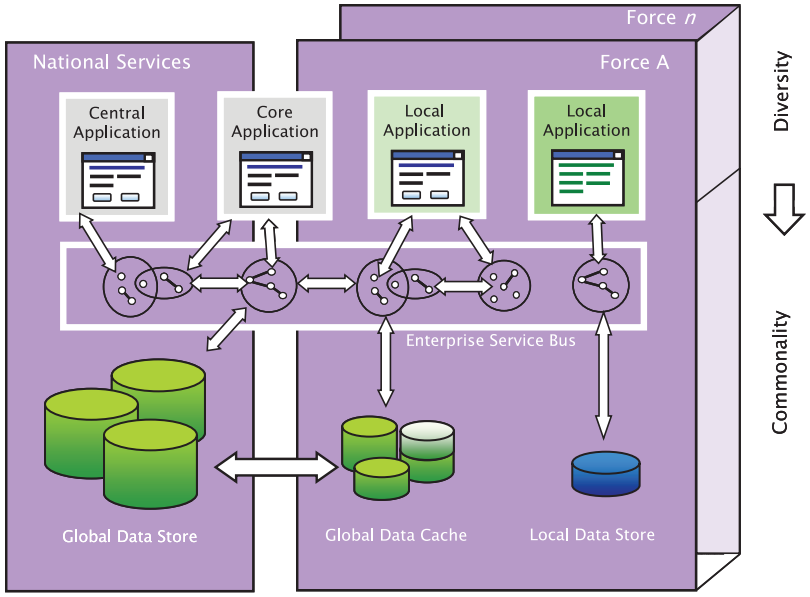

Figure 6 Globalising the Architecture

Benefits

The benefits realised in Phase 3 are:

Policy	Benefits Realised in Phase	
7 Sharing Information and Services	Data visibility within a force	Full
	Data visibility across forces	Full
	Data visibility with other organisations	Full
8 Managing Information	Data equivalence	Full
	Data integration and simplification	Full
	Data security	Full
9 Empowering Police Officers & Staff	Data quality	Full
	Improved Infrastructure capability	Full
10 Common Services to Citizens	Data consistency at a national level	Full
	Increased consistency for the public	Full
11 Shaping the Future of Police IS/IT	Minimising dependencies	Full
	Enabling regional reorganisation	Full
	Enabling agility	Full
12 Adopting a Common Architecture	Simplicity of design	Full
	Increased use of new technology	Full
13 Deploying Corporate Solutions	Increasing economies of scale	Full
14 Coordinating Service Management	Improved quality of service	Full

Table 3 Summary of Phase 3 Benefits

Timescales

Phase 3 is expected to complete in year 6 of the implementation roadmap.

2.3 Global Data Store/Service

2.3.1 Approach

The End-Game architecture holds core data from several sources and is accessed from a Global Data Store/Service (GDS) to provide a single view of data across the entire police enterprise. It will provide national visibility, ensure consistency, and assist in improving the quality of data.

- **The GDS** will allow users to search through the entire collection of police data in order to acquire all the data that the Police Service holds for a particular request. This will provide a facility for Police Officers and Staff that is only partially possible at present.
- **The GDS** will assist users when entering new data by letting them know if this data already exists. This will assist in preventing duplicate effort (entering data more than once) and duplicate data being stored. It will also assist in maintaining a high quality of data.
- **The GDS** will allow new applications access to any of its data through a set of well defined interface services. This will eliminate the need for new applications to have their own services built to support data types already stored on the GDS. Thus applications will be cheaper to build.
- **The GDS** will require the implementation of a common security policy for access to its data.

Core data is defined as data that is of national interest to the Police Service. Local databases continue to hold data items that are purely of local interest. The Corporate Data Model (CorDM) will provide the starting point for defining the logical structure of the core data. The mapping of the core data onto the database tables within the GDS, the physical data model, will be based on the practical experience of the CRISP project and analysis of business use.

The move to a single logical transactional data store will be a major change from the current environment. However, the approach of having a single integrated transactional data store is not a novel one. Several Forces have migrated to an architecture where applications share a single database. The GDS is simply a scaled-up version of this approach. Initial estimates show that the size and performance required by the GDS is achievable using current technology[12].

2.3.2 Design

The GDS will have the following characteristics:

Design choice	Description/benefit
CorDM and CRISP	The GDS design will be based on both CorDM and CRISP. Lessons will be taken from both projects to design the physical data model capable of supporting the data volumes and concurrent access requirements for the GDS In particular, the logical CorDM data model, the CorXML data structures, the CRISP physical data model, and the practical implementation of CRISP will strongly influence the design.
Disaster Recovery	The GDS will hold data of national importance; it is essential that there are plans for business continuity in the event of a disaster. The GDS will have a primary and secondary site with full disaster recovery linked by fast networking with facilities for automatic switching between sites.
Data Access Services	Services will be developed to provide access to data. The services will include business rules for managing access to data, ownership and maintaining associations between data items.
Local Caching	The GDS will provide the option for Forces to use the Global Data Cache (GDC), which will store a copy of some of the data from the GDS locally or regionally. This will increase the efficiency while maintaining a single logical master database.
OLTP and OLAP	The GDS will be tuned for On-line Transaction Processing (OLTP). If this does not prove efficient enough for complex searches to support tactical and strategic decision making, a separate read-only database could be implemented tuned for On-Line Analytical Processing (OLAP).
UPSA	A Unified Police Security Architecture (UPSA) will be used for identity management and authentication.

Table 4 Characteristics of the Global Data Store/Service

12 Initial estimates have been based on current and predicted transactional usage of the PNC and research conducted in industry leading architectures for large volume transactional databases.

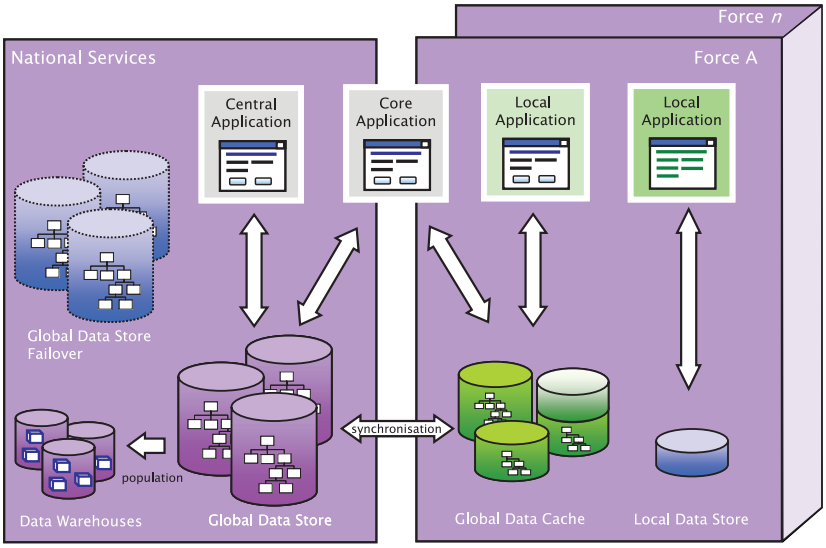

Figure 7 Global Data Store/Service Architecture

2.3.3 Data Quality

There is a business requirement for the Police Service to have access to high quality data. Without high quality data, many of the benefits of the GDS will be lost or minimised. The existence of the GDS will assist in ensuring high quality data, in that it will be easier to check for and eliminate duplicate entries. However, it is essential that this is supported by a set of data management business processes.

A set of data quality standards and processes for placing data into the GDS and then managing it will need to be agreed. These standards and processes will define:

- The minimum data quality standards of the source of the data in the Forces;
- The rules for cleansing data within the GDS;
- The business rules on ownership and management of the data within the GDS that are applied to meet the quality standards.

The Police Service requirements on data are complex, for example, suspects may give false details; historical details of people, such as, physical appearance need to be kept. These complexities give rise to several database entries being kept for a single physical person, or any other data entry.

The quality standards will provide rules for checking whether an entity (person, vehicle etc.) already exists in the database before creating a new entity. They will identify the matching algorithms (fuzzy matching) that need to be available to identify data items. Once stored all major data items will have a unique identifier. The data quality standards will incorporate procedures to be followed when working with legacy applications, such as, checking through the query interface to determine whether an entity already exists in the GDS before creating a new one.

The data quality standards will define the business rules for data ownership, weeding, audit, access control, and mandatory fields for different business transactions. These rules will be implemented by the data access services. The data ownership rules will support a data owner for each object (person, vehicle etc.) stored in the GDS. In some cases, one person will store data about a person (or other object) in the GDS, while another will add additional information at a later stage. In this case, different people may own different parts of the data.

This example illustrates how the GDS would operate in practice. Consider three Forces A, B and C. A user in Force A enters details of a vehicle reported as stolen in their area through their application. Details entered are immediately stored in the GDS and made available to all Forces with a local cache of the data.

Force B receives a report of an abandoned burnt-out car. When entering the details in their application, the GDS identifies that the car stolen in Force A is likely to be the same vehicle. Force B provides a link from the information they have entered with that provided by Force A along with a reason describing the link.

Force C is investigating an armed robbery and so searches the GDS for records of matching vehicles. They find the record of the stolen vehicle in Force A, and track the link to the burnt out car in Force B.

2.4 Core Applications

As the ISS4PS Roadmap is enacted through its three phases, there will be an increasing use of core applications. This section provides more detail on these core applications.

2.4.1 Approach

Core applications will support core police-specific business processes, for example, Command & Control, Crime, Custody and Intelligence. To date, these have been addressed by a range of specialist suppliers and bespoke developments. As business processes are harmonised across the Police Service, there will be increasing advantages to be gained in procuring a single product, or perhaps a small number of products, that support these core business processes.

A national Core Application set will be identified to support these business processes, which store data in the Global Data Store/Service (GDS). Core applications could be Commercial Off-The-Shelf (COTS) products, Police Off-The-Shelf (POTS) products or bespoke developments. Any product used would need to be integrated with the GDS. This represents a fundamental change for suppliers and the Police Service. The business processes will be exposed as a service to enable reuse.

Core applications will be assembled from a number of shared and local services to deliver the full functionality required. Shared services will access data in the GDS and local services, implemented by the Forces, access the local data stores.

There are other business functions that are not unique to the police service, such as, HR, Office Automation and Finance. In most cases configurable COTS products exist that can meet these needs. These business processes may contain core data items that need to be stored within the GDS and use the GDS data services.

Central applications will be deployed centrally and provide a national service. They will be evolved from the current national applications to write directly to the GDS and meet the design principles outlined below in 2.4.2.

Local applications, specific to a Force that contain core data may also need to access the GDS.

2.4.2 Design

The development of core applications will use the following design principles:

Design principle	Description/benefit
Common Presentation To Users	Applications and services will use technology that collates and presents information from different sources via a single user interface. It also provides a simple mechanism for the delivery of information to different types of devices, for example desktops and mobile devices. See section 3.2.4 for more details.
Service-Based	Systems will be developed using a Service-Based approach. This will be achieved using the Service-Oriented Architecture (SOA) design model. This is a modern and agile approach to delivering solutions. Because of the greater agility of SOA, system changes can be achieved quickly. SOAs lend themselves to maximise reuse of software and therefore achieve economies of scale.
Business Services	Business processes will be modelled and implemented in technology as business services. Applications will be built from sets of related business services.
Modularity	Business services are modular, loosely coupled components, built to implement a particular business function, and can be re-used in different applications. They will be built from common modules, such as, a module to manage Vehicles, or one to manage Nominals.
Service Integration	Service Integration will use a consistent method to integrate business services and transfer data between modules. Products that provide integration facilities for shared services, commonly referred to as Enterprise Service Bus (ESB) products, will be used.
Modern Development Methodologies	The use of rapid design and deployment methodologies (such as Model Driven Architecture (MDA) and re-use of patterns) will speed development and reduce cost.
Open Standards	All systems will use open standards, that is, non-proprietary published industry, government or police standards defining how different systems and components work together. This will ensure interoperability between different supplier and partner products.

Table 5 Design Principles for Core Applications

Using the design principles outlined, the End-Game offers a number of possible deployment options. Forces could choose to host data and core applications locally using the Global Data Cache (GDC), or they could use a regional or centrally hosted system.

2.4.3 Legacy Applications

The migration to the End-Game will support legacy applications, which will be operating within the Police Service for the foreseeable future. They can be incorporated into the architecture in a number of ways, for example, using wrapper technology to expose service interfaces. The ability to support a mixed ICT economy is an essential part of the migration strategy.

2.4.4 Central Applications

Central applications will provide a national service. The process of migration will involve two stages. The first to use the GDS as its database/service and the second to meet the design principles discussed in 2.4.2. The migration plan for each central application will be considered and agreed in turn, with the requirement to write to the GDS and to expose ISS4PS compliant services being the major goals.

2.4.5 Outsourced Services

The End-Game will support business areas that have been fully outsourced, for example, the national IDENT1 service. In the End-Game architecture, outsourced services will be configured to write (and potentially read) relevant data to (and from) the GDS through the data services provided. Where implemented on the same physical infrastructure, outsourced services will interface to the GDS in the same way as any other application.

2.4.6 Third Party Suppliers

The Police Service will source applications, business services, components and outsourced services from third party suppliers as well as potentially retaining in-house development capability. These components could be:

- COTS products;
- POTS products;
- Bespoke components.

It is important that all products fit into the architecture of the solutions being built, in order that the solution is conformant to the ISS4PS. It is likely, therefore, that the work to integrate COTS and POTS products will need to be carefully thought through in order to achieve this. The role of the Technical Authority will be established in order to ensure that this is done.

2.5 Delivering the End-Game

The End-Game, described in sections 2.2 to 2.4, explains the vision of the technical architecture and defines the phases in which it will be achieved. The realisation of the End-Game requires a number of fundamental management and supporting processes to operate effectively to achieve success.

2.5.1 Procurement

The realisation of the 'End Game' requires a fundamental change in procurement. To achieve the cost saving benefits of the core business applications and corporate solutions a national Procurement Authority is needed. The Procurement Authority must be responsible for procuring the core business applications and setting up procurement frameworks for procuring COTS products on behalf of the Police Service.

From the supplier point-of-view the development of the core application set represents a fundamental change to the market. Suppliers will compete to develop service components and products that will fit within the overall technical architecture, and will integrate these with approved components developed by other suppliers. Contractual SLAs will need to reflect the interdependence between suppliers.

In some cases, the Police Service may wish to retain Intellectual Property Rights (IPR) for bespoke developments. In other cases, the only thing that will be required is some guarantee of stability of interfaces. The intention is that there is a stable environment for integration.

2.5.2 Design & Development

The development of core business applications will use a proven agile development framework. The software engineering methodology will be required to support the following fundamental concepts:

- Iterative development;
- Requirements management;
- Visual modelling;
- Verification of software quality;
- Controlled changes to software.

Clear checkpoints shall be built into the development cycle to provide progress review points.

It is not the intention to restrict suppliers' development methodology, particularly for COTS and POTS products. It is the intention that the Police Service retains sufficient control over the development to ensure speedy changes and conformance to the ISS4PS, in an environment where business requirements are known to change.

2.5.3 Service Management

The Police Service will take an enterprise view on service management based on ITIL. As part of the Service Authority and Technical Authority roles, a common approach to the implementation of ITIL will be agreed together with the identification of common tools for its implementation. A migration plan will identify a phased approach to its implementation within the Police Service. Suppliers providing outsourced services will be required to fit into this regime.

2.5.4 Technical Governance

A Technical Authority will be created to provide the proactive technical expertise, leadership and the coordination needed to create the End-Game technical architecture. The role will operate nationally and locally, at the enterprise, programme and local level. Section 4 defines the role in more detail.

One of the key responsibilities will be developing and maintaining a Technical Reference Model (TRM), which defines the End-Game technical architecture, and a Technical Reference Implementation (TRI), which will be an example implementation of the technical architecture.

2.5.5 Coordinating National & Local Priorities

The national view of the End-Game requires the Police Service to have a national and coordinated view of ICT priorities. The Capability Plan, which is produced annually, prioritises the business needs and is a companion document to the ISS4PS. Delivering the End-Game requires a national Police ICT plan, based on the Capability Plan and the ISS4PS, to be maintained. It must be produced in consultation with Forces and in sufficient time to meet their local planning needs.

Section 3 ISS4PS Technical Foundation

This section describes the technical architecture of the End-Game. It focuses on the key areas for those seeking to apply the ISS4PS and identifies a set of principles and actions that will aid architects and designers in applying the technical architecture.

Contents

3.1 Frameworks, References and Standards

The common technical architecture for the Police Service will be defined and documented based on non-proprietary open standards. Open standards underpin interoperability and sharing of data providing a common reference taxonomy and delivery framework.

This section describes how foundation documentation for the ISS4PS technical architecture will be captured, described and published.

The following topics are covered in this section.

- **Enterprise Architecture Framework**

  Describes the use of an Enterprise Architecture Framework to document and plan Police Service business and technology.

- **Standards Information Base**

  Provides facts and guidance on standards that underpin the ISS4PS.

- **Technical Reference Model**

  Describes the key components of the technical architecture and establishes a common Force-wide technical language.

- **Reference Implementation**

  Details the physical implementation of the TRM proving the best practice guidance in the SIB and TRM.

- **Compliance Assessment**

  Describes the methods and approach to assessing architectural compliance.

3.1.1 Enterprise Architecture Framework

An Enterprise Architecture Framework (EAF) is a system that supports the management of the entire business life cycle by providing a single place where knowledge on business processes and systems is recorded and coordinated. Research shows that the use of an EAF achieves agility, standardisation, security, performance and consistent management across an organisation[13].

The Police Service has not yet embraced an integrated view of itself as an enterprise. This has resulted in Forces and national programmes taking a parochial approach that does not take into account the requirements of the Police Service enterprise.

Issues	Principle: Documentation
The lack of an overarching Enterprise Architecture Framework with national scope inhibits consolidation and integration across the Police Service.	An ISS4PS Enterprise Architecture Framework will be used to understand, plan and document the business and technology landscape.

Approach

A national EAF will be made available to Forces providing a broader perspective to the entire business life cycle and the ISS4PS technical architecture. Forces may decide to have a local version of the EAF or can use the central service to build on the national perspective to meet local needs. The national EAF will support formal methodologies to deliver improved clarity about their business requirements and technical solutions.

There are a number of framework reference models that have been developed, sometimes for proprietary use, which are used to define the EAF. A commonly-used EAF is the Zachman Enterprise Architecture Framework[14].

The national EAF will provide a standardised way for the Police Service to manage its business and technical artefacts through:

- **Taxonomy**
  A standardised taxonomy describing the business and technical artefacts;
- **Models**
  Models that can be used to document the interrelationship of business processes, information systems, technology, and describe the graphical and textual elements of the models;
- **Definition**
  The goals and objectives of national and local programmes being clearly defined;
- **Governance**
  The relationships to direct and control the enterprise to achieve the goals of joined-up working;
- **Standards**
  The XML and UML will be the standards used to define the relationships between different areas of the technical reference model;
- **Business Process Definition**
  Understanding of elements, including business processes, at a primitive level making them independent of notation and methodology.

The use of formal methods improves the clarity in expressing business requirements and is directly relevant in the broader perspective of an EAF[15]

The Police Service needs an EAF to clearly document the broader and national interests of the Police Service.

Action 1	Deliverable
PITO/NPIA and the Forces will: Deliver and populate the ISS4PS EAF tool.	 Operational and fully populated EAF implementation.

13 Gartner Real IT Strategies Report 2004.
14 See http://www.zifa.com/ for details on the Zachman Framework.
15 Some of the best known formal methodologies are The Open Group's Architecture Forum Architecture Design Methodology (TOGAF ADM), Integrated DEFinition Methods (IDEF), Unified Software Development Process (USDP), IBM's Rational Unified Process (RUP) and Structured Analysis and Design Methodology (SSADM).

3.1.2 Standards Information Base

A Standards Information Base (SIB) is a single source of information on the standards used in a technical architecture, providing both references to the standards that have been adopted and guidance as to how they should be applied. Having an SIB for the Police Service means that there will be no barriers to Forces, national programmes and suppliers in implementing solutions that use these standards.

Issues	Principle: Standards
Documentation on standards to support the ISS4PS architecture is currently fragmented.	A freely available SIB will be created, published and maintained to support the implementation and procurement of ISS4PS-compliant systems.

Approach

A knowledge base of open industry and government standards, open police standards and guidance material will be made available to document all technical aspects of the ISS4PS. The standards in the ISS4PS SIB will include:

- Industry standards, such as, HTTP, XML and SOAP;
- Government standards, including ITSEC E3, e-GIF and e-GMS;
- Police Service standards such as CorDM and SMART.

The standards in the SIB will be free of licensing and copyright restrictions. Some standards will have legal status, others will be mandated and some will be recommendations to reflect best practice. The status of each standard within the SIB will be maintained along with any other relevant information, such as, guidance notes or links to complementary standards. The ISS4PS SIB will have three primary uses:

- **Architecture Development**
  To document a technical reference for developing an ISS4PS compliant architecture.

- **Procurement**
  To define the compliance and procurement guidance and criteria for all new systems and solutions.

- **Guidance**
  To provide a catalogue of ICT standards as a centrally maintained source of relevant standards and guidance material for the Police Service.

Procedures and processes will ensure that the contents of the SIB are up-to-date and accurately mirror best practice of the ISS4PS technical architecture.

When creating new police specific standards the Police Service must commit to making them as open as possible. Updates to the SIB will be one of the drivers to refresh the ISS4PS.

Action 2	Deliverable
PITO/NPIA will: Develop the ISS4PS SIB and identify standards that are appropriate for use and populate the SIB with them.	 An online searchable ISS4PS Standards Information Base.

3.1.3 Technical Reference Model

A Technical Reference Model (TRM) is a recognised approach to describing a technical architecture. It provides a universal language for expressing the common products and corporate solutions that have been adopted (see Policies 12 and 13). The TRM gives a definitive representation of the architecture so that Forces, national programmes and suppliers can design and implement compliant solutions.

