Volume 2

Annexes

Contents

Annex A Standards

This annex establishes a list of standards to be used as the seed data for the ISS4PS Standards Information Base (SIB). It is not a definitive listing of standards that will appear in the SIB. Police Forces and national programmes should use this list as requirements for all new developments and procurements until the ISS4PS SIB is established. During Phase 1, the Technical Authority will have the task of approving the standards and including them in the SIB.

Contents

A.1 Sources

A number of sources have been used to define the initial set of standards: UK Government, the Police Service, the e-GIF Technical Standards Catalogue and Industry sources such as the TOGAF SIB.

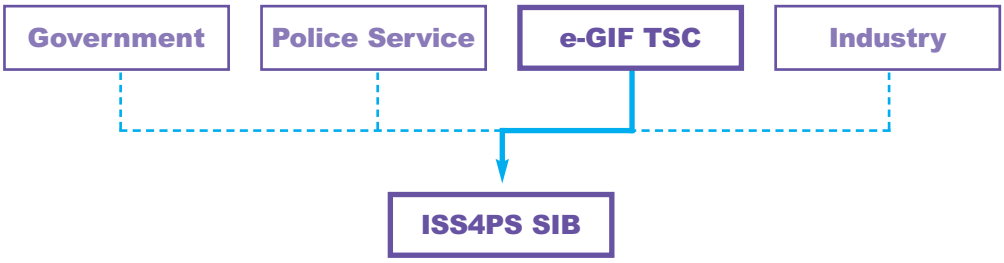


Figure A1 ISS4PS SIB Sources

The most significant source of standards is the Government's e-GIF Technical Standards Catalogue[2] as it will form the basis of the ISS4PS SIB. In general, standards adopted by e-GIF will be adopted by the ISS4PS for mandatory use within the Police Service. Each major release of the e-GIF Technical Standards Catalogue will be reviewed by the Technical Authority to ensure that exceptions to this rule are highlighted within the ISS4PS SIB. Other sources will be used to extend the e-GIF TSC and align it with Police business.

Each entry in the SIB will show the origin of the standard. The following are possible sources:

I	**Industry**	This includes standards bodies such as ISO, IETF, OASIS and W3C.
e-GIF	**The e-GIF Technical Standards Catalogue**	Based on version 6.2 of the Technical Standards Catalogue.
PS	**The Police Service**	
SG	**The ISS4PS Style Guide**	
Gov	**Government**	This includes legislation.
Int	**International**	This includes British and ISO Standards.
CPS	**The ACPO Community Security Policy**	

Table A1 ISS4PS SIB Source Origin

A.2 Status

Each standard within the SIB has associated with it a status that indicates where in the adoption process the standard currently is. Adopted standards will have gone through a rigorous process of review by the Technical Authority. Identifying this gives developers and architects a clear indication of whether or not a standard is fit for use.

The status levels used by the SIB will be those used by e-GIF with the addition of one further level: withdrawn. The levels are:

A	**Adopted**	The standard has completed the review process and has been adopted for use within the Police Service.
R	**Recommended**	This standard is of sufficient maturity and is being recommended for adoption by the Technical Authority.
U	**Under Review**	The standard is a candidate for inclusion in the SIB and is currently being reviewed.
F	**For Future Consideration**	An emerging standard that may be considered at some point in the future.
W	**Withdrawn**	A standard that is no longer part of the SIB but is maintained for historical reasons.

Table A2 Status levels for standards

2 http://www.govtalk.gov.uk/egif/contents.asp

A.3 Classification

The e-GIF Technical Standards Catalogue defines the minimum set of standards that conform to the e-GIF technical policies. The ISS4PS SIB will expand on this to provide a minimum set of standards for ISS4PS compliance, a set of recommended practices and additional guides to assist architects and developers. As a result, each standard within the SIB will be classified according to its use within its domain of applicability[3], specified in a Statement of Applicability. Each standard will be classified as one of the following:

M	**Mandatory**	The standard must be implemented to achieve conformance to the ISS4PS.
R	**Recommended Practice**	The standard is not required for conformance but there should be a strong argument as to why a different approach is taken.
G	**Guide**	There will be additional benefits gained by implementing the standard but it is not essential.
N	**None**	The standard is yet to be classified.