Issues	Principle: Endorsement
There is no single Force-wide reference to assist Forces in developing their local architecture in accordance with the ISS4PS.	An ISS4PS Technical Reference Model will be developed and used as the basis for the development of all new local and national Police Service systems.

Approach

The TRM will provide clear guidance to Forces to assist them in evolving their local architecture to be ISS4PS-compliant. It complements the Standards Information Base by linking standards, specifications, products and technologies.

A common vocabulary will be established enabling interoperability and portability to be consistently addressed across all Forces through the definition of core infrastructure components and services.

The ISS4PS TRM will focus on aspects of relevance to the Police Service architecture, specifically the:

- Business Applications;
- Security;
- Data Management;
- Data Interoperability;
- Transaction Processing;
- Software Engineering;
- Communications Infrastructure.

The TRM allows Forces to build their own architecture by identifying the relevant products and solutions in the different service areas. The TRM fosters commonality in Force architectures by focusing on common products. This will build on work already begun in the Police Technology Database.

The widely adopted and vendor neutral The Open Group Architecture Framework (TOGAF) TRM will be considered when defining a police-specific ISS4PS TRM.

Action 3	Deliverable
The Technical Authority will: Develop the TRM and identify products that are appropriate for use by the Police and populate the ISS4PS TRM with them.	 An ISS4PS Technical Reference Model and an updated Police Technology Database containing references to the ISS4PS TRM.

3.1.4 Reference Implementation

A reference implementation is an implementation of the technical architecture outside the operational environment. The ISS4PS requires proof that the technical architecture is practical, can be implemented successfully and provides a baseline demonstrating the theory behind it. This will be proved through a reference implementation, which will evolve as the technical architecture evolves. This will enable both new technology and emerging standards to be proved outside an operational environment. It is through this route that it is possible to ensure that existing solutions remain interoperable with potential changes to the service environment. Ultimately, the reference implementation will de-risk delivery plans by providing a compliant environment, in which solutions are assessed and accepted against best practice.

Issues	Principle: Provability
Forces and suppliers need tangible proof of the best practice guidance for applying the ISS4PS. Emerging technology and standards require proving prior to being adopted into the SIB and TRM and thus made available to the development community.	A reference implementation of the ISS4PS technical architecture will be provided. In proving relevant emerging standards and technology, the strategy and the SIB can be kept current while minimising the impact on existing deployments.

Approach

A reference implementation of the ISS4PS architecture will provide a complete physical implementation of the technical architecture. It bridges the gap between the theory and real-world operations by providing a complete physical implementation of a technical architecture. It proves the best practice defined in the TRM and SIB.

The Reference Implementation will:

- Demonstrate the core characteristics of the technical architecture;
- Prove the TRM and Standards Information Base;
- Provide a definitive and standard managed platform where solutions can be tested for compliance;
- Provide the basis for assessing compliance;
- Provide a platform for strategic assessment of emerging technologies and standards and enable an impact assessment on the existing architecture;
- Enables a degree of performance assessment to occur.

The TRM and the SIB will be the primary resources used in building the ISS4PS Reference Implementation. The act of building a physical implementation will generate a set of artefacts and assets that can be used to further develop these resources.

Action 4	Deliverable
PITO/NPIA will: Develop the ISS4PS reference implementation.	 A full implementation of the ISS4PS Technical Architecture End-Game and a set of best practices and guidance.

3.1.5 Compliance Assessment

The ability to continually assess compliance during the procurement and development of the ISS4PS applications eliminates costly errors. An Application Test Framework provides the tools and control structures supporting continual assessment. The Police Service needs a way of verifying that solutions and Force infrastructures comply with both the ISS4PS technical and information architecture. Annex C documents what compliance is and how it will be assessed in detail.

Issues	Principle: Conformity
A lack of criteria and associated assessment of both technical designs and architectures leads to an inconsistent level of technical solutions.	A series of both architecture and implementation assessments will occur during a programme life cycle. Assessment will be made against a series of checklists to gauge both strategic and infrastructure alignment of programmes.

Approach

To assist both Forces and vendors in complying with the ISS4PS strategy, assessment criteria will be gathered from programmes and projects to build up the Application Test Framework for publishing. The contents of the framework are based on the TRM and SIB and will include:

- **Test Specifications**

  The test specifications will define the ISS4PS conformance criteria and testing resources to support an automated test capability.

- **Assessment Tools**

  The assessment tools will provide automated testing and guidance for the elements of a programme that provide information exchange facilities.

- **A Test Environment (sandbox)**

  The test environment will be a physical implementation of the TRM separate from the reference implementation. It provides programmes with an isolated environment to undertake assessment of compliance prior to submitting for formal ratifications against the reference implementation.

As a minimum, the compliancy assessment will cover:

- **Compliance Checklists**

  Step-by-Step guides enabling key ISS4PS aspects for applications and environments to be recorded as compliant. These can be found in Annex C and will evolve over time.

- **Regression Tests**

  Tests that evolve over time and supplied with every component and service, allowing the Police Service to continuously monitor compliance of items supplied, upgraded and maintained.

- **Software Tools**

  Tools will be provided to assess applications compliance against the baseline ISS4PS architecture and SIB. To support vendors and Forces, the tools will need to be designed and delivered in electronic form to support development and testing of solutions remotely from the centrally managed test environment. The tools will be provided under a ‘creative’ licence allowing them to be extended either by vendors or Forces, providing that those changes are made available to the wider community.

Action 5	Deliverable
PITO/NPIA will: Define the ISS4PS Application Test Framework, applicable test tools and test environments.	An Application Test Framework suitable for remote, stand-alone and integrated testing of solutions. This framework will include automated tools where applicable to automate testing as far as possible.

3.2 Application Architecture

The ISS4PS technical architecture enables solutions to be built that meet Force and national business needs as well as working together in a national joined-up ICT environment. The architecture is both forward-looking and risk-averse, using modern but well-established technologies and integration principles.

The following sections detail the architectural principles and preferred approach to constructing Police Service applications.

- **Service-Based Architecture**

  Service-Based Architecture is the modern approach to developing business solutions. It enables solutions to be assembled from autonomous components in a manner that allows collaboration between different applications. It also provides the flexibility for solutions to evolve with changing business needs.

- **Service Integration**

  Integrating existing services is essential to achieve the economies of scale in developing new applications and promote joined-up working.

- **Components and Services**

  Components and services are the reusable elements from which business solutions are made.

- **Presentation**

  The technology behind the user interfaces enables different devices to be configured to access the business solutions.

3.2.1 Service-Based Architecture

The ISS4PS architecture model is service-based. Systems in a service-based architecture provide reusable business functions that enable new applications to be built from existing solutions. Reusable functions are built as autonomous units of software, made available for reuse as a service. These shared services represent the building blocks for applications that support the automation of business processes and can adapt to change.

Progressive adoption of shared services will allow the Police Service to achieve a greater level of consistency and simplify data sharing across the Police Service, Criminal Justice System and other government agencies.

Service-based Architecture is a departure from complex application development, promoting standardised interfaces and increased joined-up working. It is an evolution of previous design models making better use of ICT. The ISS4PS architecture can be delivered using the Service-Oriented Architecture (SOA) design model and its associated open standards. (See Annex A for details of standards applicable to the ISS4PS).

Issues	Principle: Reusable Services
The increasing rate of business-led change has left ICT solutions struggling to keep pace, more often a constraining factor on success rather than an integral part. The Police Service is no different, finding itself constrained by a disparate mix of ICT solutions and unable to adapt quickly.	The architectural basis for new applications will be shared services using a Service-Based Architecture.

Approach

A service-based architecture is set apart from previous architectural design models as users focus on services rather than ICT systems. This enables the Police Service to procure services from various ICT service providers that support the architectural principles of the ISS4PS or build their own. This architecture supports loose coupling allowing services to be written with less interaction between developers and suppliers. This loosely coupled environment enables a shorter time to deliver solutions by combining and reusing services. Data that is passed between services provides the coupling. This presents a challenge as data must be consistently defined across the services. The ISS4PS addresses this by standardising the data held in the Global Data Store/Service (GDS). The ISS4PS data and service-based End-Game is delivered in three phases:

Phase 1: Federating the Data

Federating the data delivers consistency for exchanging data between Forces. It is a crucial step that provides the ability to combine data nationally in a GDS and begin planning for shared services. Although shared services are not delivered in this phase it is recommended that Forces plan a training programme around SOA in preparation for future work.

Phase 2: Globalising the Data

Forces will migrate Force level data of national interest from the Force federated data stores, delivered in phase 1, to the GDS to provide national consistency and visibility of core data. New applications will use the GDS as their data store. Shared services will start to emerge during this phase and be adopted by all new applications. Service Level Agreements will be defined for the shared services to clearly identify operational responsibilities within the loosely coupled SOA environment.

Phase 3: Globalising the Architecture

Central and core applications will be delivered during this phase for all common Police Service activities. These will use shared services within an SOA. Local solutions will complement these by operating against local data stores and the GDS for core data. The interface between the GDS and local solutions will be achieved via shared services.

3.2.2 Service Integration

Assembling self-contained reusable service requires a robust mechanism. The service-based architecture of the ISS4PS benefits from infrastructure capabilities that enable applications to be composed of several shared services irrespective of their location.

The infrastructure capabilities for integrating services must support message and event-based interaction in a mixed ICT environment. These capabilities are currently provided in products and are commonly referred to as Enterprise Service Buses (ESBs). For the ISS4PS the key benefit of an ESB is the ability to share services across the Police Service and intelligently route messages based on content. For example, changes in a Duty Roster system for a police officer typically require Command and Control systems to be updated. This enables a higher degree of joined-up working and process automation.

Issues	Principle: Integration
The Police Service needs an implementation that will deliver the value of a service-based architecture, in a consistent manner, nationally and locally. The implementation needs to provide both the flexibility and control that is required to create an agile environment.	New initiatives requiring integration between services and applications will use an Enterprise Service Bus (ESB).

Approach

Integrating non-standardised services is a challenge. The ISS4PS addresses this by requiring services to be standards-based. Shared services will be accessible via an ESB supporting reuse of local and national components. New applications will reuse existing services and, where appropriate, develop new ones. Adopting service-oriented principles will ensure that the Police Service is able to respond to unforeseen changes in local and national requirements. An ESB can be product based or a bespoke development. Product based ESBs offer advantages over bespoke initiatives, for example, performance monitoring, technology adapters enabling legacy solutions to migrate piecemeal to an SOA, and prioritisation of service requests so that time-critical processes are prioritised over non-critical processes. The Technical Authority will assess ESB products for the Police Service at local and national levels and publish a list of recommended products.

In the context of the ISS4PS an ESB must contain the following qualities:

- Support Force wide shared service architecture;
- Provide reliable messaging between services and applications;
- Support the transformation of data when required;
- Orchestrate services into business processes;
- Provide a management infrastructure;
- Support open-standards.

The ISS4PS advocates that Forces will implement service buses at the Force level that interact with other service buses across the Police Service. It is envisaged that, over time, all existing non-ESB-based integration solutions will be replaced with ESB alternatives. In this way, an ESB provides a flexible way for Forces to migrate to a SOA. This inherent flexibility means that it provides a migration path for most, if not all, of the different types of Forces within the Police Service.

Action 6	Deliverable
The Technical Authority will: Select one or more ESB products suitable for the Police Service at local and national levels.	A list of recommended Enterprise Service Bus products.

3.2.3 Components and Services

Project Valiant introduced the concept of reuse through the use of Component Based Design (CBD) in developing applications. This is a valid approach for applications that rarely change. However, where requirements change more often, and in unexpected ways, CBD inhibits the ability of the Police Service to respond to change in a timely manner.

Insufficient configuration control on components can result in reuse being achieved via a 'copy and change approach' giving rise to many divergent copies of a component being used on projects. Evolving CBD by applying a Service-Based approach delivers an agile business-led technical architecture supporting business change. It also provides the appropriate configuration control and reuse via a 'discover and use' mechanism.

Issues	Principle: Standardisation
There is little evidence to suggest that component reuse is being achieved, either at a local or national level. Applications developed around CBD typically deliver reusable components as tightly coupled, inflexible silo applications. CBD does not address the central issue of agility, instead 'hard-coding' of business logic, workflow and other forms of business knowledge is delivered in compiled code.	New applications will be built from services, wherever an applicable component or service has been identified as a police standard.

Approach

The Police Service will evolve the CBD concept to address the issue of how components are coupled together to provide agility. Components will be accessed via Services to achieve reuse. Service interfaces will be defined and published in a Service Library enabling intelligent design and integration requirements to be made.

Components
Components contain functional units of business logic. They are typically assembled into an application to deliver a specific business. Enterprise components provide common functionality for use by several applications to deliver a specific business need.

Services
A Service represents a coarse-grained autonomous unit of business logic, such as, retrieving an ANPR report for a vehicle. They have clearly defined interfaces that are separate from the implementation of the business logic allowing 'mixed economy' solutions to contribute collaboratively to serve real-world business activities. Services differ from components in that they expose messaging end-points rather that an API. Services will typically be built using components supplied by vendors as libraries or developed as part of the applications.

Business Services
Business Services is a term used to describe how several Services are brought together to provide a reusable end-to-end business process. These vary in scope and functional granularity according to business needs. These are typically defined and managed within middleware products, for example, an Enterprise Service Bus.

The ISS4PS service-based architecture delivers application functionality by orchestrating services into combined business services.

It is important to note that services are not necessarily based on web-services and an SOA implementation need not use web -services. Web-services are a practical open-standard approach for realising services and are advocated for the ISS4PS.

The terms Service and Business Service are known by many other names when describing a service-based architecture. Formalisation of these terms is taking place as part of the work by OASIS[16] in establishing a reference model, announced in May 2005.

Action 7	Deliverable
The Technical Authority will: Identify and maintain a set of standard enterprise components and services.	A core set of components, services and business services defined and documented in a Service Library.

16 OASIS (Organization for the Advancement of Structured Information Standards) is a non-profit, international consortium whose goal is to promote the adoption of product-independent standards for information formats.

3.2.4 Presentation

Police officers and staff make use of many different applications through a variety of different devices and with a range of different user interfaces. Applications are often restricted to a particular type of device – typically on the desktop. Users have to be taught to use applications with many different user interface styles and data presented in inconsistent ways. Typically, to change the user interface requires extensive changes to the application.

Issues	Principle: Presentation
Traditional application development has produced applications where the user is locked into one user interface and where it is difficult to extend the application to cope with other presentation delivery mechanisms. Lack of integration between applications at the user interface level has led to an inconsistent look-and-feel and behaviour.	Browsers will be used as the primary presentation mechanism for all new applications. New applications will use the principles set out in the ISS4PS Style Guide (version 3.0 or later). New applications will allow for access from a range of client devices.

Approach

The goals of the ISS4PS presentation architecture are:

- To enable applications to be built in such a way that users can interact with them through a variety of different devices (mobile, desktop, PDAs etc.);
- To present the same information to the user, no matter what device is used;
- To present data items in a manner that is consistent, irrespective of the business process that the user is involved in.

The primary mechanisms for achieving these goals are:

- Separation of the data from the business logic;
- Separation of the presentation mechanism from the business logic;
- Use of consistent data definitions;
- Use of the ISS4PS Style Guide.

Although browsers will be the primary mechanism for presentation to the user, the architecture allows a variety of methods depending on the business need, for example, a high-resolution 3D imaging application may be more suited to smart-client technology.

Separation of the business logic and the user interface allows the flexibility to evolve applications to new devices, for example, a firearms licensing application, accessible from a desktop can more easily be extended to allow access from an Airwave mobile device.

Action 8	Deliverable
The Technical Authority will: Create guidelines and standards relating to what client devices applications should be accessible from.	 Guidelines and standards on accessibility to client devices to accompany the existing ISS4PS Style Guide version.

3.3 Infrastructure

Infrastructure is the foundation of the ISS4PS technical architecture. This section describes how a level of commonality and capacity will be achieved.

The following topics are covered:

- **Commonality**

  Describes the need for Force-wide commonality in infrastructure to deliver interoperable systems.

- **Communications Capability**

  Describes how the communications capability of the Police Service will be enhanced so that it has the capacity to cope with the increased demand.

- **Mobile Services**

  Details the support for mobile working and how the ISS4PS relates to the continually evolving mobile telephony market.

3.3.1 Commonality

Many Forces have implemented infrastructures according to their own local requirements and architectural approach. This diversity in architectures introduces design difficulties when implementing corporate solutions and common products, whether centrally or locally, resulting in costly implementations. Due to the scale of inequality between architectures it will not be practical to extend an identical infrastructure across all Forces. However, a minimum standard of common infrastructure is required to enable the deployment of corporate solutions.

Issues	Principle: Commonality
The differences in Force infrastructures has led to problems in implementing national solutions at a local level, problems in delivering national solutions from a central location and problems in providing a joined-up Police Service.	Police Forces and national programmes will standardise their infrastructures to the extent that central applications can be accessed in a standard way and corporate solutions can be implemented across all Forces.

Approach

The Police Service must agree on the extent of a common infrastructure and those technology products and processes that need to be adopted as standard. Obtaining an agreed set of standards will be an ongoing exercise and managed by the overall Technical Authority backed by the appropriate governance structure.

Focused studies are required where different products and standards are used. The Technical Authority will identify options and decide upon recommended product sets. Once a decision is reached it will be added to the set of target deliverables that the Forces must aim for as they migrate towards the ISS4PS standards.

Accepted standard products will be placed in the TRM, where they can be accessed by Forces implementing an ISS4PS-compliant infrastructure.

Technical standards will be placed in the ISS4PS SIB.

Action 9	Deliverable
PITO/NPIA and the Technical Authority will: Identify, agree, and implement minimum standards for Police Service infrastructure.	 A master list of common infrastructure products, standards and processes.

3.3.2 Communications Capability

There are a number of aspects of end-to-end delivery of data to users that are of concern:

- The local Force networks (WAN and LAN) need to have sufficient capacity to meet the increasing business requirements;
- The national network, currently provided by the Criminal Justice Exchange (CJX) also needs to have the capacity and flexibility to meet the increasing business requirements;
- The PNN2 contract currently provides a different level of communications capability to each Force.

It is not currently possible to distinguish the traffic type for particular applications with the CJX. As a result, high priority business critical traffic cannot be distinguished from non-critical, low priority traffic. In some cases, this has led to critical systems, such as, the National Firearms Licensing Management System (NFLMS) being denied service by traffic generated by public internet access. The Police Service infrastructure needs to be able to prioritise traffic based on attributes including application, type, source and destination.

Issues	Principle: Performance
The 2Mbps CJX connection that most Forces have in place just meets current bandwidth demands. Some projects have had to invest significant resource to work within this limit. Bandwidth locally and nationally will need to be significantly increased to keep pace with the expected rise in traffic resulting from joined-up working.	The Police Service will implement high performance, scalable, rugged and flexible networks that will meet a minimum set of standards.

Approach

It can be confidently predicted that there will be an increased demand for bandwidth with the introduction of the Global Data Store/Service (GDS). It is more difficult to predict the actual rate by which the traffic will increase. Changes in legislation, national objectives and advances in technology can all have an impact on bandwidth requirements with little or no notice. Current systems have limited flexibility to cope with unpredictable changes in traffic. This results in inconsistent performance across the Police Service.

A single network is required that can handle growing levels of traffic. It will also need to cater for an increasing number of different types of traffic, including intra-Force queries and multimedia documents. The network must be able to take account of the various performance standards that services and applications using the network must meet. The CJX will be unable to provide such a network in the medium to long term.

Over time, the percentage of inter-Force traffic will reduce as more requests are directed at the GDS. While the emphasis shifts towards centralised services, an IP network maintaining links between Forces will continue to meet the needs of the Police Service. Performance, flexibility and reliability are enhanced by the availability of multiple, high-capacity paths that link nodes within the IP inter-Force network.

The PNN2 national telecommunications network contract is due to expire in autumn 2006 and, at the time of writing, the procurement process for the new replacement PNN3 contract has begun. This contract needs to support the IP inter-Force communications approach, using modern networking technologies to deliver far greater flexibility, scalability and resilience than at present operating against clearly defined Service Level Agreements.

Forces will need to revisit their network strategy to ensure that the Force provided WAN does not become the bottleneck in the end-to-end delivery of system services. Forces with a network that cannot support the increased end-to-end delivery requirements in either the short or the long term will need to instigate a plan for improvement. PNN3 must offer Forces the option to contract part or all of their local WAN through the new contract. The degree to which Forces will wish to take advantage of this facility will depend largely on the incentives offered by the contract.

One problem facing Forces will be estimating the WAN bandwidths between sites that will be needed for the future. Bandwidth planning has always been a difficult exercise to conduct with accuracy and this situation is unlikely to improve given the number of unknowns as the systems migrate towards the ‘End Game’. For that reason Forces should ensure that any local network procurement plan is sufficiently agile that they can readily expand bandwidths across their estate to meet unexpected demand.

Increasingly there is a blurring between traditional voice-only telephony and data networks. However, the ISS4PS strategy recognises the need to support traditional telephony for some time to come whilst evaluating new tools and technologies and providing Forces with information on the benefits of moving towards these.

The strategy recognises the efficiency savings that can be made though infrastructure products, for example, Customer Relationship Management (CRM) for call centres as well as exploiting investments in network infrastructure for Voice-Over-Internet Protocol (VoIP) and Personal Computer PBX-based systems.

Action 10 and 11	Deliverable
10 PITO/NPIA will: Agree requirements and implement national network.	PNN3 National Network.
11 PITO/NPIA and Forces will: Agree requirements for Force networks, assess Force network against requirements and upgrade where necessary.	Force network assessments and Force networks upgraded.

3.3.3 Mobile Services

The use of mobile services has become more widespread with the availability of commercial cellular radio (GSM and GPRS) and 'closed user group radio carrier services' offered by the Police Service Airwave system. Several Police Forces have pioneered projects that have tested different approaches to mobile service provision. The Police Service must further develop this domain at a national level to ensure ICT supports officers in the fulfilment of their work.