Table A3 Classification of Standards

The classification of a standard will be determined by the ISS4PS Technical Authority and may be subject to change as it progresses through the adoption process.

The standards tables have, in the absence of an ISS4PS Technical Reference Model, been organised using the structure of the Federal Enterprise Architecture Technical Reference Model[4]. It contains four Core Service Areas that are then further divided into Service Categories and Service Standards.

1 Component Framework

Business Logic
- Platform Dependent
- Platform Independent

Data Interchange
- Computer Graphics
- Data Exchange
- Digital Audio and Video
- XML Digital Signature
- XML Path Language

Presentation/Interface
- Content Rendering
- Static Display

Security
- Certificates/Digital Signature
- Supporting Security Services

2 Service Interface and Integration

Integration
- Middleware

Interface
- Service Description/Interface
- Service Discovery

Interoperability
- Data Format/Classification
- Data Types/Validation

Supporting Platforms
- Wireless/Mobile

3 Service Access and Delivery

Access Channels
- Collaboration Communications
- Other Electronic Channels

Service Requirements
- Service Management

Service Transport
- Service Transport

Supporting Network Services

4 Service Platform and Infrastructure

Database/Storage
- Storage

Hardware/Infrastructure
- RFID
- Video Conferencing
- Voice Communications

Software Engineering
- Modelling

Supporting Platforms
- Platform Dependent
- Platform Independent

3 For example, SQL only has application when working with relational database management systems and will not have application when developing an email system.

4 http://www.whitehouse.gov/omb/egov/a-6-trm.html

A.4 Component Framework Standards

Reference and Title	Summary	Source	Applicability	Classification	Status
Component Framework – Business Logic – Platform Dependent					
.NET Framework 1.1 Microsoft .NET Framework, Version 1.1	The Microsoft .NET platform.	I	All new .NET based development must be targeted at version 1.1. All products running on the .NET platform must run on version 1.1	A	M
.NET Framework 2.0 Microsoft .NET Framework, Version 2.0	The Microsoft .NET platform for the 2005 version of their development platform.	I	Greenfield .NET developments and those using SQL Server 2005 and Visual Studio 2005.	F	N
Component Framework – Business Logic – Platform Independent					
Business Process Execution Language for Web Services version 1.1	Business Process Execution Language for Web Services BPEL4WS as defined by the BEA, IBM, Microsoft, SAP AG and Siebel http://www-106.ibm.com/developer-works/library/ws-bpel/	e-GIF	BPEL4WS provides a platform independent means of describing business logic. It applies to all new integration style implementations. Integration type products should at least support import and export of BPEL4WS data.	A	M
WSBPEL 2.0 Web Services Business Process Execution Language	Next iteration of Business Process Execution Language for Web Services. Now under the control of OASIS. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsbpel	I	As for BPEL4WS, though support is currently not mandated.	F	N
ISO/IEC 23270:2003 ECMA-334 C# Language Specification	The C# programming language.	I	C# can be considered for any development project. The recommended platform would be the Microsoft .NET Framework. The mono platform will be investigated and may be an option in the future. Any development platform must conform to the standard.	A	M
JavaTM 2 Platform Standard Edition 5.0	The specification for the Java platform and language.	I	New projects should consider the use of Version 5.0 of the J2SE platform where support for it is provided by products.	R	N
J2SE 1.4.2 JavaTM 2 Platform Standard Edition 1.4.2	The specification for the Java platform and language.	I	The J2SE platform can be considered for any development project. Products based on the Java platform must support this version or greater.	A	M
J2EE 5.0 Java 2 Platform, Enterprise Edition (J2EE) 5.0	Standards for developing component-based multi-tier applications on the Java platform.	I	New projects should consider the use of Version 5.0 of J2EE where support for it is provided by products.	R	N