Delivery of data, applications and voice to mobile devices requires an infrastructure that extends beyond the scope of 'land line' connectivity. The delivery of mobile information guarantees new capabilities with potential benefits in terms of efficiency and effectiveness for police business. It is likely to revolutionise the way front-line staff discharge their responsibilities, providing improvements in accessing systems and data that will empower them to make informed decisions in closer proximity to an event.

Issues	Principle: Mobility
Technology within the mobile service arena is developing rapidly both in terms of the mobile devices and the connection technologies. The ISS4PS architecture must provide the flexibility for new and developing technologies, support current technologies and leverage the investment already made.	The ISS4PS will support mobile working for the Police Service throughout the stepwise migration to the End-Game.

Approach

The ISS4PS will accommodate mobile access to applications across the mobile data bearer technology. Mobile service must be considered once the business needs have been identified. The mobile architecture is not dependent on the End-Game architecture. The strategy permits tactical interim integration solutions to legacy applications to coexist with the service-based approach of the End-Game.

A prioritised capability list of business requirements for mobile services has been published[17]. This identifies that solutions must cover:

- **On-line Query**

  The ability to search data held in police systems.

- **Remote Working**

  Having access to all desktop services while away from the office.

- **Off-line Working**

  The ability to create and analyse information while not connected to a fixed site such as preparing forensic drawings in a location where remote connectivity is not available.

The ISS4PS contains a pragmatic approach to supporting these differing operational needs and is cognisant of the ICT 'mixed economy' that will exist throughout the migration to the 'End Game'.

A high-level overview of the approach to mobile services within the ISS4PS is shown in Figure 8. The technologies detailed in this section are a representation of the likely delivery mechanism for mobile services. Connectivity may extend beyond the applications shown to include non-operational voice systems and back-office systems such as Human Resources and Finance.

Device

Forces recognise that there is no single mobile device to suit all modes of mobile working. For example, there are specific devices for Airwave communications. These when used in conjunction with other devices, fully meet the needs of mobile working.

Devices supporting off-line working will require software installed that is service-aware, enabling access to services that provide the business information needed.

17 PITO Mobile Information User Group, Mobile Information Business User Requirements (CM-MI-03-02), June 2005.

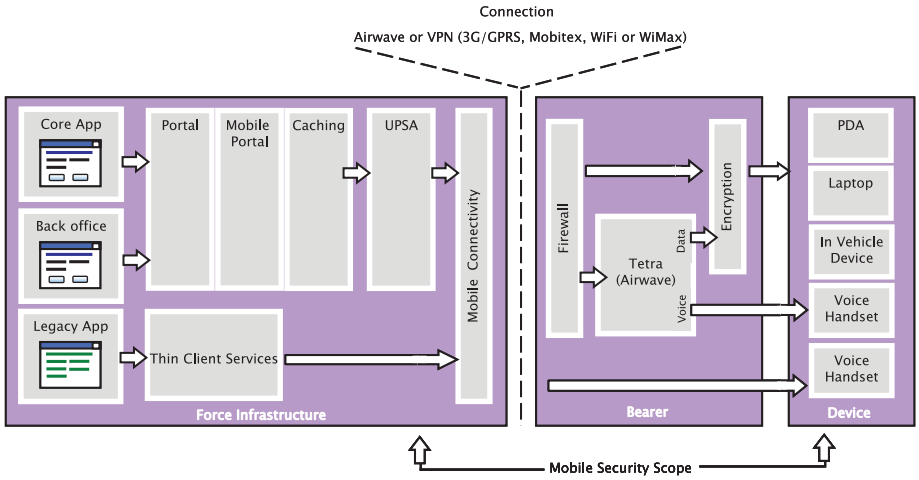

Figure 8 Mobile Architecture

Bearer

A bearer provides the mobile connectivity between Force data and mobile devices. The ISS4PS accepts that a combination of Airwave and other bearers may be required to meet all connectivity needs. Where appropriate, Airwave will be the bearer of choice for all voice and data services with other bearers providing non-Airwave device data services. All connectivity must meet the CSP and UPSA requirements.

Connection

The connection must provide secure wireless services, for example, Airwave, a Virtual Private Network over 3G/GPRS, Mobitex[18], Wi-Fi[19] or WiMax[20].

Force Infrastructure

The ISS4PS compliant applications must offer a service interface that permits data exchange between the mobile device and legacy application. The flexibility with portal technologies will maximise support for mobile technologies. Legacy application integration can be enabled using the ISS4PS compliant services, Citrix and Citrix Secure Gateway or specific mobile client code.

To support mobile working a Mobile Gateway is required that can provide the remote access and authentication services for the applications and bearers.

Mobile Security Scope

Airware is accredited to carry information up to and including RESTRICTED as defined in the GPMS. All data classified as RESTRICTED and above must be encrypted before transmission. Where data needs to be stored on a non-Airwave mobile device the storage media must support encryption and the data stored for the appropriate period of time to enable a piece of work to be completed.

Action 12, 13 and 14	Deliverable
12 PITO/NPIA will: Develop standards to be applied to the use of mobile information.	Standards for the use of mobile information.
13 PITO/NPIA will: Create and operate centre of expertise to provide expertise and guidance to forces on the use of mobile services.	Service to provide support and guidance to forces on the use of mobile services.
14 PITO/NPIA will: Develop technology demonstrators for proof of concept of proposed technology.	Technology demonstrators to form part of the technical reference model.

18 Mobitex is a wireless network architecture that specifies a framework for the fixed equipment necessary to support all the wireless terminals in a packed-switched radio-based communication system.
19 Wi-Fi (Wireless Fidelity) is a term covering wireless local area networks that use 802.11 family of specifications.
20 WiMAX is a wireless industry coalition whose members aim to advance the 802.16 standards for broadband wireless access (BWA) networks to support multimedia applications and wireless range up to 30 miles.

3.4 Information

The way that information is structured and stored needs to be standardised across the Police Service. This section explains what standards need to be applied and how these will be developed.

Topics covered are:

- **Structured Data Storage**

  This describes the Global Data Store/Service and relationships between data objects.

- **Unstructured and Semi-Structured Data Storage**

  Details how the Police Service is addressing unstructured and semi-structured data.

- **Data Quality**

  Explains the importance of data quality within the Police Service and how it will be improved.

- **Managing and Exchanging Legacy Data**

  Describes how data exchanged between systems, including legacy systems, will conform to common standards

3.4.1 Structured Data Storage

The ISS4PS End-Game has a single Global Data Store/Service (GDS) providing a master transactional data service for all data of national importance. Local copies of the GDS will be available as a Global Data Cache (GDC) that is synchronised with the centrally-held GDS.

The GDS is considered the most practical technical option to meet the goals of improved data management, quality and sharing at a national level. The need for change is universally recognised and there have been Force-led initiatives to improve data storage. Examples include the use of On-Line Transaction Processing (OLTP) integrated data stores, CRISP and Force data warehouses. The ISS4PS supports this investment in the piecemeal migration to the End-Game.

Issues	Principle: Consolidation
Moving to a single logical transactional data store is a significant change. The majority of data currently held is of varying degrees of CorDM compliance and held in application silos.	Forces will implement a Force-level federated data store as a stepping-stone to using a Global Data Store/ Service. A Global Data Store/Service will be used as a national data store for all core data within the Police Service.

Approach

There have been a number of advances in database and supporting technologies. These remove the barriers to globalisation of data, which make the GDS realistic and practical. These include:

- **Capacity**
  The size of databases from leading vendors can support millions of terabytes, well beyond the largest estimates for data within the Police Service.

- **Latency**
  To support for low latency data access ensures that transactional data is available to users in near 'real time'.

- **Capability**
  The necessary building blocks are available to create a physical data model for the GDS. The CorDM provides a logical data model for data within the Police Service. Initiatives, such as, CRISP are practical implementations of data models covering the major functional areas of the Forces.

- **Collaboration**
  Clustering and grid technologies to enable data to be distributed across several servers maximising the use of all resources. They provide scalability for the future.

The key enabler of the GDS is a physical implementation of the Police Service Corporate Data Model (CorDM). As part of the physical implementation process, the CorDM and CRISP data models will be brought together.

"A corporate data model is an enterprise-wide view of the data and its relationships. It normally includes a high-level model which is an overview of each subject data area and the relationships between them, as well as logical data models for each subject data area."

The GDS will be defined and a proof of concept developed as part of the work to be undertaken on the TRM.

The GDS, using CorDM compliant data, enables national visibility of data based around common police business activities. It supports each business function and delivers a joined-up environment supporting shared data. Figure 9, shows the importance of CorDM in delivering a structured solution with the GDS.

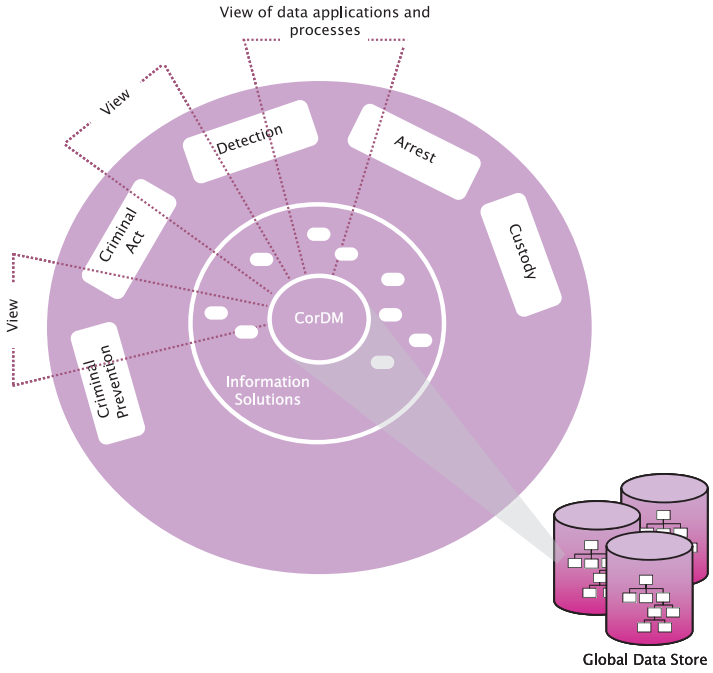

Figure 9 Delivering Structured Information Solutions with the GDS

Accessing data in the GDS must be controlled using a standard interface. A set of data access services will sit above the database providing the interface to the GDS. It will map from the CorDM based objects in the application area to the entities in the database. The Data Access Layer will provide a view onto the persistent data within the database enabling application developers to select the entities they need to work with and adapt them, where appropriate, within the constraints of CorDM. To support interoperability data must be exchanged using XML.

To operate this service successfully business rules will need to be defined on creation, update, and deletion from the GDS. For example:

- Services will require rules for data entry which will include the use of constrained values and the definition of mandatory fields for different business processes;
- Ownership and weeding rules will need to be defined. For example the rules will ensure there is one nominal record per person with the creator of the initial record as the owner. However, updated segments of the record may be owned by different organisations.

Figure 10 shows the relationships between applications and data.

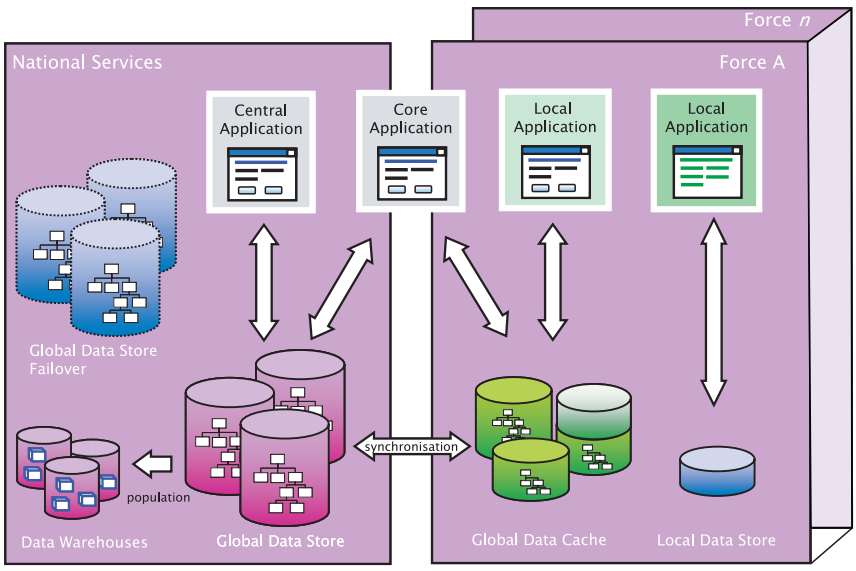

Figure 10 Structured Data Relationships with Applications

Central applications and centrally hosted core applications will access the GDS. Core applications that are deployed within a Force environment can access the GDS or GDC. Local applications will access local data and/or the GDC.

Global Data Store/Service

The GDS will be an On-Line Transactional Processing solution built around industry-strength COTS Relational Database Management System (RDBMS).

The results of detailed sizing estimates will lead to options being available for the chosen database, documents and multimedia items. The location of data could be held within the same database or could be held within separate linked database(s), for example, faster advanced text searching techniques or to apply specific types of processing for images or fingerprints. Whatever the approach, the GDS must provide the capability of searching across both structured and non-structured information. It also needs to provide a records management process for both data categories. The final decision about physical data location can be made once a full analysis of sizing has been carried out.

Data Warehouses

Affecting operational use of the GDS must be avoided. Intensive computing analysis must be executed against data warehouses populated from the GDS and optimised accordingly. This will support, for example, looking for crime patterns for intelligence purposes.

Global Data Store/Service Failover

The GDS is a critical part of the Police Service ICT infrastructure where performance and resilience is mandatory. The architecture must support a second instance of the GDS providing the disaster recovery capability for the main GDS.

Action 15, 16 and 17	Deliverable
15 Forces will: Implement federated data stores.	
16 PITO/NPIA and Technical Authority will: Define, agree and publish definitions of core data and begin to harmonise CRISP, CorDM and core data to define the physical data model for GDS.	A definition of Core Data, GDS data model and a populated and operational GDS.
17 PITO/NPIA will: Perform detailed technical analysis for the GDS, initiate procurement and begin to populate the GDS in conjunction with an existing major national programme.	

3.4.2 Unstructured and Semi-Structured Data Storage

Unstructured data represents information that is stored without strict rules or definition and requires human intervention to determine the meaning of the content. Unstructured data includes text documents, letters, presentations and faxes. Semi-structured data represents data that is contained in a mechanism capable of being stored in a database, such as, spreadsheets, web pages, e-mails, digital audio and digital video. Semi-structured data typically supports the concept of metadata to provide key information on the data source, such as, author and creation/update time.

Issues	Principle: Accessibility
Large amounts of information within the Police Service is held in a variety of unstructured, semi-structured, and incompatible formats complicating information exchange between Forces. It is often impossible to link related information held in different documents. Forces need a common language and document location mechanism to facilitate linking information.	The Police Service will implement intelligent services that provide unstructured and semi-structured data as a source of actionable, time-critical business intelligence.

Approach

The Strategy for Metadata and Related Taxonomies project (SMART) has already established a high-level 'helicopter view' as a basis for providing a single strategy for metadata within the Police Service underpinning a national standard for classifying information. Detailed taxonomies are needed to provide a practical catalogue to support information retrieval along with an ontology providing the associations between data.

As detailed taxonomies become available, systems can be built that take advantage of them to discover unstructured and semi-structured data, generate metadata for structured storage, classify data and provide sophisticated analysis capability.

There are a number of ways that Forces can initially handle unstructured and semi-structured data while taxonomies are being developed.

- **Document Management System (DMS)**
  Introducing a DMS that implements a file plan will enable a Force to bring together data from across the enterprise and store it in a searchable structure.

- **Discovery Systems**
  Generic search engine technology, together with specialised, data-specific retrieval mechanisms, for example for facial recognition, can be used to support human discovery and information processing.

- **Metadata Assisted Search**
  Metadata searching allows users to locate information by querying the metadata associated with electronic files.

Having data taxonomies in place will help to resolve issues of meaning in the Police Service and enable an enterprise-wide 'semantic web'[21] to be built. Currently in its infancy, the vision is that the 'semantic web' and its underlying technologies will allow unstructured data across the Police Service to be linked in a meaningful way.

Action 18	Deliverable
PITO/NPIA will: Develop a set of detailed taxonomies for the Police Service. Investigate how best the semantic web technologies can enhance the handling of unstructured/semi structured data.	Detailed taxonomies and guidance on implementing semantic web technologies.

21 The Semantic Web is an extension of the web where information is given well-defined meaning, better enabling computers and people to work together. Tim Berners-Lee et al, The Semantic Web, Scientific American, May 2001.

3.4.3 Data Quality

Data quality is fundamental to any information management strategy. Following clearly defined and common data quality standards ensures that accuracy, currency and relevance of information is maintained.

The Bichard Inquiry Report found that there was a lack of national guidance on record creation, retention, and deletion, with different Forces taking a separate approach to the definitions of 'review' and 'delete'. As a result, a new Code of Practice has been commissioned by NCPE[22] to provide guidance on these issues.

Issues	Principle: Quality
Lack of applying data standards in a consistent way has resulted in information being held in differing formats that is often duplicated and inconsistent within and across Forces. When information is brought together from several sources its value declines unless quality standards are applied. Research into data accuracy clearly identifies the need for cleansing and checking of data within the Police Service[23].	The new Code of Practice for Police Information Management will be used as the basis for continuous improvement in data quality.

Approach

Data quality standards will be defined for the Police Service. The Code of Practice for Police Information Management will be reviewed against the ISS4PS data quality criteria to further refine data quality standards for the ISS4PS.

An audit is required at the local and national level to determine any divergence from the standards, and an action plan developed to improve data quality.

The three focus areas for the data standards are shown in table 2.

Focus	Summary
Integrity	This covers the formal definition of comprehensive rules and the consistent application of those rules to ensure high integrity data.

Areas for consideration

1 Consistent Use of Constrained Values
The CorDM has identified an initial set of constrained values. These need to be reviewed and updated (where necessary) by the business.

2 Constraints for Data Types
Appropriate constraints to be made, for example, a check made that a postcode field conforms to the rules for valid UK postcodes rather than simply having data supplied.

3 The Use of Default Values

4 Data Structure Integrity Including Cardinality

5 Referential Integrity

6 Data Retention Integrity
Appropriate data retention policies need to specify how long a data item or set of related data items must be kept to prevent the loss of critical data through updates or deletion. This becomes particularly complex as we move towards the ISS4PS End-Game of an integrated data store where applications are sharing data objects.

7 Removing Redundant Data
There is a need to identify where redundant data exists and how it can be managed until it is possible to remove it from the data store.

22 The National Centre for Policing Excellence (NCPE) is part of Centrex, the Central Police Training and Development Authority, and was established in April 2003 under the Police Reform Act.

23 Several reports studying data accuracy have quoted data errors in excess of 80% between PNC and Force data. See the data audit carried out by the Metropolitan Police's Security Inspection Unit, 2002. the CRB PNC Data Accuracy Report 2001, and comments in the Bichard Report 2004.

Focus	Summary
Accuracy	This covers how the stored data represents the real world. To measure it the business needs to specify the accuracy needed for each business area and then compare the data against this.

Areas for consideration

8 Currency
How applicable and up to date as the data is compared with business requirements?

9 Origin
Where the data has originated from.

10 Precision
The level to which data needs recording.

Focus	Summary
Completeness	This covers whether the data being collected meets the business needs.

Areas for consideration

11 Coverage
Undertake a data resource survey to cover data needs and data availability on a local and national basis.

Table 6 Areas to be Covered in the Data Quality Standards

Establishing appropriate data quality management guidance is essential in creating a GDS built from the migrated PNC and Globalised Force data from phase 2 of the ISS4PS. Prior to migrating data a cleansing exercise is required and comparisons between all source data made to eliminate duplicates and provide links between related data. Part of the data quality procedure will require users on legacy applications to search against the GDS prior to adding data to reduce the occurrence of duplicates.

There is a legal need and added value for storing historical information within the Police Service. There is also a need to define links between two potentially related items of data, such as, pseudonyms for a person. The CorDM supports these needs, ensuring that potentially valuable intelligence information is not lost and any changes to data are recorded. To assist this, the business rules engine in the GDS will review each data record received and decide what action to take, such as, whether to create, merge, update or delete a data item in the GDS.

Unstructured and semi-structured data will be classified based on the standards delivered from the SMART project.

Action 19, 20 and 21	Deliverable
19 PITO/NPIA and Central Customer will: Define data quality standards for structured and unstructured data based on Code of Practice for Police Information Management.	A published set of data quality standards for structured data.
20 PITO/NPIA and Central Customer will: Define business rules for cleaning and matching of data to be input to the GDS.	Business rules and processes for data cleaning and matching for data to go into the GDS.
21 PITO/NPIA and Central Customer will: Perform a data quality audit at local and national level, and create local and national plans for improving data quality.	Audit report against quality standards at local and national level. Local and national plans for meeting quality standards.

3.4.4 Managing and Exchanging Legacy Data

Information collected within the Police Service is held in a variety of formats and systems in each Force making data sharing difficult. Increased mobility within society requires a more collaborative approach to sharing within the Police Service. Underpinning the capability to share data is the Police Service CorDM covering all of the operational business areas.

Standardising on information interchange increases the ability to share data throughout the Police Service. Successful data sharing relies on a common meaning, syntax, definition and delivery mechanism. Recent releases of the CorDM have provided Messaging Development Process and Standards based around a CorDM-compliant XML schema. This is an open standards approach for managing and exchanging data.

Issues	Principle: Interoperability
Much of the current data exchange within a Force is application specific and does not follow any specific standards for the data or transfer mechanisms, making information sharing unnecessarily difficult and slow to implement. There is a need to establish data sharing and interoperability standards with the legacy systems during the migration to the ISS4PS End-Game.	Data exchange and interoperability standards will be used throughout the Police Service based on open standards technologies.

Approach

A single standard is the most efficient way of establishing data exchange interfaces.

The CorDM provides this single standard and provides the baseline semantics for data entities used throughout the Police Service. CorDM defines each element in terms of:

- Its type, defined both in terms of its storage and its XML type.
- Its meaning, and where appropriate the valid values that it can take (Constrained Values).