Component Framework – Business Logic – Platform Independent

J2EE 1.4 Java 2 Platform, Enterprise Edition 1.4	Standards for developing component-based multi-tier applications on the Java platform.	I	The J2EE platform can be considered for any enterprise development project. J2EE products must support this version or greater.	A	M
ISO/IEC 9899:1999 C	The C programming language.	I	C should be considered only where there is a defined need for a platform specific application or component (eg, device driver).	A	R
ISO/IEC 14882:2003 C++	The C++ programming language; an object-oriented version of C.	I	Consideration should be given first to C# or Java before selecting C++ for new projects, though it may be used where there is a specific requirement.	A	R
e-GIF TSC, Table 2 Web service choreography	An XML-based language that describes collaboration between parties that results in accomplishing a common business goal.	e-GIF	There is a choice of three standards for Web Service choreography, none of which has been ratified by the W3C. Thus, the current ISS4PS recommendation is the Web Services Choreography Description Language Version 1.0 which is currently at last call status.	F	R
e-GIF TSC, Table 2 WS-Coordination	Web Service Coordination.	e-GIF	This specification describes an extensible framework for providing protocols that coordinate the actions of distributed applications. Such coordination protocols are used to support a number of applications, including those that need to reach consistent agreement on the outcome of distributed activities.	U	R
e-GIF TSC, Table 2 WS-Business Activity	Web Services Business Activity Framework.	I	This specification provides the definition of the business activity coordination type that is to be used with the extensible coordination framework described in the WS-Coordination specification.	F	R
e-GIF TSC, Table 2 Business Collaboration	Business Process Modelling Language 1.1 and the Collaboration Protocol Profile.	e-GIF	Specifying business process behaviour for two or more partners interacting with the same business process.	F	R
e-GIF TSC, Table 6 Scripting	Standard ECMA-262 Scripting language.	e-GIF	Computer workstations.	A	M
e-GIF TSC, Table 6 Extended programming	Extended programming facility at the browser level.	e-GIF	When additional functionality needs to be provided to an application using browser-based delivery.	A	M
e-GIF TSC, Table 7 Scripting	ECMA 262 Script.	e-GIF	Channels other than computer workstations.	A	M

Reference and Title	Summary	Source	Applicability	Classification	Status
Component Framework – Data Interchange – Computer Graphics					
e-GIF TSC, Table 6 Graphical/still image information exchange specifications	JPG, GIF, PNG and TIF image formats.	e-GIF	For all static images.	A	M
e-GIF TSC, Table 6 Vector graphics	SVG image format.	e-GIF	For describing two-dimensional graphics within applications.	A	M
Component Framework – Data Interchange – Data Exchange					
XQuery 1.0 2005 XQuery 1.0: An XML Query Language	A language used for processing and evaluating XML data. http://www.w3.org/XML/Query	I	The standard is applicable in any situation where XML documents are queried or manipulated.	R	N
CorDM 5.0 Police Corporate Data Model, Version 4	Intended to cover all data within the Police Service, the Corporate Data Model is a significant part in enabling systems to be joined together.	PS	Any interface between systems. The data exchange format will be CorDM compliant. This ensures that data flowing between systems can be translated.	A	M
ePMF Police Metadata Framework	This framework is intended to be the definitive representation of the eGMS/PRO metadata standards for Police Forces. It also provides details of the encoding schemes to be used in the metadata framework.	PS	Any system where metadata is created for information sources or interfaces are developed for searching information sources.	A	M
e-GIF TSC, Table 2 Web service request delivery	SOAP v1.2	e-GIF	For determining delivery status of messages between two services.	A	M
e-GIF TSC, Table 2 Web services business repositories	ebXML Registry Services Specification 2.1 and XML Registry Information Model 2.1	e-GIF	To provide information describing the storage of data and operation of key services that are part of transactions with partners.	R	R
e-GIF TSC, Table 2 Web service basic interoperability profile	Basic Profile 1.0	e-GIF	To define a consistent instance of a Web service.	R	R
e-GIF TSC, Table 2 Web service attachments interoperability profile	Attachment Profile 1.0	e-GIF	For interoperability between solutions that require additional information in the form of attachments.	U	R