These already have been, or are in the process of being developed as part of the CorXML project.

XML provides the common syntax for data exchange for the ISS4PS data exchange standards. The standards will exhibit the following characteristics:

- **Defined Rules for Content and Delivery**
  Managing fields and their structure.
- **Business Area Definitions**
  Support for namespaces and message schema for specific business areas as manageable self-contained units.
- **Extensibility**
  Support the capability to include elements from other government standards.
- **Transparent Mapping**
  The mapping and transformation of data items to CorDM is identified, allowing business specific names to be used as aliases to the generic CorDM names.
- **Constrained Value Filtering**
  Constrained values sets can be filtered to distil the lists down to the values necessary and appropriate to a specific business need.

The ISS4PS data sharing interoperability architecture will be achieved through integrated services, that are integrated using an Enterprise Service Bus (ESB) enabled product. Section 3.2.2 covers ESB in more detail.

Action 22	Deliverable
PITO/NPIA will: Define and implement the ISS4PS Data Exchange and Interoperability Standards as a superset of CorXML and the CRISP/CorDM harmonisation initiative.	ISS4PS Data Exchange and Interoperability Standards and a library of examples for police business areas.

3.5 Information Assurance

Police IS/ICT solutions are a significant component of the Critical National Infrastructure (CNI) within the UK. Services, such as, Airwave, PNC and the Police National Network (PNN) are relied upon to support operations. The ICT infrastructure and information assets within the Police Service face numerous threats, including inappropriate disclosure of intelligence, deletion or corruption and deliberate interruption[24].

This section describes how the Police Service will store, handle and transmit information in a secure manner.

- **ACPO/ACPOS Police Community Security Policy**

  Describes the importance of adopting the ACPO/ACPOS Community Security Policy (CSP).

- **Identity Management**

  Explains how a common approach will be adopted for managing the identity of police officers and staff when using information systems.

- **Proactive Management and Response**

  Describes how the Police Service can plan for security incidents/breaches so that the effects of them are minimised.

24 National Criminal Intelligence Service (NCIS) The Recording and Dissemination of Intelligence Material code of practice and the United Kingdom Threat Assessment Report highlight these issues.

3.5.1 ACPO/ACPOS Community Security Policy

Recognising the requirement for a national standard for Information Assurance, the ACPO/ACPOS Community Security Policy (CSP)[25] was ratified by ACPO Council in January 2003. It details the strategy for the security of information processes throughout the police community, and forms a framework for other subordinate policies. It explicitly cites standards of compliance, namely Her Majesty's Government (HMG) Manual of Protective Security (MoPS), BS7799 and Communications and Electronics Security Group (CESG) Information Security Standards.

The strategic aims of the CSP are to:

- Provide adequate and consistent protection for the information assets of member organisations;
- Comply with statutory requirements and meet ACPO/ACPOS expectations of the Police Service to manage information securely;
- Help assure HMG that Police service elements of the Critical National Infrastructure (CNI) are adequately protected;
- Facilitate effective participation with e-government strategies.

Issues	Principle: Security
With the emergence of joined-up systems across the Police Service, there will be a need to establish trust between Forces. This can only happen where there is a controlled, secure environment for information sharing across the Police Service. Higher levels of integration between Forces mean that threats to Forces are threats to the Police Service as a whole. As a result, Forces have a greater responsibility to maintain a coordinated effort in providing countermeasures to threats.	The Community Security Policy (CSP) will be implemented throughout the Police Service. As part of the CSP, a common security architecture will be adopted.

Approach

This global approach to security was one of the central recommendations of the original Valiant project from which a joint PITO/ACPO project was created to define the Unified Police Security Architecture (UPSA). The UPSA will provide a reference implementation of a sub-set of the policies within CSP. It will provide a federated approach for identity management, authentication and local and global directory facilities.

ACPO endorsed the definition of compliancy and a Compliancy Matrix for use with CSP. Forces will be able to claim compliance when the elements of compliance criteria have been considered, implemented as appropriate, and senior management have accepted any 'residual risk'. The ISS4PS is cognisant that this process continues to be the subject of systematic review due to changes that are likely to occur in the baseline standards. The target date for compliancy has been agreed by ACPO as 1st January 2006. Forces must review their current information security capabilities against the CSP and where necessary implement a plan to achieve compliancy.

The development of the UPSA will continue to provide common standards for implementing the CSP. It will provide a reference implementation for Forces.

Action 23	Deliverable
Forces and PITO/NPIA will: Forces and national services will implement the Community Security Policy by the end of 2005.	A compliancy matrix measuring compliance against the Common Security Architecture.

25 ACPO/ACPOS Information Systems Community Security Policy, February 2003

3.5.2 Identity Management

Information sharing across the Police Service is a strategic priority, but brings with it concerns about data security. The Police Service operates as a federation of organisations, where each Force is responsible for vetting, enrolling and managing staff. Forces and national services must therefore be satisfied that persons making requests for information are who they say they are, particularly when those requests arrive electronically from outside of the Force. It is vital that the Police Service develops a consistent and secure method of authenticating both the users themselves as well as requests for services and data received from users who may be from other Forces.

Issues	Principle: Identity
The Police Service does not have a consistent way of managing the identity of users across the Service. A lack of Information Assurance architecture has resulted in a plethora of usernames, accounts and user roles for a single user being stored in differing locations and directories.	A standard method of managing the digital identities and roles of police officers and staff will be implemented throughout the Police Service.

Approach

Maintaining separate silos of accounts and access permissions is an overhead nationally and within a single Force. Extending the current model across the entire Police Service is unrealistic. It would require every Force to manage accounts for every Police Service worker who may require access. The technical solution of federated identities (authentication and non-repudiation) and role-based access controls (authorisation) allows Forces to maintain information for their own users, and to share that information with other Forces. It is explicit in the design of the UPSA[26,27] and the report from the ITAG Role-Based Access Control Working Group[28]. Operational systems, such as, CRISP[29] also follow this approach and are currently implementing federated identities. Forces should consolidate their local directories to a single directory.

To establish Service-wide trust a federated identity approach based around common standards for managing identities and access rights to information systems needs to be adopted. The UPSA will identify the common set of security standards and products.

Within a federated environment, a central directory of staff information will be required to operate as an 'electronic phone book' for staff and departments. In addition, the directory will hold the digital certificates used to establish the access rights of staff using the ICT services. For the national directory to be of value, all Forces must provide details of their staff except those working in covert roles, who will be managed appropriately.

The authentication and role-based access required by trusted third party organisations will be handled in the same way as the federated identity approach advocated for the Police Service.

Action 24, 25 and 26	Deliverable
24 PITO/NPIA will: Implement tools and central infrastructure for managing digital identities and roles (currently within the UPSA project).	An identity and access management infrastructure based on standards.
25 Forces will: Consolidate local directories into an enterprise directory(ies). Implement the enterprise directory using the UPSA Police Schema for Directory Services.	A consolidation of Force directories to a manageable number.
26 PITO/NPIA and Forces will: Implement national 118 Directory.	The Police 118 Directory populated with details of staff from all Forces.

26 Unified Police Security Architecture, V4.00, Police Service ICT Security Working Group.
27 UPSA Outline Business Case, Central Customer, Dec. 2004.
28 National Role-based Authorisation Reference Model, 1.0, Jan. 2005.
29 Cross Region Information Sharing Project, Technical Architecture, CRISP/TA/1.0.

3.5.3 Proactive Monitoring and Response

A Service-wide view of security incidents, which covers applications, servers and services, enables a centrally coordinated approach to be taken and timely advice provided to individual Forces.

Issues

The Police Service will continue to be subject to directed, malicious attempts to exploit its information systems. This could, for example, take the form of a 'denial of service' attack on the critical infrastructure in conjunction with a terrorist act against an economic or civilian target. As part of the Critical National Infrastructure, the Police Service needs the means of detecting, and responding to, attacks on systems and networks. This needs to be automated wherever possible.

Having concluded that attacks on the Police Service are inevitable, the Service needs to plan how it will respond to those attacks. Plans and procedures need to be put in place. These will allow the Police Service to invoke the necessary actions, in a timely manner, to recover from successful attacks.

Principle: Protection

Methods of detecting and responding to attacks on systems and networks, IT service continuity facilities, and plans to respond to security incidents will be developed and implemented.

Approach

The Police Service Information Assurance architecture will provide countermeasures to attempts to compromise the reliability, integrity and availability of Police systems. The dynamic nature of the threats means that attacks can never be 100% prevented. Therefore, business critical systems require a comprehensive business continuity plan and service in place.

The Central Sponsor for Information Assurance (CSIA) sets out the HMG strategy in "A UK Government Strategy for Information Assurance." It ensures, amongst other things, that "Government has a core risk management capability to support public sector information assurance activity and to direct the national response to any systemic attack on our critical national infrastructure."

There will inevitably be an expectation from the public that the Police Service effectively manages the risk involved[30]. Consequently, Senior Information Risk Officers, will be required to assess their own department's status against a range of metrics on information assurance policy, risk, management and planning.

Police Forces can put other agencies at risk should they fail in the protection of their own networks and systems. In order to limit the impact of an attack, Forces must ensure that mechanisms are in place to record system events that will enable attacks to be identified and investigated. Protective monitoring may be taken as a managed service[31] to provide the necessary automated scanning of the logs and sensor data.

With monitoring in place, having a prepared and validated plan is necessary to guide response to an incident. The plan will begin from an assessment of the business impact of a system failure and address the cost/benefit of different approaches to providing continuity. The plan will also address when, in the interests of the community, the Force

30 "Protecting our information systems - working in partnership for a secure and resilient UK information infrastructure", Cabinet Office.
31 CESG InfoSec Memorandum "Intrusion Detection on Managed IT Systems", IM37 Issue 1.0 January 2005

should disconnect from the shared services. The plan should also address how to capture forensic information in order to investigate the source and cause of the incident and the business importance of doing forensic examination versus recovering the service.

Action 27, 28 and 29	Deliverable
27 Forces and PITO/NPIA will: Develop methods of detecting and responding to attacks on systems and networks, ICT service continuity facilities, and plans to respond to security incidents at both Force and national levels.	Protective monitoring scheme with alerting mechanism triggered when a possible attack is detected.
28 Forces and PITO/NPIA will: Develop and test response plans at Force and national levels.	Validate response plans.
29 PITO/NPIA will: Develop mechanisms for coordinating incidents to provide a Service-wide view of threats.	Agreed and validated plans for responding to an information assurance incident.

Section 4 Delivering ISS4PS

The previous section described the technical foundation underpinning the End-Game. This section moves the vision forward to detail how the End-Game will be delivered in a coordinated and controlled manner.

ISS4PS is a comprehensive strategy that cannot be delivered overnight.

Contents

4.1 Governance for ISS4PS Delivery

To facilitate the successful delivery of the End-Game the corporate level governance needs to be in place to enable a Technical Authority (TA)[32] to be established and operated effectively. The approach adopted for corporate level governance is to use a programme portfolio structure to bring coherence and control to the programmes that have a national impact. The Police Service must have a national view on priorities for IS/ICT work if it is to prevent the Service being pulled in different ways, leading to uncoordinated and wasted effort. Having a national view will enable Police Forces to plan effectively to meet local priorities while participating in national initiatives.

Issues	Principle: Consolidation
There is no overall management role to ensure coherence and compliance against an agreed benefits realisation plan for the enterprise and consequently a consistent technical architecture and strategy cannot be defined.	A programme portfolio approach supported by a TA role will be established to provide the technical leadership and coordination required to achieve a coherent and fit-for-purpose implementation of ISS4PS. The role will operate nationally and locally, at the enterprise, programme and project levels with support provided from a programme assurance office established at the enterprise level.
Requests for Police Force participation in national projects are not coordinated by the Police Service. This has resulted in conflicts over resource requirements. National projects are not always coordinated and this has led to Forces receiving an incoherent and conflicting set of actions from different projects. To enable Forces to plan for, and fully participate in, national initiatives, the Police Service needs to share information in a consistent and timely manner.	A Police National IS/ICT plan will be produced and maintained to coordinate and assist forces in supporting national initiatives. National Initiatives will participate in the production of the Police Service IS/ICT plan. This will be coordinated and assured by an enterprise programme assurance office. Police Forces will plan their local IS/ICT initiatives taking into account local priorities and national priorities as delineated in the police national IS/ICT plan. The Capability Plan will continue to be improved and be used as the basis for documenting national priorities.

32 The TA provides the leadership necessary to ensure that the global architecture remains cognisant of changes to business strategy and objectives.

Approach

4.1.1 Police National ICT Plan

The Capability Plan provides a mechanism for establishing national priorities and is a companion document to the ISS4PS. The Capability Plan meets some of the needs of the Police Service with regard to IS/ICT prioritisation. It is revised annually and continues to evolve.

To support the Capability Plan, the ISS4PS governance body needs to ensure that there is a Police National IS/ICT plan that feeds into the local Force planning cycle. This plan will need to cut across the core business themes and should be based on:

- The priorities in the Capability Plan that tie to the core business strategy for the Police Service;
- The strategy laid out in the ISS4PS.

The National Police ICT Plan should:

- Delineate the key points where Forces need to be involved in national initiatives, including key delivery dependencies, critical architectural changes, changes to business process, training, and an appropriate communications strategy;
- Estimate the total resource costs at a national and Force level, both in terms of IS/ICT and business involvement;
- Indicate the priorities defined in the enterprise portfolio so that Forces can add their local priorities in order to produce a consolidated action plan in line with national requirements;
- Avoid, or minimise, conflicting requirements through the realignment of the enterprise level benefits realisation plans.

The relationship between the Enterprise Portfolio, Capability Plan and National Police ICT Plan is shown in Figure 11.

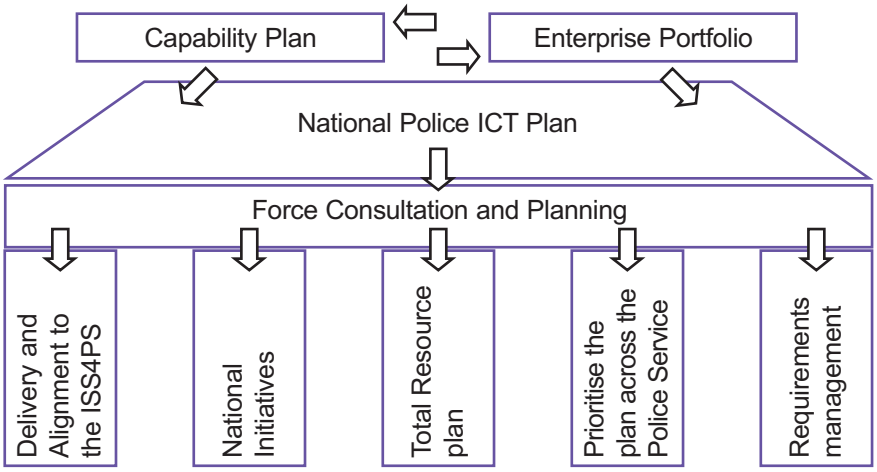

Figure 11 Relationships with the Enterprise Portfolio and Capability Plan

Police Forces typically have an annual planning cycle that defines budgets and resource usage. In order to be effective, the Police National IS/ICT plan, delivered as part of the enterprise portfolio[33] plan, must feed into the Forces' annual planning cycles to give them sufficient time to use the input to create local plans and assess their own portfolio of programmes and projects.

The Police National IS/ICT plan must be produced:

- In consultation with Forces.
- Reviewed on a regular basis.
- With sufficient time to feed into the local planning cycle.

The Capability Plan will be integrated into the work to establish the programme portfolio and set the overall priorities for the police service. The roles required to ensure the effective delivery of ISS4PS and the Police National IS/ICT plan are defined opposite.

33 Refer to Glossary for a description of the enterprise portfolio.

4.1.2 Technical Authority

The emphasis of volume 2 is on the delivery of the technical architecture to enable the successful delivery of the ISS4PS. Therefore, the TA role is developed in more detail. The TA will be deployed at different levels to ensure cohesion across all programme tiers.

The TA will be deployed:

- At the enterprise level – The Enterprise level Technical Authority (ELTA) will provide the assurance function required to maintain coherence across the whole enterprise portfolio.
- At the lower tiers – The TA will provide a proactive technical expertise and leadership role that is needed to create technical solutions that are "fit-for-purpose", taking into account the ISS4PS vision and policies.

The ELTA will be responsible for bringing together, from the various internal and external sources, the End-Game technical artefacts and processes defined in the National ICT Plan. The ELTA will ensure that the design of each artefact and process is consistent with the ISS4PS policies and standards, and is compatible with the supporting services and infrastructures. This role will encompass the consideration of the whole life cycle for a programme or project, including deployment, operations and ITIL-based support.

The ELTA will not mandate compliance, manage the programme, determine the business change or implement and roll out the solution. The ELTA will have the authority to determine the technical solution. The framework for compliance will be established at the enterprise level and all programme and project TAs will assure compliance against it.

The scope of the ISS4PS declares operation at enterprise, programme and project levels. The ELTA will need to operate at each of these levels. At each level the TA will report to the ELTA, programme and project-level executive respectively. Where a supplier organisation is involved, there will be a mirror role at the programme and project level that will be the Design Authority within the supplier organisation.

The overall coordination of the TA role will need to be taken into account to ensure that the most economical resources are deployed. The TA role at the programme and project level will form part of the normal resource plan developed to support each of the programme and project levels.

The TA governing body will be the ELTA and the standards and compliance metrics will be managed via the key ISS4PS architecture board as part of the overall programme portfolio. The intent is to ensure that all tiers comply with both the enterprise and local TA demands. It is suggested that for all supplier-led programmes and projects the TA role will be embedded in the supplier organisation as an assurance TA. This will provide the assurance required by the Enterprise that the capability delivered complies with the ISS4PS.

Enterprise Level

At the enterprise level the TA shall be appointed by the NPIA/ACPO. This role will lead the technical work to establish and define the ISS4PS and how it will be applied coherently in programmes and projects across the Police Service. This work will include the development of the framework and standards discussed in Section 3.
Each of the programmes or projects will require formal agreement of the ELTA (or appointed representative) before funding can be committed to a programme that will impact the ISS4PS approach. The formal agreement can involve the issue of an ISS4PS compliancy waiver. An essential role at the enterprise level is the design authority. The ELTA will need to confirm the overall design for all national level programmes and, as necessary, proactively advise national level SROs of issues that need to be addressed. In addition, approval of the overall safety case for the programme portfolio needs to occur. This will feed into the corporate level risk plan.

Programme Level

Programmes are collections of projects that must be coordinated to achieve a business change. Every programme should have a programme level TA to oversee the coherent technical solution across all constituent projects and to ensure that the programme and projects meet the enterprise technical requirements. The programme TA will work closely with the business architect to maintain coherence between the business needs and the technology capability to be delivered.

34 The ISS4PS architecture board is the overall accountable body responsible for architectural compliance to the ISS4PS, and maintains the service provision standards and compliance.

Project Level

The project TA will oversee the delivery of a coherent technical solution consistent with the ISS4PS at the project level. The TA is responsible for the technical solution that meets the business need and will work with the appropriate resources to achieve this goal.

4.1.3 Programme Assurance

To help coordinate the portfolio for Police Service IS/ICT there is a need for a Programme Assurance and support role. The enterprise-level support forms the core coordination and coherency level for all national level programmes and those programmes managed by Forces. The role is to provide the management and control mechanism for each of the programme levels. The role is not to manage the delivery but to provide a coherent enterprise-wide view across the programme. This is critical in maintaining coherency in the technical architecture and in the provision of a single view of the risk being taken by the Police Service in terms of its IS/ICT operation and developments. It is concerned with how best to control the business, technical and organisation change.

The SRO for each of the programmes will ultimately be responsible for the delivery of the programme. The escalation for each level will need to be defined and core risks and issues managed at the appropriate programme tier. Resource commitments will be prioritised against the portfolio and the delivery plan. The coherence needs to be managed by the programme assurance office on behalf of the overall accountable body for the delivery of the IS/ICT delivery plan. One area of consideration in the overall governance framework is a responsible owner for the delivery of the IS/ICT delivery plan. The Home Office will define this function as part of Policy 1.

The role of Programme Assurance is necessary to ensure the successful delivery of the ISS4PS and to provide proactive support to Force programmes. The role will need to work closely with the ELTA and nominated Business Change Lead operating at the enterprise level[35] to ensure coherence between business processes and expected Force wide strategy and direction. The key functions will need to include:

- Business Assurance.
- Technical Assurance.
- Programme Support.
- Configuration Management.

4.1.4 Configuration Management

Configuration Management is crucial to the management of the programme portfolio and assures that the right level of control is being taken at each of the programme tiers. This not only involves the implementation of new programmes but also the maintenance of existing in-service capability. To facilitate this activity the Technical Reference Model[36] will enable the TA to have a level of assurance that the changes being presented are not going to adversely impact the existing architecture or performance of the services being provided. The configuration management role will maintain the continuum between design, development, implementation and deployment. All of these must be coordinated to ensure that the performance and compliance to the ISS4PS is not adversely impacted.

4.1.5 Architecture Board

The ISS4PS Enterprise Architecture Board will be the vehicle for change control. An area that needs to be actively managed is the overall performance of the service. All programmes may impact performance and an assessment will need to be conducted to ensure that each of the programme deliverables does not adversely impact performance of the service. In line with performance the in-service supply for IS/ICT will need to be managed. It is assumed that each Force will retain a level of service management (otherwise a programme level support function will need to be developed). The local in-service function will assure that performance is managed effectively to deliver local SLAs/MOUs and any SLAs/MOUs that may span between Forces. This will provide a framework to manage the implementation of ITIL. All scope changes will be managed under configuration management to the framework established by the Enterprise Level Technical Authority (ELTA) and administered by the ISS4PS Architecture Board. The relationship between the ELTA, TA, and the Architecture Board is shown at Figure 12.

35 A Business Change Lead will operate at the enterprise level to ensure that the overall business requirements and benefits of the Police Service are being met by the delivery of the enterprise portfolio. This role may be a group role nominated by the NPIA or Home Office.
36 See section 3 for details on the Technical Reference Model.

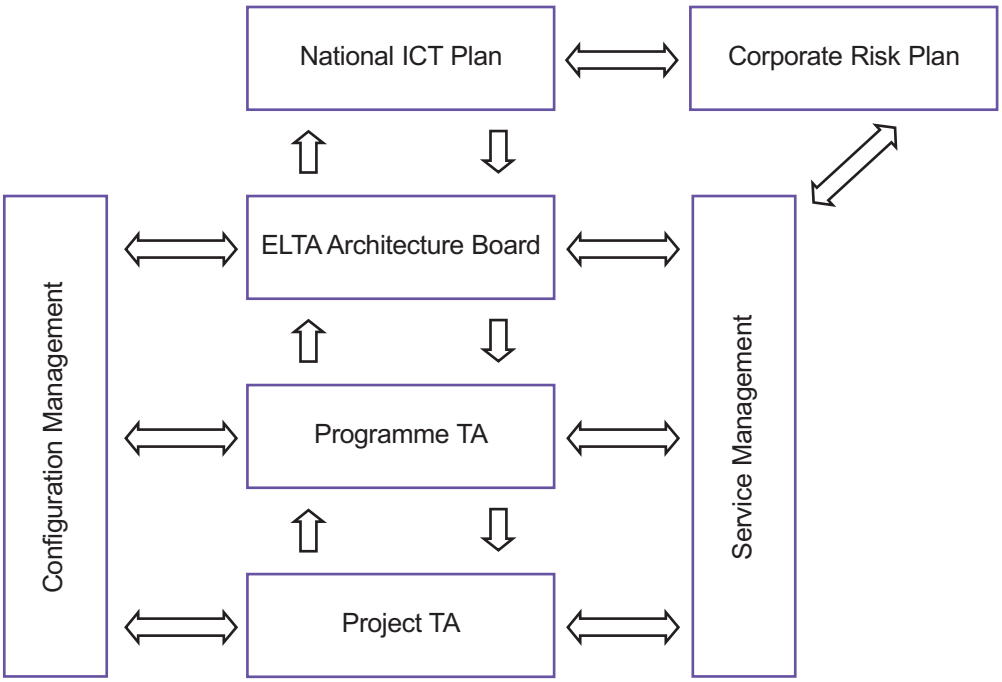

Figure 12 Relationship between the ELTA, TA, and the Architecture Board

The ELTA will have executive powers to overrule changes that can impact service delivery. Under normal conditions the ELTA will be advisory and the core implementation will be the responsibility of the programmes. Escalation paths will need to be available if any programme does not agree with a decision made by the Architecture board.

Actions 30-35	Deliverable
30 ACPO/NPIA will: Produce Police Service IS/ICT plan as part of the programme portfolio plan.	Police National IS/ICT Plan as part of the enterprise portfolio.
31 Forces will: Produce local IS/ICT plan that links to the Police Service IS/ICT plan.	
32 NPIA / Central Customer will: Produce Capability Plan as part of the overall police strategic plan.	
33 ACPO/NPIA will: Appoint a national level Programme Assurance function.	The Programme assurance structure to support all national programmes.
34 Programme Assurance will: Develop a process to ensure local resource priorities are identified and factored into the prioritisation of national programmes.	Resource management process that defines the prioritisation procedures for national and local programmes to enable the allocation of resources.
35 ACPO/NPIA will: Appoint an overarching ELTA role for the Enterprise and programme and project TA roles.	ISS4PS coordination and coherency framework produced.

4.2 Building ISS4PS-Conformant Systems

With an active governance framework in place, the approach for building ISS4PS-conformant systems can begin alongside alignment of the existing application architectures. Key to successfully achieving conformant systems is the adoption of a standardised technical architecture based on common standards and products to support interoperable information systems.

Issues	Principle: Auditable
Previous attempts to define conformance criteria for common standards and products have lacked the identification of who is responsible for establishing compliance, resulting in a subjective view of compliance criteria and thus products that do not truly conform.	Assessments will be made against a series of compliance checklists enabling results to be audited. The contents of the checklists will evolve over time allowing for inclusion of additional points both as technology matures and as assessments are made to encompass a feedback loop into the assessment process.

Approach

Both building conformant systems, and making an assessment of existing Force application architectures, are supported by the Technical Authority role. The Technical Authority (TA) role will both encompass corporate programme assurance for new applications, and provide tactical decisions for existing applications, with both being reported to the Enterprise Level Technical Authority (ELTA).

As the TRM is developed, the criteria for a particular system or product being conformant will be produced. One should not expect, therefore, an 'ISS4PS Conformance kite mark' that can be given to a product or system, since the criteria will evolve over time.

The conformance criteria depend on which point in time the evolution of the conformance criteria is at and also on the circumstances of the programme or project. Therefore, conformance to the ISS4PS is more of a gateway process for a programme or project rather than a kite mark for a specific product.

The responsibility for ensuring that conformance to the ISS4PS strategy is achieved stems from 'Policy 2: Securing Alignment across the Forces' and in 'Policy 3: Making National Programmes Accountable'.

To enable these assessments to take place, a series of compliance checklists are available in Annex C. While they represent the current thinking in terms of conformance, they will evolve over time to become more tangible and concrete. To aid in the assessment of both existing and future applications conformance levels have been defined in Annex C and these terms must be used to answer the questions that comprise the assessment.

The following products will be delivered with the aim of providing consistent assessment processes:

- Step-by-Step guides enabling key ISS4PS aspects for applications and environments to be recorded as compliant. These can be found in Annex C and will evolve over time.
- Tools will be provided to assess applications' compliance against the baseline ISS4PS architecture and SIB.

Action 36	Deliverable
PITO/NPIA and Technical Authority will: Develop and maintain conformance requirements for products and developments.	ISS4PS conformance criteria and assessment toolsets.

4.3 Owning the Full Life Cycle

Clearly identifying key parts of the lifecycle that the Police Service will own brings consistency to the delivery of programmes and projects in support of business improvements.

Currently there are many models of ownership throughout the Service. In some cases ownership is restricted to the specification, user acceptance testing and the intellectual property rights (IPR) of the system source code, in others a more encompassing ownership is held. To prevent interoperability lockout by vendors, ownership must extend to the potential reuse of functional areas within information systems to realise the architectural End-Game.

Issues	Principle: Ownership
Suppliers have a strong negotiating position as the Police Service does not own the knowledge of how their systems are constructed. Reuse is minimised as the Police Service does not have knowledge to define user components of applications, often resulting in crude data file exchanges to achieve interoperability.	The Police Service will take ownership of all key points in the life cycle.

Approach

Each part of the development life cycle must be considered separately. Successfully applying the ISS4PS requires the TA to manage and coordinate the following across all programmes and projects:

- **Requirements Specification**

  All Statement of Requirement must remain with the Police Service.

- **Architectural Design**

  The overall design must remain with the Police Service to maximise visibility and assessment for reuse.

- **System Testing**

  Testing of deliverables must be owned by the Police Service to ensure that solutions are integrated in accordance with the architecture and gain knowledge of how a solution works.

- **Acceptance Testing**

  Acceptance of the total solution must be owned by the Police Service.
  At the lower tiers the TA will provide a pro-active technical expertise and leadership role that is needed to create technical solutions that are “fit-for-purpose”, taking into account the ISS4PS vision and policies.

Action 37	Deliverable
The PITO/NPIA will: Develop guidelines as to how to retain ownership of these key points in the development life cycle, particularly when a third party is contracted to undertake development.	A coordinated approach to the adoption of standards that include the four elements of requirements specification, architectural design, system testing and acceptance testing for all programmes and projects.

4.4 Managing Suppliers

Within the life cycle it is important to identify how suppliers will be managed as the ISS4PS evolves. Forces largely have autonomy in the procurement of ICT products and services and their priorities reflecting local needs. Policy 6: Engaging with Industry states the need to develop a Service-wide approach to working with suppliers, enabling the collective power of the Police Service to require that products meet the architectural goals of the ISS4PS to deliver an effective and interoperable Service-wide ICT environment.

Issues	Principle: Supplier Engagement
Procurement autonomy prevents Service-wide best-value acquisition of products and less leverage over suppliers for the ISS4PS to achieve compliancy. It is not possible to mandate that suppliers provide products that are ISS4PS compliant, unless specifically commissioned.	The Police Service will act corporately in its dealings with suppliers in order to achieve value for money and drive industry into providing ISS4PS-compliant products.

Approach

A twin track approach will be taken to manage suppliers. Ultimately, the standards to be applied by Forces and nationally need to be defined. Procurement information will need to reflect the requirements to the ISS4PS compliance and the relevant sections applied to all ITTs.

Approach	Description
Short term	A standard set of criteria and standard weightings for the ISS4PS conformance will be used.
Long term	A single agency to coordinate procurement of products to drive the industry into providing the ISS4PS-compliant products to achieve greater value for money.

Table 7 ISS4PS Procurement Approach

There are three categories for products Commercial Off The Shelf (COTS) and Police Off The Shelf (POTS) and bespoke development. The approach taken for procuring each different type of product and bespoke software is different.

Type	Product type	Description
Bespoke	N/A	One-off software development designed to meet a specific set of Police Service requirements.
Product	COTS	COTS products designed to meet wider market needs than just the Police Service.
Product	POTS	Development designed for a specific Police Service need.

Table 8 Product Categorisation

ISS4PS compliancy is assessed in terms of how well a bespoke development, COTS or POTS product is aligned to the high-level architectural principles. From these principles compliancy guidance forms a series of evolving statements against which assessment will be made. The methodology for assessment must be standardised and well documented with a view to being able to provide an assessment of the ISS4PS compliancy areas.

By adopting a standard and published set of criteria, suppliers will be encouraged to move their products towards full compliance. This push towards compliant products will occur irrespective of whether the product in question is a bespoke development, POTS, or COTS procurement.

Establishing a single Procurement Authority with the responsibility and authority to procure key ICT products and services for the whole of the Police Service is impractical in the short term. However, a migration path that could lead to such an authority needs to be taken and should follow the path taken by other government departments that also operate in a decentralised way.

One of the issues that a Procurement Authority will need to tackle is one of trust. Police Forces will naturally be wary of such an organisation on the grounds that it may not procure in line with local strategies, it may not supply the value for money that local knowledge may be able to provide, and it may act slowly. Thus, the central Procurement Authority must be implemented gradually, learning the best way of doing things and gaining the trust of the Forces and suppliers. The Procurement Authority will need to demonstrate the following characteristics:

- Act efficiently.
- Demonstrably achieve value for money.
- Gain the trust of the Forces to act on their behalf.
- Enforce increasing compliance with the ISS4PS.
- Enforce government and police procurement rules.
- Be a communications channel to the suppliers.

Action 38	Deliverable
Home Office/NPIA will: Establish a Procurement Authority for all national IS/ICT procurement programmes, including terms of reference.	Procurement Authority established to provide best practice principles and guidance.

4.5 Integration

Existing systems within the Police Service do not, overall, comply with the principles of the ISS4PS. As ISS4PS infrastructure and applications are developed over the coming years, there will be a need to operate in a 'mixed economy' of applications that conform to the ISS4PS principles. The legacy systems that remain in service will need to be integrated wherever this provides a business advantage. How this integration is done depends on the type of application and the phase of the ISS4PS roadmap in which the integration occurs.

Issues	Principle: Leveraging Investment
A highly heterogeneous environment with a large number of tactical integration solutions complicates migration to the ISS4PS.	Integrating legacy systems with ISS4PS solutions is through application level integration using services, an Enterprise Service Bus (ESB), Federated Data Store and finally achieved in the Global Data Store/Service (GDS). Forces and national service providers should plan for a migration so that their systems become increasingly conformant with the ISS4PS.

Approach

The integration of legacy applications will require careful planning to identify whether the legacy applications can be replaced effectively by a core application. The planning will need to ensure that all aspects of integration are taken into account, including the connection to the ESB, access to the GDS and the business change aspects of integration.

Integrating Legacy Applications

Force systems are highly heterogeneous. Some systems are integrated and share data, while others are application silos with little or no integration. The degree of integration of these applications varies. From an ISS4PS point of view, practically all applications that currently run at the Force level are legacy. However, they are business critical, have no immediate replacements, and therefore must form part of the architecture going forward.

There is a need to run a 'mixed economy' consisting of both legacy and the ISS4PS services that interoperate at each stage of the migration process.

The mixed economy will operate in an environment in which the legacy implementations of the core services are replaced gradually by the ISS4PS-compliant applications, whilst the remaining legacy applications will be on a path of convergence to ISS4PS. Integrating legacy applications into the ISS4PS architecture will not be a simple task in view of the diversity of approach and the technologies with which the legacy applications have evolved.

The ISS4PS End-Game identifies the following preferred methods for integration:

- Application Integration.

  Where the legacy application forms part of a business process work flow, and where technically feasible, it will generally be appropriate to integrate using services through the ESB.

- Data Integration.

  Where there is data that must be shared, data integration can be achieved either through the data access services of the GDS or extracting data through an ETL process into the Federated Data Store.

  Legacy applications may be integrated using application integration or data integration or both.

Migration of legacy systems will be performed where there is a dependency on a national or local programme or there is an opportunistic benefit of performing the migration. Figure 13 illustrates the integration methods that will support the mixed economy and the ISS4PS 'End Game' at a Force level.

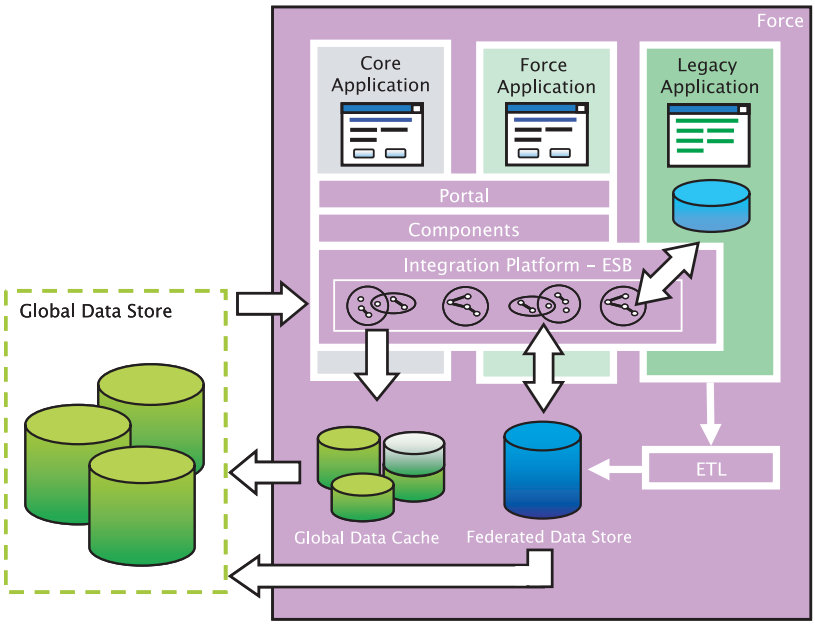

Figure 13 Force Level Integration Model for the Mixed Economy

There are different approaches to integration depending on the integration sets defined as follows

- Legacy applications with local data.
- Legacy applications with local and core data.
- Packaged applications/Integrated Data Stores.
- Data warehouses.

The ISS4PS approach for integrating each of these legacy types is different.

Legacy Applications with Local Data

Legacy applications with local data are those that contain data of local interest. There is no business requirement to warrant the provision at a national level. Therefore, to expose the data to other Forces is not required.

Where there is a need to integrate legacy applications or data with a core application the legacy application should be updated to use the new services from the relevant core application.

Legacy Applications with Local and Core Data

Legacy systems containing core data must expose this for compliancy with the ISS4PS. The three phases to the End-Game and their relationship with legacy applications with local and core data are:

- **Phase 1-2** supports an Extract, Transform and Load (ETL) interface to a local data store.
  The applications from which the data is required will require the development of ETL scripts to an integrated data store.

- **Phase 2** supports application interfaces to read/write from the GDS.
  Integration with the GDS will require changes to the application logic to use the data access services to access the database. Applications moving data to the GDS should also consider how much historical data will move and the data cleansed and translation required.

- **Phase 2-3** supports exposing CorDM compliant interface to search and retrieve from the GDS.
  The CorDM interface is based on XML messages.

- **Phase 3** supports applications reading and writing directly to the GDS.
  The ISS4PS End-Game supports the use of services and Business Process Management in a ServiceOriented Enterprise. This enables applications to be built from a composite of services accessed by legacy applications using a wrapper to bridge the technology gap between a service-based and legacy architecture.

Packaged Applications/Integrated Data Store

Where possible, packaged applications should be integrated in the same way as other legacy applications. However, it is recognised that the Police Service has less control over the integration points available to them through COTS and POTS products. It may also be the case that a COTS or POTS application covers more than one business process, making integration even more complex. It may be necessary to delay the integration of such applications until such time as it is economically and technically feasible, or simply to replace them once a more conformant product is available.

Data Warehouses

A number of Forces use a data warehouse approach for bringing together data from legacy applications for the purpose of tactical and strategic decision making. In the mixed economy, all core data will be available either through the GDS or local applications. Therefore, in the medium term the data warehouse will need to continue to exist until all core data is directly sent to the GDS.

A practical exception to this rule is where the local need is to combine data from both core and local applications, in which case it may be necessary to continue to pull data from local applications into a local data warehouse or data store.

Integration with Partners

The Police Service forms a key part of the wider community concerned with policing issues, which includes Government, private sector companies and partner organisations. Within Government, the Police Service needs to form part of a joined-up multi-agency approach to areas such as offender management and violent crime. The ISS4PS supports the multi-agency approach with defined principles of integration with partner organisations.

The current IT landscape of partners is varied. The range of IT solutions includes both custom-built and commercially available packages that need to exchange data. The ISS4PS provides the framework for integration with partner organisations. Services are provided and integrated using technologies such as Enterprise Service Bus (ESB) enabled products. See Section 3.2.2 for details on Service Integration. The ISS4PS ESB enables services to be discovered and used, primarily within the Police Service and, where appropriate, extended to trusted partners and organisations. These Services will hold the business and data transformation rules for other organisations to interoperate with the police systems. This ensures the Police Service controls the specification for all police data exchanged with partners.

The ISS4PS supports integration through the principles of:

- **Data Exchange Standards**
  Based on open industry standards of SOAP and XML, and the use of CorXML, will provide a standard for data exchange.

- **Shared Services**
  The service-based approach enables the Police Service to control the data exchange specifications for police information and provide services that can be shared across Government.

- **Security**
  A common security architecture implemented.

The ISS4PS takes a pragmatic approach to integration with partners. Where there are currently point-to-point integrations and an alternative can be achieved through the ESB, for example, data exchange between the PNC and DVLA, the ESB approach will be taken. Where integration exchanges already exist for defined workflows between partners, the ISS4PS will be able to integrate with them through the ESB, resulting in no (or only minimal changes) for partner agencies. Whilst this approach does include an additional level of indirection, it supports the ISS4PS principle of loose coupling and encapsulates knowledge of Police business rules, data transformations and security within the Police Service.

Migration Planning

Forces need to compile a migration plan for their legacy applications that need alignment with a national migration plan. When compiling the migration plan it needs to recognise that some legacy systems are still at the implementation stage.

The migration plan must:

- Identify the legacy applications that contain core data and any legacy applications that interface with these.
- For each application identify the area that will be modernised and the level of compliancy to be achieved.
- Identify the dependencies between the legacy applications.
- Show how the existing connectivity and interoperability will be maintained.
- How the proposed compliancy will be achieved, for example, functional decomposition and data integration.
- Check that multiple applications interface through an ESB.
- Check plan alignment with the overall national ISS4PS migration.

In addition to maintaining the national migration plan, there is an opportunity for identifying local cost savings by coordinating the changes that need to be made between Forces. For example, where several Forces have the same application, the cost of building an interface from it to the GDS could be delivered from a national perspective. PITO/NPIA should be proactive in managing and coordinating the local migration plans to achieve these cost benefits.

In addition to ICT, the change management requirements need to be considered, in particular training, recruitment and service migration. This is important even at the migration planning stage.

Action 39	Deliverable
PITO/NPIA and Forces will: Develop a migration plan that identifies when legacy applications and services will be provided using the ISS4PS approach.	A migration plan that defines when compliance to ISS4PS will be achieved.

4.6 National Planning for Convergence

Migration from individual Force systems and national services, such as, PNC, ViSOR and IDENT1 to the ISS4PS End-Game requires careful and coordinated planning. Achieving convergence without disrupting the day-to-day business activities is a major challenge.

The ISS4PS compliance of outsourced services such as IDENT1 is challenging, particularly in the area of shared infrastructure and services meeting service level agreements and opening up their architectures in a Service-based approach.

Issues	Principle: Supplier Modernisation
There is a danger that migration towards the ISS4PS End-Game could occur in a piecemeal fashion, each programme working towards an independent plan.	Migration progresses in a coordinated, controlled and non-disruptive manner and is documented in national and local migration plans that are continuously monitored and maintained.

Approach

All national services will be migrated towards the ISS4PS. The compliancy of each service and the plan for meeting this level of compliance will be set out in a national migration plan.

Services will be migrated either as part of on-going maintenance, where it is convenient and low cost, or opportunistically through a project where there is a need to integrate with other ISS4PS compliant services.

National and local migration plans will be produced to coordinate migration to the ISS4PS End-Game ensuring that there are no unexpected omissions. Plans will cover all aspects of migration including application, data, processes and training needs. All planning will be organic and continuously reviewed and updated during migration. The creation and maintenance of these plans is illustrated in Figure 14.