Component Framework – Data Interchange – Data Exchange

e-GIF TSC, Table 3 Data description language	Resource Description Framework (RDF) a language for representing information about resources in the World Wide Web.	e-GIF	For encoding, exchanging and reuse of structured metadata.	A	M
e-GIF TSC, Table 3 Ontology-based information exchange	Web Ontology Language Semantics and Abstract Syntax (OWL).	e-GIF	When extending the data description language to identify data for diverse sources and express data equivalences that appear different but are actually the same.	A	M
e-GIF TSC, Table 3 Data modelling exchange	XMI (XML Metadata Interchange), version 2.0.	e-GIF	For exchanging metadata information on data models enabling the models to be used by different modelling tools.	R	R
e-GIF TSC, Table 4 Metadata harvesting	Open Archives Initiative Protocol for Metadata Harvesting 2.0.	e-GIF	When consistency is required in exposing metadata, it is provided in an archive enabling services to be built using metadata from multiple sources.	U	R
e-GIF TSC, Table 4 Content syndication	Really Simple Syndication (RSS).	e-GIF	To support the publication of frequently changing data to a wide audience that is linked to additional information on selection.	A	M
e-GIF TSC, Table 4 Context-sensitive linking	The OpenURL is designed to enable the transfer of the metadata from the information service to a service component that can provide context-sensitive services for the transferred metadata.	e-GIF	When context sensitive events are required based on the data transferred.	A	M
e-GIF TSC, Table 4 Distributed searching	The standard specifies a client/server-based protocol for searching and retrieving information from remote databases.	e-GIF	Where users are required to search remote databases with an indication of the number of data matches returned and optionally a summary based on the users specified format.	A	M
e-GIF TSC, Table 6 Document file types	File formats that may be used provided they meet the technical policy for document handling defined in the e-GIF.	e-GIF	When maximum portability is required use of Rich Text Format (RTF), plain text files, hypertext (HTM) as appropriate. Use of Acrobat and Microsoft Word readers is also recommended.	A	M
e-GIF TSC, Table 6 Spreadsheet file types	File formats that may be used provided they meet the technical policy for document handling defined in the e-GIF.	e-GIF	When maximum portability is required use hypertext files, delimited files (CSV) as appropriate. Use of Microsoft Excel reader is also recommended.	A	M
e-GIF TSC, Table 6 Presentation file types	File formats that may be used provided they meet the technical policy for document handling defined in the e-GIF.	e-GIF	When maximum portability is required use hypertext files as appropriate. Use of Microsoft Powerpoint readers is also recommended.	A	M

e-GIF TSC, Table 6 Character sets and alphabets	UNICODE character encoding standards.	e-GIF	For maximum portability and support of diverse character sets.	A	M
e-GIF TSC, Table 6 General purpose files and compression	File types .zip, .gz, .tgz and .tar are permitted.	e-GIF	For all data, that requires compression.	A	M
e-GIF TSC, Table 7 Document file types	Plain/Formatted Text as (.txt) files and Hypertext documents as (.htm) files.	e-GIF	For communication channels such as PDAs, Smart Phones and kiosks.	A	M
e-GIF TSC, Table 7 Spreadsheet file types	Hypertext documents as (.htm) files.	e-GIF	For communication channels such as PDAs, Smart Phones and kiosks.	A	M
e-GIF TSC, Table 7 Presentation file types	Hypertext documents as (.htm) files.	e-GIF	For communication channels such as PDAs, Smart Phones and kiosks.	A	M
e-GIF TSC, Table 7 Character sets and alphabets	UNICODE character encoding standards.	e-GIF	For communication channels such as PDAs, Smart Phones and kiosks.	A	M
Component Framework – Data Interchange – Digital Audio & Video					
e-GIF TSC, Table 6 Moving image and audio/visual information exchange specifications	MPEG-1/ISO 11172	e-GIF	For capturing and storing moving pictures and audio up to 1.5 Mbit/s	A	M
e-GIF TSC, Table 6 Audio/video streaming data	Real Audio, Macromedia Shockwave, Windows Media and Apple Quicktime formats. Also wav and mp3 audio formats.	e-GIF	When streaming audio and video data to applications for display upon request.	A	M
e-GIF TSC, Table 6 Animation	Macromedia Flash, Apple Quicktime.	e-GIF	When required to provide moving images within applications.	A	M
Component Framework – Data Interchange – XML Digital Signature					
e-GIF TSC, Table 3 XML signatures	XML-Signature Syntax and Processing.	e-GIF	When required to provide confirmation of integrity, data authentication and signatory authentication.	A	M
e-GIF TSC, Table 3 XML encryption	XML-Encryption Syntax and Processing (XMLenc).	e-GIF	When required to secure XML data using encryption and decryption.	A	M

Component Framework – Data Interchange – XML Digital Signature					
e-GIF TSC, Table 3 XML signature and encryption	An XML Signature 'decryption transform' that enables XML Signature applications to distinguish between those XML Encryption structures that were encrypted before signing (and must not be decrypted) and those that were encrypted after signing (and must be decrypted) for the signature to validate.	e-GIF	When specific portions of an XML document need to be signed.	A	M
Component Framework – Data Interchange – XML Path Language					
XPath 1.0 XML Path Language (XPath) Version 1.0	A query language for providing access to subsets of nodes within an XML document.	I	The standard is applicable in any situation where XML documents are queried or manipulated.	A	M
Component Framework – Presentation Interface – Content Rendering					
XHTML1 XHTML 1.0	Family of XML-based document types that reproduce and extend HTML 4.	SG	All browser presented applications. See the ISS4PS Style Guide for more information.	A	M
REC-CSS1 Cascading Style Sheets, level 1 (CSS1)	Cascading Style Sheets allow authors and readers to attach style (eg, fonts, colours and spacing) to HTML/XHTML documents.	SG	All browser presented applications. See the ISS4PS Style Guide for more information.	A	M
REC-CSS2 CSS2	An extension of CSS1 (with a few exceptions) that includes support for media-specific style sheets.	SG	All browser presented applications. See the ISS4PS Style Guide for more information.	A	M
Component Framework – Presentation Interface – Static Display					
e-GIF TSC, Table 6 Hypertext interchange formats	HTML v4.01 and XHTML v1.0	e-GIF	When authoring web-based applications.	A	M
e-GIF TSC, Table 7 Hypertext interchange formats	HTML v3.2	e-GIF	When authoring web-based applications on delivery channels such as PDAs, Smart Phones and kiosks.	A	M
Component Framework – Security - Certificates / Digital Signature					
e-GIF TSC, Table 3 XML key management where a PKI environment is used	XML-Key Management Specification (XKMS 2.0)	e-GIF	Where there is a requirement to distribute public keys.	A	M