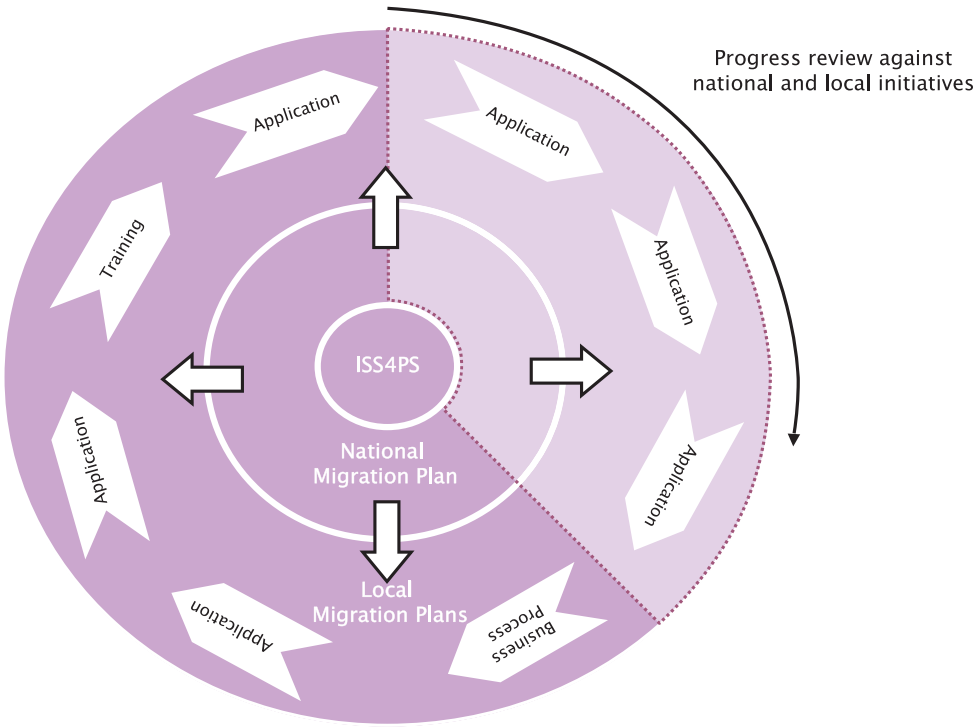

Figure 14 ISS4PS Migration Planning

Issues with outsourced services will be a concern, in particular with the way the ISS4PS architecture may affect a project's ability to meet Service Level Agreements, for example, using the GDS as the transactional data store and sharing CJX with other network traffic. The ISS4PS Technical Reference Implementation will enable performance analysis to be undertaken and Service Level Agreements reviewed.

Interfaces with other CJOs

All core data migrated to the GDS will be held in the CorDM format. Adapters will need to be developed to translate between CorDM and external CJO schema with integration being achieved through an ESB.This exercise has already been proven for a number of candidate schemas, for example, Libra, as part of the CorXML project. This exercise will need to be undertaken for each external interface which is not CorDM-compliant.

Action 40, 41 and 42	Deliverable
40 PITO/NPIA will: Include GDS in all modernisation programme plans.	A National Migration Plan that clearly identifies a practical roadmap to convergence at a national level supported by a GDS seeded with data from the national applications.
41 PITO/NPIA will: Develop and implement a migration plan for national services.	
42 PITO/NPIA will: Coordinate national and local migration plans with regular reviews of progress and comparison with national and local priorities.	

4.7 Service Management

Services delivered by the Police Service information systems must be managed to high standards. This section describes how the Police Service will base its service management on the best practice described by the Office of Government Commerce (OGC) Information Technology Infrastructure Library (ITIL). In 2002 the Police Service agreed, through the adoption of the ISS4PS version 2.0, to adopt a common approach to service management based on Information Technology Infrastructure Library (ITIL). Forces have moved independently towards this goal, with little coordination or coherence in their approaches.

Issues	Principle: Service Management
Force level autonomy has led to a disparate approach to service management. There are different levels of support for ITIL throughout the Police Service. The uncoordinated approach taken by the Police Service in adopting ITIL has resulted in there being no common processes or support tools available to assist Forces in implementing service management.	The Police Service will develop a consistent and holistic implementation of the ITIL framework.
As ICT throughout the Police Service becomes more integrated and inter-dependant, there is an increasing need for some ITIL disciplines to be applied at a Police Service level. Some Forces have already started to implement ITIL-based service management practices. In many cases, the order, and manner, in which the disciplines are being introduced is based on local priorities.	In order for the whole service management functions to remain cohesive, they will need to be integrated with those implemented at Force level. These functions need to be identified and an approach taken that will consider the interaction between the disciplines at various levels. The Police Service will coordinate a migration to ITIL, ensuring a consolidated approach is adopted.

Approach

4.7.1 Adopting a Common Approach to ITIL

ITIL is a United Kingdom government initiative providing a generic framework of best practices for IT service management. A public domain publication, it has become the de facto standard in scalable service management throughout the world.

It is widely accepted that organisations applying ITIL are able to plan and take control of IT reducing costs while delivering improved levels of service to their users. Successful adoption of ITIL requires the definition of the processes and tools that will be used to meet best practice.

BS15000 is a British standard whereby organisations that adopt ITIL can be independently audited to ensure that they have properly implemented ITIL best practice. It provides clear criteria to ensure that all the ITIL disciplines are properly implemented. Organisations can be measured against these criteria and gain BS15000 certification.

There are a number of tools designed specifically to support service management (the prevalent configuration management system within the Police Service is PVCS). This provides the benchmark against which any configuration management system is measured. There are a number of commercial tools supporting ITIL disciplines. These tools enable an automated approach to be implemented providing operational efficiencies that minimise errors, provide additional management information and highlight possible future problem areas.

It is becoming increasingly untenable to treat police ICT as a series of independent service providers – Forces, PITO and third party providers. The Police Service must now take a corporate view of service management.

Much of the service management responsibilities will have to be delegated to Forces or individual service providers. However, a holistic view of service management will require central coordination, providing central governance, common processes and common tools.

Service management within the Police Service is not yet mature enough to gain BS15000 certification. The value of gaining certification has not yet been assessed, nor is it appropriate to do so now. The Police Service needs to evaluate the advantages of achieving BS15000 certification at a time when the level of service management is more mature.

4.7.2 Implementing ITIL

ITIL consists of 11 different disciplines, split into two sections, Service Support and Service Delivery. Integration of these, at all levels, forms a cohesive service management capability.

Some of the ITIL disciplines are best implemented centrally by the Police Service as a whole. Whereas other disciplines are best implemented at the Force level, and for national services, by the service provider. Table 9 provides an initial view on where the focus of implementation should lie.

ITIL Set	ITIL Discipline	Force	Service Provider	Police Service
Service Support	Configuration Management			✔
	Change Management			✔
	Release Management			✔
	Problem Management			✔
	Incident Management	✔	✔	
	Service Desk	✔	✔	
Service Delivery	IT Continuity Management	✔	✔	
	Availability Management	✔	✔	
	Capacity Management	✔	✔	
	Service Level Management	✔	✔	
	IT Financial Management	✔	✔	

Table 9 ITIL Discipline Responsibilities

Though the processes and tools for a discipline may be delivered and coordinated at the Police Service level, the responsibility for performing many of the tasks relating to that discipline will still rest with each Force. For example, the Police Service will provide a national Configuration Management Database in which individual Forces will manage their own Configuration Items.

To ensure that there is a coherent approach to service management, a set of common standards and tools must be developed. These need to promote integration between the disciplines, regardless of whether they are implemented at Force or Police Service level, and between Forces.

Where disciplines are developed locally, Forces may take advantage of the economies of scale by grouping together to develop solutions. It is possible, for example, for a regional group of Forces to share a Service Desk and thereby reduce the overheads involved. Common standards and products for service management need to be in place for a federated approach to be viable.

4.7.3 Migration to ITIL

ITIL recognises that implementing all 11 service management disciplines simultaneously is impractical for most organisations. Even in ‘green field’ organisations, there will rarely be the financial resource or experience available to apply the whole of ITIL in one go. Introducing the disciplines in stages is a recognised practical approach to implementation.

The ITIL disciplines all rely on Configuration Management (CM) being in place. CM is therefore the key discipline that is required.

The first stage must be to run a project to establish the most effective and efficient way to operate service management in the Police Service, and to get agreement on any funding issues that arise. Following this, the migration can start.

It is impractical to introduce the ITIL disciplines all at once. Although the disciplines are all reliant on each other, there is a natural order in which they can be introduced.

- Introduce Configuration Management at a national level first.

- Other disciplines are naturally implemented singly or in pairs:
  - Change and Release management.
  - Problem and Incident management.
  - Service Desk.
  - Service Continuity and Availability management.
  - Capacity and Service Level management.

- Financial management for IT services is most naturally introduced after the other disciplines.

Forces and central services will find that they will need to change the way they already perform service management disciplines. Where they already have an integrated approach, there may be a period of disruption when they have to run on as a 'mixed economy'. This is one of the pitfalls of migration and it cannot be avoided.

Action 43, 44, 45, 46 and 47	Deliverable
43 PITO/NPIA will: Define and agree on the common approach to implement ITIL.	The Police Service will develop, implement and migrate to a consistent and holistic implementation of the ITIL framework.
44 PITO/NPIA will: Agree and procure common tools for implementing ITIL.	
45 PITO/NPIA will: Migrate Forces and Central services in concert to the agreed standard processes and tools.	
46 PITO/NPIA will: Identify the standards and products required.	A list of standards and recommended products to enable the Police Service to adopt a coherent approach to service management.
47 PITO/NPIA will: Appoint a central service management coordination authority.	A central service management coordination authority.

Section 5 Roadmap

This section describes a set of work streams that form the roadmap of activities that must taken place as part of the ISS4PS journey.

Contents

5.1 Roadmap

This section describes the deliverables required to meet the implementation requirements of the ISS4PS. It covers the three phases introduced in section 2.

Within each phase each deliverable has been categorised into five core work streams:

- Governance and Standards.
- Infrastructure.
- Core Data.
- Core Services.
- Legacy Integration & Migration.

5.2 Overview

Sections 2 and 3 explain the End-Game and provide guidance on the content of each of the core building blocks. Section 5 provides a roadmap for migration from the current situation as, described in Section 1.4 ‘As-Is’, to a compliant End-Game.

The complexity of managing whole programmes of work required to meet the ‘End Game’ should not be under estimated, it will require careful and coordinated planning by all Forces, PITO/NPIA, ACPO, Home Office, APA and stakeholder organisations. Commitment will be required by all parties if the ISS4PS is to be a success. The key to achieving the objectives of the ISS4PS is a feasible, clear roadmap to identify the tasks and the timescales that will need to be undertaken and, where feasible, show the responsible owner for ensuring that the deliverable is achieved.

Crucial to the development of a feasible roadmap is the indication of dependencies and the identification of how these will be managed. The deliverables shown on the roadmaps in this section have been derived from the actions identified in Sections 3 & 4 and additional deliverables required to ensure that a complete roadmap is defined.

The roadmap has been assembled based on the following planning principles:

- Identify clear milestones that map to the three phases for the End-Game as discussed in Section 2:
  - Phase 1 - Federating the data.
  - Phase 2 - Globalising the data.
  - Phase 3 - Globalising the architecture.
- Ensure the necessary building blocks and infrastructure are in place to support each of the above phases.
- Show the alignment of IMPACT implementation to the ISS4PS.
- Understand the need to maintain business continuity and minimise risks through the change process.
- Recognise the need for gradual change and migration to the ISS4PS.

The plan for achieving the End-Game is shown in Figure 15. It identifies the proposed work steams and shows the milestones that will be used to measure progress.

It is highly likely that strategic objectives will change during the progress of this plan due to the annual publication of the National Policing Plan and the Home Office Police Science and Technology Strategy.

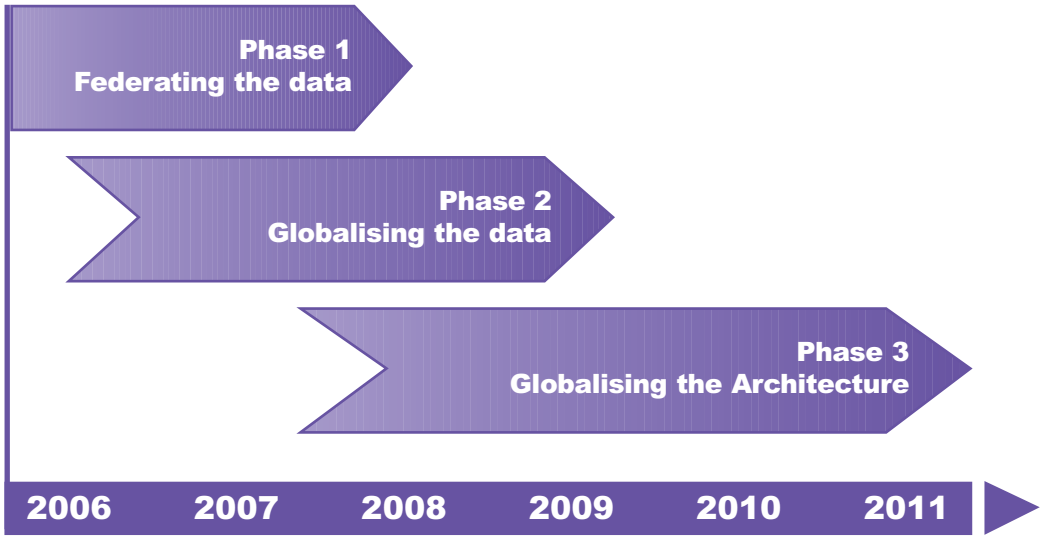

Figure 15 ISS4PS Delivery Overview

5.2.1 Work Streams

The work streams identified provide a context that group a number of actions and deliverables identified in Sections 3 and 4 into a plan. A summary explaining each of the work streams is given below.

Governance and Standards

This work stream covers the principle of establishing the framework for knowledge sharing for the ISS4PS and establishing the initial technical framework. Governance and standards work streams are expected to be in place by mid-2006. Thereafter, they will continue to operate throughout the life of the ISS4PS.

The main deliverables for this work stream are as follows:

- Governance structure;
- Technical knowledge created;
- Reference model and reference implementation created and in place;
- Establish the role of Technical Authority to oversee ISS4PS compliance.

Infrastructure

This work stream covers the update of the national and Force infrastructure to support the ISS4PS. The main deliverables for this work stream are as follows:

- Minimum network standards for Forces defined;
- The ISS4PS infrastructure products selected;
- Priority Force changes to meet the minimum requirements implemented.

Core Data

This work stream covers specification, procurement and implementation of the Global Data Store/Service (GDS) and the migration of core data.

The main deliverables for this work stream are as follows:

- Federated Data Store used to feed the GDS with core data currently held within legacy applications;
- PNC data migrated to the GDS;
- Current national systems migrated to use the GDS data layer.

Core Services

This work stream covers the specification, procurement and implementation and rollout of core services.

The main deliverables for this work stream are as follows:

- Core Service rolled out for intelligence delivered through IMPACT;
- Core applications rolled out and in use by Forces;
- Harmonised ITIL implementation.

Legacy Integration/Migration

This workstream covers the work necessary to effectively migrate the legacy applications from local forces to the ISS4PS defined core applications and services.

The main deliverables for this work stream are as follows:

- Local migration plans created;
- Legacy applications interfacing to CRISP;
- ESB capability implemented moving away from point-to-point integration;
- Legacy applications migrated into the ISS4PS. This will be an on-going activity driven by the local migration plans.

5.3 Summary of the Key Phases

Each phase has a set of key milestones. These are summarised below and can be used as the minimum number of review points for all programmes. Figure 16 shows the timeline for the key milestones and table 5 defines the key milestones for each of the phases.

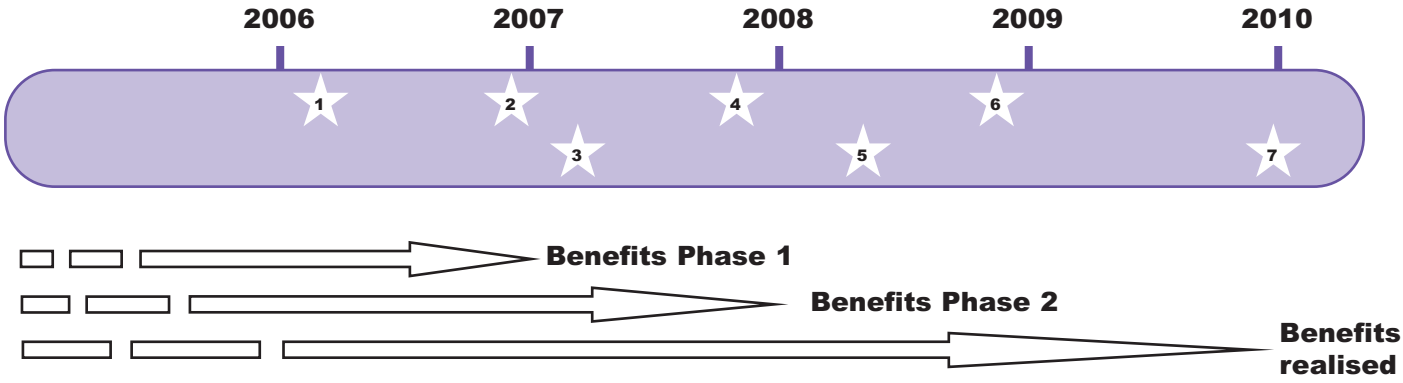

Figure 16 Timeline for delivering key ISS4PS milestones.

Phase	Phase name	Milestone	Milestone name
1	Federating the Data	1	TRM implemented for best practice delivery of service.
		2	National capability to access data across all forces.
2	Globalising the Data	3	GDS implemented.
		4	GDS populated with data from legacy applications.
		5	Data warehouse implemented where applicable.
3	Globalising the Architecture	6	ISS4PS intelligence application in service.
		7	All core services access the GDS as the primary data source.

Table 10 ISS4PS Milestones

Federating the Data

At the end of this phase updates will have been made to the Federated Data Store, which will be rolled out to the majority of Forces as an interim operational data store to collect data from legacy systems. There will be a national capability to access data from core legacy systems. Forces will have updated their infrastructure to meet the minimum level requirements ensuring sufficient bandwidth for the operation of the Federated Data Store and other national, centrally hosted, browser-based applications. The work on data standards and quality issues will provide a firm basis to start to improve data quality across the Forces.

The Technical Reference Model (TRM), its implementation and associated standards and studies will be complete, proving the feasibility of the approach, and providing a test-bed and best-practice example for delivery of the services. The technical reference implementation will provide the core business services and will shape the first ISS4PS compliant application to support Phase 2. Detailed plans will be in place for national and local migration. The ESB will provide the national integration capability.

Globalising the Data

Globalising the data consists of two main stages, building the GDS, and populating the GDS. This phase focuses on completing the implementation of the GDS, ready for data population, and the availability of the query and data load application to access the data. This phase builds on the migration of legacy data and will deliver the first ISS4PS compliant application to access the data via the data access layer.

The GDS will provide the first physical implementation of the CorDM. Data cleansing and mapping for PNC data will have been completed prior to the start of data migration to the GDS. The services offered by the PNC will have been wrapped and implemented on the GDS so that the GDS can provide these interfaces. The Federated Data Store (or local equivalent within a Force) will be feeding the GDS with data. The requirements for PNN3 will be fully understood and its implementation will be in progress, ready to provide the necessary bandwidth and performance as the GDS is populated.

At the end of this phase the GDS will be populated indirectly from legacy applications via the Federated Data Store and data migration from PNC to the GDS will be complete (although the PNC will continue to operate alongside the GDS as a contingency measure). In addition, the data exchange with CJOs, which is currently through the PNC, will be migrated to the GDS.

Globalising the Architecture

Globalising the Architecture phase consists of two main stages, implementing an ISS4PS-compliant Intelligence Application, and the move to a full set of core services.

At the end of this phase all of the major building blocks will be in place. The GDS will have become the master source of data on all objects, and all national and ISS4PS-compliant applications will use the GDS directly as their transactional data store. The development of the query and data load tools (delivered at the end of Phase 2) and intelligence applications will use and prove the common business services which will speed the development of the remaining ‘core’ services over the second stage of implementation.

A data warehouse built on the GDS and tools for performing sophisticated analysis of the data on a national level will be available. The remaining ISS4PS core service applications will be developed and their current data will be migrated to the GDS. As more ‘core’ services are available, the data being shared via the Federated Data Store will decrease until all core applications interface directly with the data access layer on the GDS.

5.4 Roadmap Context

There are a number of key national programmes and projects that are to be delivered within the proposed timescale for the realisation of the ISS4PS roadmap. From the point of view of ISS4PS it is useful to divide them into the following categories:

- ISS4PS-enabling programmes/projects.
- Ongoing national projects.
- New national projects.
- Other programmes within Criminal Justice.

The characteristics of each of these programme/project types and their relationship to the ISS4PS are discussed below.

5.4.1 ISS4PS-Enabling Programmes/Projects

ISS4PS Enabling Programmes/Projects are new or existing projects and programmes through which a sub-set of the ISS4PS functionality identified on the roadmap will be delivered. As such the ISS4PS is dependent on these programmes and projects.

Of all national programmes and projects, IMPACT will be the key enabler for ISS4PS and is aligned with it. It will be one of the first major programmes to deliver solutions that have been procured and managed through the full delivery process against the ISS4PS strategy.

The IMPACT programme is divided into five key releases; R1 IMPACT 2005, R2 IMPACT CRISP, R3 IMPACT Integration, R4 PNC refresh and R5 for which there are a number of strategic options. The roll-out of CRISP within R2 is aligned with CorDM, a deliverable of Phase 1 of the ISS4PS, realising the federated data store through CRISP or a CRISP equivalent data store. R2 is currently planned to be complete by the end of Q1 2007. In this timeframe the PNN3 programme will deliver the necessary national infrastructure to support the federated data store and the UPSA project will deliver the security component to support the common security model.

The strategic options for R5 of IMPACT due for delivery in Q1 2010 have been identified to be a national database, national intelligence system or a virtual information network. Of these options the national database would deliver the proposed Global Data Store/Service together with an intelligence application as one of the first core services.

5.4.2 Ongoing National Projects

There are a number of national projects which have recently rolled out or are due to roll-out within timeframes for Phase 1 and Phase 2 of the ISS4PS. Examples include locally hosted applications, such as, NSPIS Case and Custody and centrally hosted national applications, such as, the National Firearms Licensing Management System (NFLMS) and the Violent Offender and Sex Offender Register (ViSOR). There are also a number of planned releases for well-established national products, such as, HOLMES2 product with the release of V10, 11, 12 and 13 of the product.