e-GIF TSC, Table 3 XML security assertion mark-up	Security Assertion Markup Language (SAML).	e-GIF	Where there is a requirement to exchange security data, for example, to achieve Single Sign-On and cross-Force identity management.	A	M
e-GIF TSC, Table 3 XML access control	eXtensible Access Control Markup Language (XACML).	e-GIF	Where there is a requirement to determine if access is granted to a resource based on rules or policies.	U	R
Component Framework – Security – Supporting Security Services					
Interface specification to the national 118 directory	The Interface specification for the national 118 directory details how forces pass information from local systems to the national directory.	PS	The 118 API must be used by Forces when updating the national 118 directory.	A	M
ITSEC E3 Information Technology Security Evaluation and Certification Scheme, Assurance level E3	The ITSEC scheme provides a formalised methodology for the evaluation of the security features of IT systems. http://www.cesg.gov.uk/index.cfm	Gov	Firewalls meeting ITSEC Assurance level E3 are required for all classified networks.	A	M
Police Information Assurance Guides	Series of guides for those implementing Information Assurance at Force level.	PS	These guides offer assistance to Forces when implementing Information Assurance.	A	G
ISO/IEC 17799 Code of practice for Information Security Management	Guidelines and voluntary directions for information security management. It provides a high level description of areas of importance when implementing Information Assurance.	CSP	See the ACPO CSP for more information. http://www.acpo.police.uk/asp/policies/Data/imba_statuspage_website_revised_csp_sept02_100203.doc	A	M
BS 7799-2 2002 Specification for Information Security Management	This specification explains how to implement ISO/IEC 17799.	CSP	See the ACPO CSP for more information. http://www.acpo.police.uk/asp/policies/Data/imba_statuspage_website_revised_csp_sept02_100203.doc	A	M
e-GIF TSC, Table 1 E-mail transport security	Transport conforms to RFC 3207.	e-GIF	Delivery of E-mail.	A	M
e-GIF TSC, Table 1 E-mail content security	S/MIME v3	e-GIF	End-to-end security is required for pan-government messaging.	A	M

Component Framework – Security – Supporting Security Services

e-GIF TSC, Table 1 Secure mailbox access	Mailbox access over insecure networks shall use HTTPS, conforming to the Transport security standards listed below. This includes RFC 2595 when using TLS with IMAP, POP3 and ACAP to access mailbox.	e-GIF	When accessing mailboxes over insecure networks.	A	M
e-GIF TSC, Table 1 Security	Covers the Manual of Protective Security and e-Government Strategy framework and guidelines on security v 4.0.	e-GIF	All security requirements.	A	M
e-GIF TSC, Table 1 IP encapsulation security (for VPN requirements)	ESP (RFC 2406).	e-GIF	Implementing secure services within IPv4 and IPv6 architectures.	A	M
e-GIF TSC, Table 1 Transport security	SSL v3/TLS (RFC 2246).	e-GIF	To provide privacy and data integrity between two communicating applications.	A	M
e-GIF TSC, Table 1 Encapsulation security	CMS (RFC3369).	e-GIF	To ensure common cryptographic message syntax for digital signatures and encryption.	A	M
e-GIF TSC, Table 1 Timestamp token	TSP (RFC 3161).	e-GIF	For all timestamped data to ensure a trustworthy source of time.	A	M
e-GIF TSC, Table 1 Encryption algorithms	3DES, AES (FIPS 197), Blowfish.	e-GIF	When data need encryption.	A	M
e-GIF TSC, Table 1 For signing	RSA, DSA, DSS (FIPS 186-2).	e-GIF	When data need to be signed.	A	M
e-GIF TSC, Table 1 For key transport	RSA, DSA.	e-GIF	When transferring encryption keys.	A	M
e-GIF TSC, Table 1 For hashing	SHA-512, SHA-256 (FIPS 180-2). For backward compatibility SHA-1 and MD-5 should also be supported.	e-GIF		A	M
e-GIF TSC, Table 2 Web services security	Basic Security Profile Version 1.0 (WS-I Security).	e-GIF		A	N
	Web Services Trust Language (WS-Trust).			F	R
	SOAP Message Security 1.0			F	N
	Username Token Profile V1.0			F	R

e-GIF TSC, Table 2 WS-Secure conversation	Web Services Secure Conversation Language (WS-SecureConversation).	e-GIF	When authentication of a series of messages is required.	F	R
e-GIF TSC, Table 2 WS-Federation	Web Services Federation Language (WS-Federation).	e-GIF	When required to work across differing security realms.	F	R
e-GIF TSC, Table 2 WS-Policy	The Web Services Policy Framework (WS-Policy) provides a general-purpose model and corresponding syntax to describe the policies of a Web Service. WS-Policy defines a base set of constructs that can be used and extended by other Web services specifications to describe a broad range of service requirements and capabilities.	e-GIF	Three potential standards to define the framework, assertions and attachments.	F	N
e-GIF TSC, Table 2 WS-Security Policy	Web Services Security Policy Language (WS-SecurityPolicy) specification indicates the policy assertions, which apply to Web Services Security: SOAP Message Security, WS-Trust, and WS-SecureConversation.	e-GIF		A	M
e-GIF TSC, Table 2 WS-Access Control	SAML 2.0 Profile for XACML.	e-GIF		A	M
e-GIF TSC, Table 11a-h Smart Cards	Series of specifications providing standards to be adopted for Smart Cards.	e-GIF	When providing solutions that use Smart Cards.	A	M

A.5 Service Access and Delivery Standards

Reference and Title	Summary	Source	Applicability	Classification	Status
Service Access & Delivery – Access Channels – Collaborative Communications					
IETF RFC 2445 - 2447 iCalendar (iCal) / vCalendar	Transport and platform-independent format for exchanging calendaring and scheduling information.	I	Any system where calendaring or scheduling information is held. vCalendar is the minimum requirement, the newer iCalendar standards should be supported wherever possible. While neither standard guarantees interoperability between collaboration systems, it will ensure alignment when suitable technologies exist to solve the interoperability question.	A	M
IETF RFC 2425 - 2426 vCard	Transport and platform-independent format for exchanging personal information of the type that would normally be found on a business card.	I	Any collaboration type system where personal information is stored.	A	M
Service Access & Delivery – Access Channels – Other Electronic Channels					
e-GIF TSC, Table 5 Scheme for site identification on the WWW	A collection of standards aimed at providing identifiers.	e-GIF	Defining an address of a resource.	A	M
Service Access & Delivery – Service Requirements – Service Management					
ITIL IT Infrastructure Library	A collection of best practice for managing IT services.	Gov	All Police IT service management functions will be based on ITIL.	A	M
Service Access & Delivery – Service Requirements – Service Transport					
Bluetooth Bluetooth	Standard for short range wireless connectivity that is used in building Personal Area Networks.	I	Bluetooth can be considered for applications requiring a wireless Personal Area Network. Security in 802.11 based networks is better known and should also be considered.	U	N
UMTS Universal Mobile Telecommunications System (3G)	Third generation commercial mobile communications technology.	I	3G technologies may be considered for mobile applications where Airwave does not provide the required data rates.	R	N
IETF RFC 2460:1998 Internet Protocol v6	Successor to version 4 of the Internet Protocol (IP). Includes expanded addressing capability and header simplification.	I	Support for IPv6 should be specified when procuring new products.	R	R