National central applications are expected to have been migrated to the ISS4PS architecture by the end of Phase 2.

5.4.3 New National Projects

There are a number of new national programmes/projects which will be defined and procured during Phase 1 of the ISS4PS. Examples include the National Police Portal and Pentip. Where possible ISS4PS compliancy will be incorporated within the definition and procurement process to mitigate against the development of new legacy applications.

5.4.4 Other Programmes within Criminal Justice

The ISS4PS roadmap also needs to take into account programmes of work within the wider criminal justice community. The most relevant is the work being undertaken within CJIT in defining the architecture for the Criminal Justice System (CJS) Exchange Services. The CJIT IS strategy is also a SOA in which business services from CJOs are exposed through the CJS Exchange. The ISS4PS SOA enables the ISS4PS to be expanded to support the need for the Police Service to interoperate with the wider criminal justice community through the CJS Exchange.

5.5 Steps for Delivering Phase 1

Figure 17 at the back of the section shows the roadmap for Phase 1.

Work stream	Deliverable	Responsibility	Related Action[37]
Governance and Standards	**Enterprise Technical Authority established** To ensure the technical compliance for ISS4PS. This role provides the overall verification of the design and implementation of the ISS4PS solutions.	ACPO/NPIA	35
	Force Technical Authority established To ensure the technical compliance for ISS4PS. This role provides the local-level verification of the design and implementation of the ISS4PS solutions.	IT Directors/Chief Officers	35
	Procurement Authority established To provide guidance and procedures on how national procurement should be managed. This will include guidance for vendors and suppliers.	ACPO/NPIA Chief Constables and PITO	37
	ACPO/ACPOS Information Systems Community Security Policy implemented The national policy is required to ensure that all data and information are being managed consistently. This is a precursor to gaining data quality across the Police Service.	PITO/NPIA	23, 24, 27, 28, 29
	TRM and technical reference implementation for ISS4PS created Will provide a physical model and associated document set of the ISS4PS architecture model.	PITO/NPIA	3, 4, 14
	SIB for ISS4PS created The SIB will provide a series of standards that programmes need to comply with or use as guidance in delivering solutions for ISS4PS.	PITO/NPIA	2
	Portal for accessing SIB created This provides the distributed interface to the SIB for all Police Forces.	ACPO/NPIA	7
	National migration plan developed This provides the high-level overview of how each Force and Service will migrate to a federated data approach. It will include the development of a national IS/ICT plan. In addition, this plan will provide the key steps required to move into Phase 2 and the plan for implementing a GDS.	PITO/NPIA	39
	Enterprise architecture framework and tools selected The enterprise architecture framework is developed. The tools required to manage the enterprise architecture and ensure coherence and compliance will be in place. A view of the whole enterprise is required to ensure that an effective enterprise model can deliver the performance expected.	PITO/NPIA	1

37 The related action column shows the interdependency between the deliverable, actions and principles referred to in Annex F.

Work stream	Deliverable	Responsibility	Related Action
	ISS4PS compliance standards defined A complete list of compliance standards will be produced and integrated into procurement guidelines.	PITO/NPIA	19, 36
	Studies analysed To continue the development of ISS4PS to successfully achieve the End-Game, a number of studies will be required. These will provide the necessary information and subsequent activity to ensure successful implementation (first follow-on study is client devices for applications to accompany style guides). One of the first studies will be to establish the enterprise portfolio.	PITO/NPIA	8
Infrastructure	**Force architecture maturity assessed** Each Force architecture will need to be assessed against the standards defined by ISS4PS. This assessment will provide the vehicle for the delivery of the Force migration plan.	IT Directors/Chief Officers	9, 27
	Force network analysis completed All Force networks will be analysed to enable each Force infrastructure to be planned for migration to the common national infrastructure defined in ISS4PS.	IT Directors/Chief Officers	9, 27
	Force infrastructure complies with minimum standards This is the key enabler for migration. It provides the assurance that each Force is able to migrate towards ISS4PS.	IT Directors/Chief Officers and PITO/NPIA	9
	Infrastructure products identified Enables the product list for the infrastructure to be compiled based on lessons learned from programmes and industry best practice. A national network specification will be developed.	PITO/NPIA	12
	Implementation of common infrastructure products started As Forces begin to follow their own migration plans they will start to implement the common products suggested by ISS4PS.	PITO/NPIA and IT Directors	11, 12, 13
	National Service Bus selected and implemented Provides the means by which the national programmes and services can communicate across all Forces.	PITO/NPIA	11
	Application Architecture evaluated and an initial product specification defined The procurement specification produced.	PITO/NPIA	11
	PNN3 procured and service available The backbone to the provision of the infrastructure in place to enable the benefits of national services	PITO/NPIA	10

Work stream	Deliverable	Responsibility	Related Action
Core data	**Local data quality audit, Phase 1, completed** A review to identify the extent of the data improvement that is required to meet minimum standards and core data defined.	IT Directors/Chief Officers	12, 21, 27
	Tools for aligning data from PNC, INI and CRISP developed These are seen as three of the core systems to enable ISS4PS and all need to utilise the GDS as soon as possible.	PITO/NPIA	18
	PNC data mapped to CorDM A view of how PNC data is compliant or not with CorDM to identify the extent of work that may be required in PNC to bring the data up to minimum standards.	PITO/NPIA	16
	GDS defined, business rules agreed and supplier selected Core background procurement work carried out to ensure that the right supplier is selected to deliver the GDS.	PITO/NPIA and ACPO	15, 17
	CorDM Model upgraded This will be to v5 that will be used to ensure compliance across all programmes.	PITO/NPIA	16, 19, 36
	CRISP ISS4PS-compliant Core system to enable ISS4PS needs to align to ISS4PS to act as a benchmark for others.	CRISP SRO	16
	Federated Data Store implemented in majority of Forces (includes ETL) Provides the ability of local Forces to feed the national requirements. In addition the ETL tools will be in place and data quality improvement initiated.	PITO/NPIA, ACPO and IT Directors/ Chief Officers	15
Core services (applications)	**Core services specified** The services that will form the core set of applications will be defined and included within the ISS4PS core application list. This will enable programmes and projects to use the core service list to aid programme delivery.	PITO/NPIA	1, 25
	Data quality and load tools analysed Key tools to enable Phase 2 will be identified and a selection of tools short-listed for procurement.	PITO/NPIA and IT Directors/Chief Officers Service Directors	11
	Data models mapped to CorDM All data models will be mapped to the model defined by ISS4PS.		17
	ITIL iteration 1 complete The first phase of ITIL will be in place. This phase will be defined by the Service Authority role. A common approach defined for all Forces. This will also include the evaluation of ITIL management tools.	PITO/NPIA	43, 46, 47

Work stream	Deliverable	Responsibility	Related Action
	TRM implementation started The implementation of the TRM is an essential milestone to ensure that there is a reference model for future design and compliance evaluation. The TRM will evolve during Phase 2, however, this phase provides the first instance.	PITO/NPIA	4
	ISS4PS test suite developed The full specification for the test suite developed to include tools for compliance.	PITO/NPIA	5, 14
Legacy integration/ migration	**COTS/POTS products evaluated** The number of COTS/POTS products in service will be identified and analysed to see if any warrant the status of core applications or services.	PITO/NPIA, ACPO and IT Directors/ Chief Officers	18, 25
	Force IS/ICT strategies aligned to ISS4PS Each of the Force IS/ICT strategies will show the degree of alignment. As necessary each Force will align its strategy to ISS4PS. This will include an audit of current standards and, as necessary, begin to adopt ISS4PS standards.	IT Directors/Chief Officers	20
	Legacy applications identified A complete list of legacy applications will be compiled by each Force and coordinated by PITO/NPIA.	IT Directors/Chief Officers and PITO/NPIA	25, 26
	Local migration plans developed Each of the Force legacy systems will be assessed to determine the need to migrate and, as necessary, develop migration plans. These plans will be framed by the national migration plans.	IT Directors/Chief Officers	39
Capability delivered	• **Governance structure** • **Technical Authority function available** • **Procurement Authority function available** • **Core services defined** • **TRM and SIB available to all forces and suppliers** • **Force infrastructure compliant with minimum standards for ISS4PS** • **National Service Bus in place** • **PNN3 procurement complete** • **Federated data available for use** • **National and Force migration plans in place**		
Benefits beginning to be realised	• **Sharing information and services** • **Managing information** • **Empowering Police Officers and Staff** • **Deploying Common Services to Citizens**		

Table 11 Steps for delivering Phase 1

Federating the Data – Phase 1

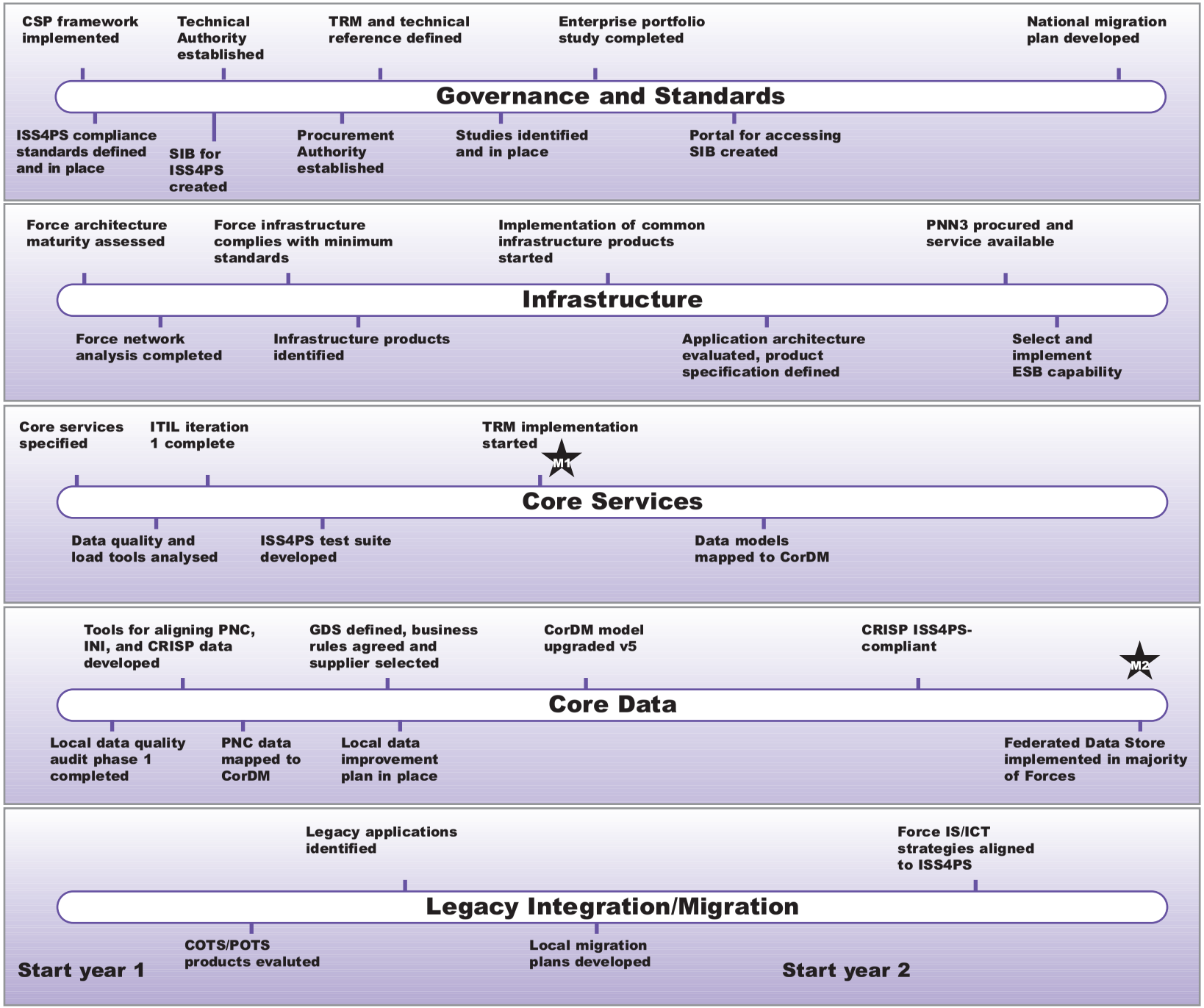

Figure 17 Roadmap for Phase 1

5.6 Steps for Delivering Phase 2

Figure 18 at the back of the section shows the roadmap for Phase 2.

Work stream	Deliverable	Responsibility	Related Action
Governance and standards	**ACPO/ACPOS Information Systems Community Security Policy compliance assessed** Force progress to adopting the CSP to be assessed to determine any national or local action plans.	IT Directors/Chief Officers	27, 28, 29
	National and local migration plans reviewed The migration plans developed in Phase 1 will need to be realigned to the live programme delivery milestones.	PITO/NPIA and Forces	39
	Common approach to ITIL implemented – Phase 2 All forces will need to have realigned their migration plans to achieving ITIL Phase 2 requirements. At this stage it is envisaged that each force in service support provider and local force providers are moving to achieve ITIL maturity as defined in the ITIL framework.	Forces	36, 43, 45
	TRM standards & procedures communicated The TRM was developed in Phase 1 however, in Phase 2 it is imperative that each force and each programme is able to utilise the TRM and implementation model to ensure alignment to ISS4PS.	PITO/NPIA	3, 4
	ISS4PS EAF populated and used Each force and new programme should now be using the EAF.	PITO/NPIA and IT Directors/Chief Officers	1
	National migration plan for Phase 2 implemented The agreed plan produced in Phase 1 is now active and being implemented and aligned to any remaining activity within Phase 1.	PITO/NPIA	40, 41, 42
	TA role compliance assessed in all programmes and projects All projects and programmes are now required to have a TA role that complies to the ELTA framework. All programmes and projects will be required to ensure compliance to ISS4PS.	Programme SROs	35
	Benefits of Phase 1 evaluated The partial benefits that will be delivered in Phase 1 will need to undergo a full review to ensure that the benefits are realistic moving into Phase 2 and are being delivered appropriately. They will feed the next phase of benefit review in Phase 3.	PITO/NPIA	Enabler

Work stream	Deliverable	Responsibility	Related Action
	Enterprise and local programme assurance functions in place The full establishment of an enterprise and local programme assurance function is in place at force and enterprise level. The programme assurance function will become the hub of activity for all levels and will provide the interdependency management required between national and Force-level programmes.	PITO/NPIA and Forces	33, 34, 47
	Core business process procedures and practices to align to the concept of GDS At the end of Phase 1 the data to support processes remains in essence the same. However, as we migrate to a GDS the issues of ownership within a process need to be aligned to the concept of a central data repository and service.	Forces and NPIA	20
Infrastructure	**Enterprise Service Bus products selected and starts to be used for integrating applications at the local level** Products identified for national and local use. Local use starts.	PITO/NPIA	6
	PNN3 available to support GDS Upgraded infrastructure is fully available at all levels.	PITO/NPIA	40
	Priority local infrastructure applications harmonised Those applications that have been defined as essential in terms of the business are harmonised. The lessons learned from this phase will be used to shape later activity.	IT Directors/Chief Officers and ELTA	25, 26
	Local force networks meet minimum defined standards. Start of the migration to common products This enables the migration to the full ISS4PS architecture. This deliverable occurs at the end of Phase 1 but is an essential precursor to Phase 2.	IT Directors/Chief Officers and Enterprise Programme Assurance	21
	Data warehouse designed & implemented This provides the physical and logical structure required to access data and information at national and local levels.	PITO/NPIA	27, 28, 29
Core data	**GDS implemented** The full GDS has been procured and the installation complete for use by all forces.	PITO/NPIA	17, 40
	Complete roll-out of federated data stores This is the catch-up activity from Phase 1 if required. It is expected that not all forces in Phase 1 will be fully compliant at the start of Phase 2.	IT Directors/Chief Officers	15, 16

Work stream	Deliverable	Responsibility	Related Action
	National applications updated to use GDS Transition from the federated approach begins with the national applications using the GDS instead of the federated data stores.	National programme SROs and service providers	40
	Data quality standards fully implemented All Forces and programmes have adopted the data standards and audited to confirm compliance.	IT Directors/Chief Officers and Enterprise Programme Assurance	18, 21
	PNC data cleansed and migrated to GDS Begins the migration of a core service to the GDS.	PNC supplier	17, 21, 22, 40
	ISS4PS test suite defined and in use by Forces and suppliers The procedures are in place for operating the test suite. All procurement contracts refer to the need for compliance and use of the test suite tools.	PITO/NPIA and IT Directors/Chief Officers	5, 14, 27,28, 29
Core services	**Query and data load application in place – first ISS4PS compliant application** Provides the mechanism for the use of the GDS by national applications and services.	PITO/NPIA	18
	PNC using the GDS PNC running in parallel with the GDS indicating the first national application use.	PNC Service provider	21, 22, 40
	Common tools for managing ITIL are procured and available Alignment of force ITIL tools can begin with the roll-out of common tools. Process and procedures to be aligned.	Service Authority	43, 44
	All suppliers comply with ISS4PS principles At this stage all new services and programmes will comply with ISS4PS. As necessary existing suppliers will be aligned.	Procurement Authority and Assurance teams	34, 37
	Standard set of components, services and business services defined and documented in service library This provides the source for all suppliers, IT Directors and procurement on the approved list for ISS4PS.	PITO/NPIA	7, 18, 22, 37
	Phase 2 of the reference implementation developed and in use The first phase of the TRM was developed in Phase 1. This assumes that during Phase 1 there was a reference model delivered to support Phase 2 implementation. This deliverable concerns itself with the development for Phase 3.	PITO/NPIA	4
	National and Force core service migration plans produced Force service migration plans linked to the national and local migration plans. This ensures that the service support is matched to the implementation of ISS4PS services.	PITO/NPIA and Forces	39

Work stream	Deliverable	Responsibility	Related Action
Legacy integration/ migration	**Local migration plans refined** With the review of the national plans, the local plans will need to reflect the changes, and vice versa.	IT Directors/Chief Officers	39, 40, 41, 42, 45
	GDS updated with core legacy application data Acts as the main step to Phase 3.	IT Directors/Chief Officers and PITO/NPIA	40
	New projects use the selected products as integral components to their designs The use of approved products ensures that the delivery of capability by future programmes and projects remains consistent with ISS4PS.	National, local programme SROs	37
	National applications aligned to use GDS Migration of national applications to use the GDS allows Phase 3 implementation to begin.	Suppliers, SROs, Enterprise Programme Assurance	39, 40
Capability delivered	• **GDS in place** • **Core data migrated to GDS** • **Core processes/applications defined** • **Compliance assessment of infrastructure and applications completed** • **Procurement aligned to ISS4PS**		
Benefits beginning to be realised	• **Shaping the future of Police IS/ICT** • **Common services to citizens** • **Adopting a common architecture** • **Coordinating service management**		
Benefits achieved	• **Empowered Police Officers and Staff** • **Improved Infrastructure Capability** • **Improved data integration and simplification – (a sub-benefit of Managing Information)**		

Table 12 Steps for delivering Phase 2.

Globalising the Data – Phase 2

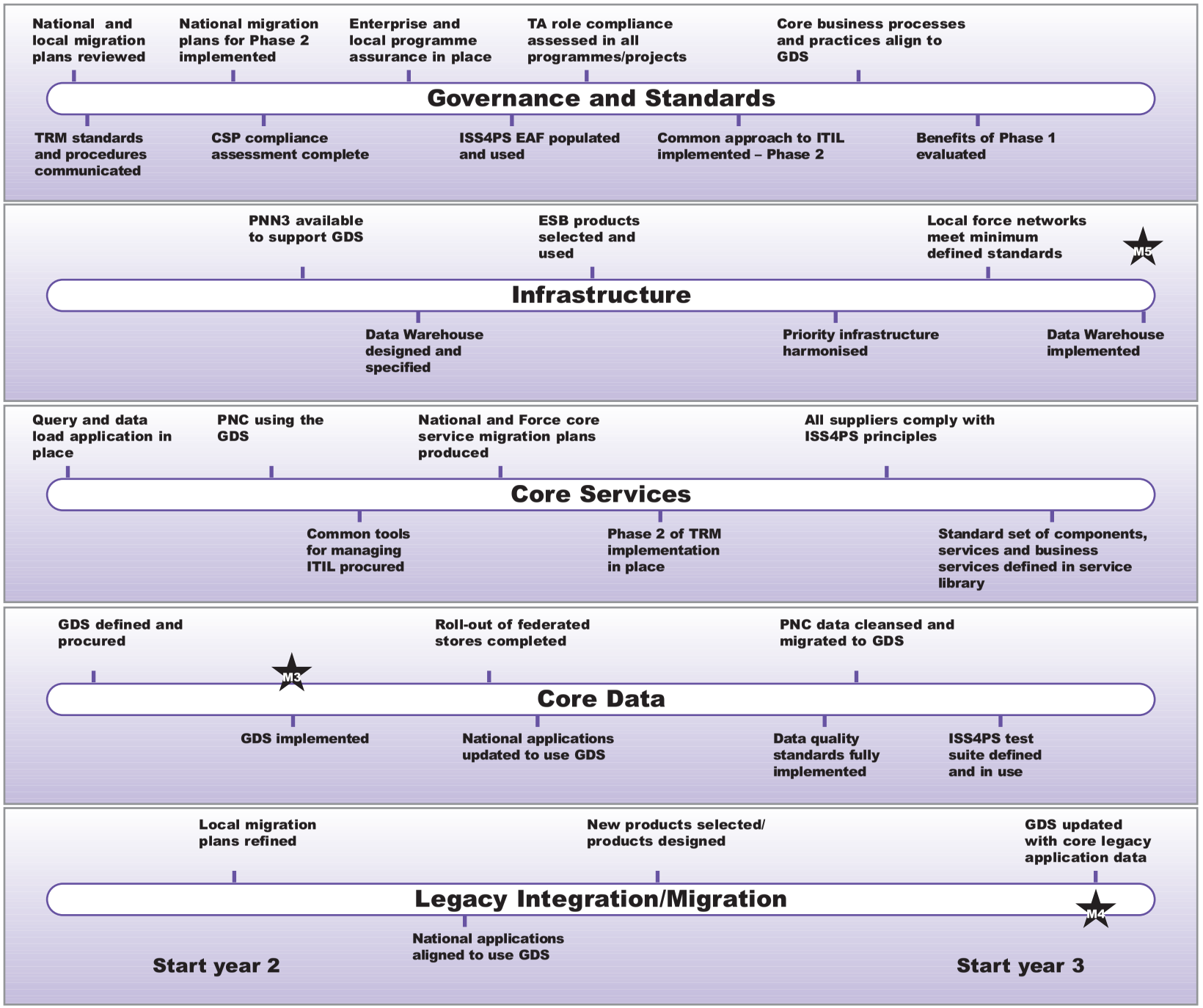

Figure 18 Roadmap for Phase 2

5.7 Steps for Delivering Phase 3

Figure 19 at the back of the section shows the roadmap for Phase 3.

Work stream	Deliverable	Responsibility	Related Action
Governance and standards	**Procurement standards aligned across the Police Service** Ensures that the procedures are consistent across the Police Service and explicitly define the approach to be taken with respect to ISS4PS.	Procurement authority	38
	Roles and responsibilities aligned to the new governance procedures Phase 1 and Phase 2 will begin to implement the critical roles. However, it is assumed that the roles will not be fully in place until the end of the NPIA shadow year.	NPIA and IT Directors/Chief Officers	41, 42
	Portfolio management process in place All programmes and projects are managed within a portfolio framework. This will introduce new financial processes defined by the NPIA. Without this it will be difficult to determine the complete investment profile.	NPIA and Enterprise Programme Assurance	31, 41, 42,
	Process and procedures in place to assess the benefits realisation The benefits will need to be tracked throughout Phase 3 and beyond to ensure that ISS4PS is delivering the expected outcomes.	ACPO/NPIA	39
	Audit the compliance to CSP at national and local levels Compliance to CSP will need to be assessed to determine core alignment to information security standards.	ACPO/NPIA	23
	Benefits of Phase 2 evaluated The benefits that will be delivered in Phase 2 will need to undergo a full review to ensure that the benefits are realistic moving into Phase 3 and are being delivered appropriately. This will feed the next phase of benefit review in Phase 3.	PITO/NPIA	Enabler
Infrastructure	**ISS4PS architecture fully in place** The move to the SOA defines a significant step in the implementation success of ISS4PS.	PITO/NPIA	39
	ESB provides the enabling mechanism for message transfer National and local use of the ESB is fully in place.	PITO/NPIA	6
	Full review of the ISS4PS architecture complete To ensure that the direction for ISS4PS still meets the business drivers, a formal assessment against best practice and the business strategy will be conducted.	NPIA	9, 30, 31 and 32

Work stream	Deliverable	Responsibility	Related Action
Core data	**Data fully aligned to CorDM** All programmes, projects, and services comply with CorDM, unless a waiver has been authorised by the ELTA. An audit of the whole portfolio will confirm this compliance.	ELTA and all Programme Assurance	18, 22
	PNC and GDS running in parallel To ensure that the PNC service is maintained during migration to the GDS, both services will operate in parallel.	Service Authority	40
	PNC parallel operation switched off When the business has assessed the risk and is content, the PNC will be switched off.	Service Authority	40
Core services	**GDS becomes the primary data store – minimal localisation of data** As the move to the GDS matures there will be less reliance on the need for localised data.	CRISP and GDS service provider	40
	All Forces align to ITIL The final progress to ITIL has been achieved.	Service Authority	43, 45, 46,
	Core applications available built using SOA constructs Identification, build and maintenance of a set of enterprise components services.	Programme SROs, ELTA and service providers	18
	ISS4PS-compliant intelligence applications implemented Intelligence applications provided to support unstructured and semi-structured data to meet the requirements of the business.	ACPO/NPIA	18
Legacy integration/ migration	**Legacy applications migrated to ISS4PS architecture** All legacy applications hold the data in the GDS. The GDS is now the master for all data in use across the Police Service.	ACPO/NPIA	39
	Force migration plans lead to harmonised infrastructure and core applications All forces comply with ISS4PS. The ELTA has total authority for the design of the enterprise services for the Police Service.	ACPO/NPIA	22, 32, 39, 41, 45
Capability delivered	• **Common architecture with standardised data and core applications** • **ISS4PS intelligence application in service** • **Data warehouse implemented** • **All core services access the GDS as the primary data source**		
Benefits achieved	• **All Phase 1 and Phase 2 benefits realised** • **Phase 3 benefits realised to the ACPO/NPIA metrics**		

Table 13 Steps for delivering Phase 3

Globalising the Architecture – Phase 3

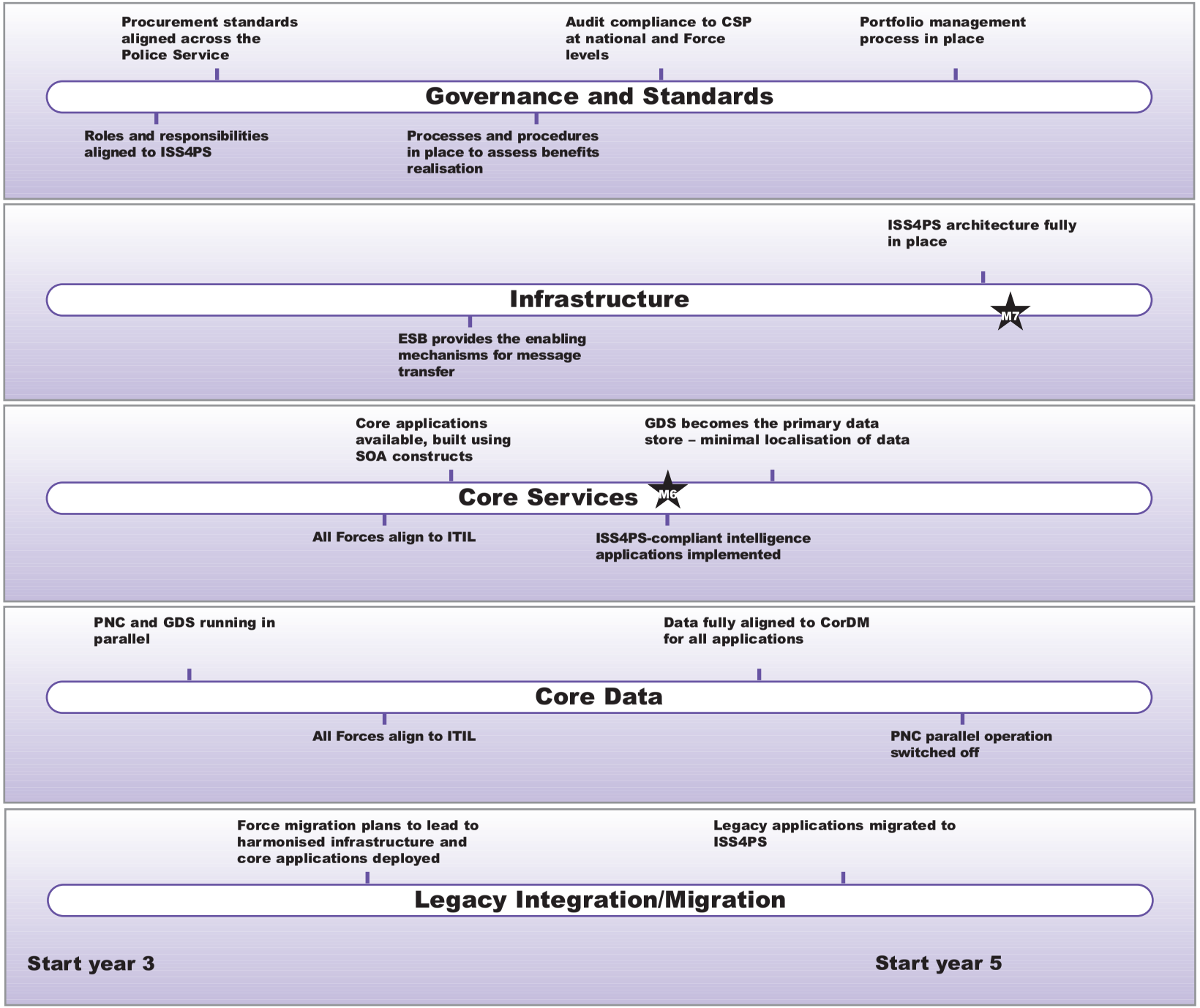

Figure 19 Roadmap for Phase 3

Glossary

0-9	
3G	3G is the term for third-generation wireless communications devices.
A	
ACPO	Association of Chief Police Officers of England, Wales and Northern Ireland – the professional body of chief police officers. Its core activity is developing policing policy.
ACPOS	Association of Chief Police Officers in Scotland.
Airwave	Airwave is a secure digital radio network dedicated for the exclusive use of the UK's emergency and public safety services.
ANPR	Automatic Number Plate Recognition is an intelligence-gathering tool. It works by capturing a Vehicle Registration Mark (VRM) as it passes a camera. This is then cross-checked against a number of national and local databases. ANPR enables officers to easily identify vehicles that are untaxed, uninsured and without a valid MOT certificate, and can assist in the removal of these vehicles from the roads.
APA	Association of Police Authorities.
Application Test Framework	Guides that document the testing methodology used to ensure that applications and architectures meet the ISS4PS compliancy requirements.
ASP	An Application Service Provider is a company that provides access over the Internet to applications and related services.
ATM	Asynchronous Transfer Mode.
B	
Browsers	The term used to describe applications that allow users to view and interact with Internet-based content or applications built using web technologies.
BPM	Business Process Management activities aim to make business processes more efficient. The Business Process Management Initiative (BPMI) promotes the standardization of common business processes, as a means of furthering e-business and business-to-business (B2B) development.
BPEL	Business Process Execution Language is an XML-based language designed to enable task sharing within a distributed computing environment realised using Web services. BPEL is also known as BPELWS or BPEL4WS.
Business Services	Business Services is a term used to describe how several services that are built from components, and are brought together to provide a reusable end-to-end business process.
C	
Capability Plan	The Capability Plan defines the priority of business requirements for the Police Service. It is issued annually by the Central Customer.
CBD	Component-Based Development is the term applied to software applications that are assembled from components that may be written in several different languages.
CBDI	CBDI Forum is an independent industry analyst and consultancy company. CBDI Forum provides a focus for the industry on best practice in business software creation, reuse and management, specialising in Service- and Component-based approaches, including Service-Oriented Architecture
CCTV	Closed Circuit Television is a television system in which signals are not publicly distributed.
Central Customer	Central Customer works with the Police Service to identify and prioritise operational and organisational business needs, and develop business cases for future IT solutions.
CJIT	Criminal Justice Information Technology.
CJX	The Criminal Justice Exchange is a network connecting more than a quarter of a million users across the Police Service and the wider criminal justice community.
Clustering	The use of multiple computers and storage devices to form a highly available system.

CNI	The Critical National Infrastructure refers to the systems that ensure the continuity of society in times of crisis.
COLIN	Common Object Linking in NSPIS. A project that illustrated the benefits of components in a phased technology migration.
Command & Control	Command and Control gives staff in police control rooms information to support decision making on how to handle incidents.
CorDM	The Corporate Data Model provides the Police with the controlled and consistent data environment needed for improved information sharing. The aim of this logical data model is to represent the structure and standards for all data of interest to the Police Service.
Core Applications	Core applications support core business processes, specific to the Police Service, for example, Command & Control, Crime, Custody and Intelligence.
Core Data	Core data are all data items that are of national interest.
CorXML	Corporate eXtensible Markup Language – XML schemas intended to validate data transfer between police data systems, ensuring adherence to CorDM data standards.
COTS	Commercial-Off-The-Shelf.
Chief Officer	The Chief Constable (senior police officer) in a Force.
Crime	A Crime application supports the business process of recording crime.
CRISP	Cross Regional Information Sharing Project. CRISP is a system that enables local and cross-regional searching of Forces' data.
Custody	A Custody application supports the business process of booking people into custody, keeping them there and dispatching them.

D

DSDM	Dynamic Systems Development Method is a framework focused on delivering high quality solutions using Rapid Application Development and addresses the need of management, developers and users.

E

e-GIF	The e-Governement Interoperability Framework is a collection of policies and standards to enable information to flow seamlessly across the public sector.
e-GMS	The e-Government Metadata Standard describes the way metadata should be structured. It is based on the internationally recognised Dublin Core system for describing information resources.
EAF	Enterprise Architecture Framework.
EAF4PS	Enterprise Architecture Framework for the Police Service.
EAI	Enterprise Application Integration refers to plans and methods to consolidate and coordinate applications. Provided as middleware that facilitates point-to-point application integration.
End Game	Is the goal that the Police Service is aiming to achieve as a result of implementing ISS4PS.
Enterprise Portfolio	An Enterprise Portfolio is a set of business-led improvement programmes that include an ICT element, providing an overview of the overall business investment.
ELTA	Enterprise Level Technical Authority. The ELTA provides the leadership necessary to ensure that the global architecture remains coherent and aligned with the Capability Plan and the Police National ICT Plan.
ETL	Extract, Transform and Load refers to three separate functions combined in a single tool. Firstly information is read and extracted from a data source. Secondly, the transform function converts the data into the desired state, and finally the load function uploads the transformed data to a target data store.
ESB	An Enterprise Service Bus (ESB) provides integration solutions for Service-Oriented Architectures.

F	
Force	One of the 43 Police Forces delivering policing across England and Wales plus the Police Service of Northern Ireland.
Fuzzy Matching	An algorithm used to search data for something that is a close match for the search criteria, as opposed to an exact match. Fuzzy matching is used for research and investigation pusposes.
G	
GDC	Global Data Cache. A local or regionalised copy of the GDS.
GDS	Global Data Store/Service. An integrated source of all Police Service data of national interest.
Governance	The structure, relationships and processes to direct and control programmes and projects in order to achieve the strategic goals while adding value and balancing risk.
GPMS	The Government Protective Marking Scheme is an agreed security classification system applicable for the creation, handling, and storage of information and other assets.
GPRS	General Packet Radio Services is a packet-based wireless communications service supporting Internet access from mobile devices.
GSM	Global System for Mobile communications is a digital telephony system.
H	
HR	Human Resources.
HTTP	Hyper Text Transfer Protocol provides the rules for transferring data on the World Wide Web.
I	
ICT	Information and Communication Technologies is a generic term used to describe the infrastructure that supports the transport and processing of information.
IDENT1	A platform to support broader identification capabilities including the national automated finger and palm print identification service.
IMPACT	Intelligence Management Prioritisation Analysis Co-ordination and Tasking. Supports the implementation of a National Intelligence Model.
Integrated Data	The term applied to data that is built around a common data model that supports several applications.
Intelligence	Information that has been subject to a defined evaluation in order to inform police decision-making, for example, to prioritise operations and identify links between crime and criminal behaviour.
IPR	Intellectual Property Rights is a catch-all term used to describe the legal status and protection that can be claimed for information and knowledge.
ITAG	Information Technology Advisory Group.
IS	Information Systems represent the applications that access data.
ITIL	The Information Technology Infrastructure Library is a set of best-practice standards for ICT service management.
ITSEC E3	Information Technology Security Evaluation Criteria form the basis where security features of IT systems and products are tested independently of suppliers to identify logical vulnerabilities. E3 represents an assurance level, one of seven. It requires the use of a defined testing procedure to verify compliance with design and against recognised standards.
L	
LAN	A Local Area Network is the term for a group of ICT equipment connected via a shared communications link within a small geographic area.
Location Migration Plan	A local migration plan is owned by the Force and shows the migration of the Force to meet ISS4PS.
Look-and-Feel	The term used to define how an application is presented to the user and behaves when used.

M	
MDA	Model Driven Architecture is the term used to define the development of applications in a platform-independent model of the business functionality.
Metadata	Metadata is data used to describe other data. Metadata is useful for describing information stored in data stores.
Mixed Economy	The operation of both legacy and ISS4PS services that interoperate at each stage of the migration process.
Mobile Gateway	The gateway between mobile devices and back office systems.
Mobitex	Mobitex is a packet-switched, narrowband network, designed for wide-area wireless data communications.
MOU	Memorandum of Understanding is a legal document describing an agreement between parties.
N	
National Migration Plan	The overall plan that defines the key migration stages to achieve ISS4PS alignment by Police Forces.
NCPE	The National Centre for Policing Excellence (NCPE) is part of Centrex, the Central Police Training and Development Authority, and was established in April 2003 under the Police Reform Act.
NFLMS	National Firearms Licensing Management System.
NNI	National Nominal Index. A searchable index enabling forces to check which force holds intelligence about an individual.
NPIA	National Policing Improvement Agency
NSPIS	The National Strategy for Police Information Systems. A range of information technology systems that aims to increase police effectiveness.
NVIS	National Video Identification System.
O	
OASIS	The Organisation for the Advancement of Structured Information is a non-profit making international consortium driving the development and convergence of e-business standards.
OLAP	Online analytical processing enables a user to selectively extract and view data from different points of view.
OLTP	Online Transaction Processing is the term describing the facility to manage transaction-based applications for data entry and retrieval.
Open Standards	The term used to describe non-proprietary standards.
P	
PBX	A Private Branch Exchange is a telephone system within an organisation that switches calls between users on local lines while allowing all users to share a certain number of external phone lines removing the need for individual telephone lines.
PentiP	Penalty Notice Project. A Penalty Notice System that supports the Government's aim of diverting more people from court by extending the use of Fixed Penalty Notices to a wider range of offences.
PITO	Police Information Technology Organisation. Responsible for the strategic development and delivery of ICT systems to the Police Service.
PNC	The Police National Computer is a nationally accessible store of data on people (such as criminals, wanted or missing persons), vehicles and stolen property.
PNN2	Police National Network 2
PNN3	Police National Network 3
Police Portal	The Police Portal, www.police.uk, provides web-based services to Police Forces, national organisations and the public. It allows the public to record crime incidents online as an alternative to reporting them at their local police station. It also enables Forces to publish localised information bulletins.

Police Technology Database	The Police Technology Database enables the police and criminal justice IT community to share information on science and technology projects and programmes that are underway within forces and criminal justice organisations, as well as solutions already deployed.
Portfolio Responsible Owner	The Portfolio Responsible Owner provides the strategic level guidance for all national programmes.
POTS	Police Off-The-Shelf is the term used to describe commercial packages that are Police Service specific.
Procurement Authority	The single responsible owner for the procurement of national police ICT products and services.
Programme Assurance and Support Office	Programme Assurance and Support Office provides the leadership and support that enables coordination and coherence between all national programmes.
Programme Level Technical Authority	The Programme Level Technical Authority provides the leadership necessary to ensure that national programmes deliver technical solutions that are aligned with the ISS4PS.
Project Level Technical Authority	Project level technical authority provides the leadership necessary to ensure that it delivers technical solutions that are aligned with the ISS4PS.
PVCS®	Professional Version Control Software. A COTS change management product from Serene Software.
R	
RDBMS	The term Relational Database Management System refers to relational database technologies and products.
RUP	Rational Unified Process is Information Systems development methodology.
S	
Service	A self-contained business function with a well-defined standards-based interface. Services do not depend upon the state of other functions or processes.
Service Authority	A Service Authority role provides leadership necessary to ensure a common holistic approach to service management.
Service Library	A documentation source of shared services describing what services are available, what they do and how to access them.
SIB	Standard Information Base.
SLA	Service Level Agreement.
SMART	Strategy for Metadata and Related Taxonomies
SOA	SOA represents an architecture based on reusable services, that are platform-independent. It provides flexibility that supports rapid business-led change.
SOAP	The Simple Object Access Protocol enables one program running on a specific platform to communicate with another running on a different platform by using HTTP and XML standards.
SPIS	Scottish Police Information Strategy.
SRO	A Senior Responsible Owner is the individual responsible for ensuring that a project or programme of change meets its objectives and delivers the projected benefits.
Style Guide	A Style Guide documents best practice standards for the development of application user interfaces in a consistent manner.
T	
TA	A Technical Authority role provides leadership necessary to ensure that the global architecture remains cognisant of the business strategy and objectives.
Technical Reference Implementation	A practical implementation of the technical reference model based on the standards defined in the SIB.
Technical Reference Model	The Technical Reference Model defines the End Game technical architecture.

TDA	Technical Design Authority.
Terabyte	A measure of computer storage of 2^{40} bytes (roughly one thousand gigabytes).
TOGAF	The Open Group Architecture Framework.
TRM	Technical Reference Model.

U

UML	The Unified Modelling Language is a standard notation for modelling real-world objects.
UPSA	The Unified Police Security Architecture is an information security architecture to provide technical information assurance for user authentication, mobile working, secure exchange of information and communication with external groups.

V

Valiant	The original Information System Strategy and the forerunner of the ISS4PS.
VoIP	Voice-Over-Internet Protocol provides a mechanism for sending voice calls over the internet using a software or hardware telephone.
VPN	A Virtual Private Network provides secure access to office resources via a public telecommunications infrastructure.

W

WAN	A Wide Area Network is a more geographically dispersed LAN.
Web Portal	A Web Portal is a website or service offering a broad array of resources from a single area. Resources can be widely distributed but appear to be local.
WiFi	Wireless Fidelity is a generic term for referring to any type of wireless network using the 802.11 protocols.
WiMax	WiMax provides wireless networking technology with greater speeds and range than WiFi technology.
Workflow	The term Workflow is used to describe, for each step in a business process, the tasks, procedural steps, organisations or people involved, required inputs, and outputs.

X

XML	eXtensible Mark-up Language is a flexible way to create common information formats to share both the format and semantics of data.

The ISS4PS is an ACPO Policy document, published on its behalf by:

The Police Information Technology Organisation (PITO)
ISS4PS Team
10th Floor
New King's Beam House
22 Upper Ground
London
SE1 9QY

Email: enquiries@iss4ps.police.uk
Internet: iss4ps.police.uk