e-GIF TSC, Table 1 Hypertext transfer protocols	RFC 2616, Upgrade mechanism in HTTP/1.1 to initiate Transport Layer Security (TLS) over an existing TCP connection.	e-GIF	When providing solution that use the HTTP/S over TCP/IP architectures.	A	M
e-GIF TSC, Table 1 File transfer protocols	FTP (RFC 959) (with restart and recovery) and HTTP. (RFC 2616) for file transfer.	e-GIF	When providing data external to applications for uncontrolled usage.	A	M
e-GIF TSC, Table 1 Newsgroup services	NNTP (RFC 977) where required, subject to security constraints.	e-GIF	When providing solutions that operate a publicly accessible newsgroup service.	A	M
e-GIF TSC, Table 1 LAN/WAN networking	IP v4 (RFC 791). Departments are to interconnect using IPv4 and plan for migration to IPv6 in due course.	e-GIF	When upgrading or installing office network infrastructure.	A	M
e-GIF TSC, Table 1 IP security (Authenticated header)	IP-SEC (RFC 2402/2404).	e-GIF	Where there is a requirement to securely transfer data at the IP level, for example via Virtual Private Networks.	A	M
e-GIF TSC, Table 1 Transport Security	SSL v3/TLS (RFC 2246).	e-GIF		A	M
e-GIF TSC, Table 2 WS-Reliable Messaging	Web Services Reliable Messaging (WS-Reliability 1.1).	e-GIF	Where there is a requirement to reliably deliver messages between distributed applications.	R	G
e-GIF TSC, Table 2 WS-Addressing	Web Services Addressing (WS- Addressing).	e-GIF	When there is a need to extend the scope of message exchange beyond a simple request and respond basis.	F	G
e-GIF TSC, Table 8 WAP specifications	The specifications to be used are defined by the WAP Forum.	e-GIF	Only when the standards defined for smart phones in e-GIF Table 7 (other channels) are not applicable.	A	M
e-GIF TSC, Table 8 GPRS	General Packet Radio Service.	e-GIF	When transferring data over mobile devices.	A	M
e-GIF TSC, Table 8 SMS	Short Message Service.	e-GIF	When transferring short text-only data over mobile devices.	A	M
e-GIF TSC, Table 8 MMS	Multimedia Messaging Service.	e-GIF	When transferring short text and static image data over mobile devices.	A	M

Service Access & Delivery – Access Channels – Supporting Network Services

Police Service Schema for Active Directory	A schema for Police specific extensions to Active Directory	PS	The Police Service Schema ensures that Police specific extensions to the Active Directory schema are implemented in the same manner across the Police Service. Where Active Directory is used, the schema should conform to this standard.	A	M
Police Service Schema for LDAP	A Police-specific schema for LDAP directories.	PS	The Police Service Schema ensures that Police specific LDAP schemas are implemented in the same manner across the Police Service. Where an LDAP directory is used, the schema should conform to this standard.	A	M
ISO/IEC 9594:1993 X.500	An X.500 Directory Service provides a structured repository for storing people type information.	I	X.500 should not be considered for any new directory implementations. Active Directory and/or LDAP should be considered instead.	W	N
ISO/IEC 8802-11:1999 IEEE 802.11	A family of six wireless LAN standards that utilise the same modulation techniques.	I	The 802.11 family of standards provide a common set of operational rules for airwave interoperability of wireless Local Area Network (LAN) products from different vendors. All wireless LAN implementations should implement 802.11 for maximum compatibility.	A	M
IETF RFC 1155 to 1157, RFC 1213 Simple Network Management Protocol, Version 1 (SNMPv1)	An application layer protocol that allows management information to be exchanged between network devices.	I	All infrastructure products must provide support for both SNMP versions.	A	M
IETF RFC 1441 – 1452, RFC 1901 - 1910 Simple Network Management Protocol, Version 2 (SNMPv2)	An enhanced version of SNMPv1.	I	All infrastructure products must provide support for both SNMP versions.	A	M
e-GIF TSC, Table 1 E-mail transport	E-mail products that support interfaces that conform to the SMTP/MIME for message transfer. This includes RFC 2821, RFC 2822, RFC 2045, RFC 2046, RFC 2646, RFC 2047, RFC 2231, RFC 2048, RFC 3023, RFC 2049	e-GIF	E-mail attachments may conform to the file types for browsers and viewers as defined for the specific delivery channel, see e-GIF Section 7 – e-Services access and Channels	A	M

e-GIF TSC, Table 1 Mailbox access	Unless security requirements dictate otherwise, e-mail products that provide mail access facilities shall as a minimum conform to POP3 for remote mailbox access. This includes RFC 1939, RFC 1957 and RFC 2449. Where additional mail facilities are required, unless security requirements dictate otherwise, e-mail products that provide advanced mail access facilities shall conform to IMAP for remote mailbox access. This includes RFC 3501, RFC 2342, RFC 2971, RFC 3502, RFC 3503 and RFC 3510.	e-GIF	Interfaces for e-mail systems are to conform to POP3 or IMAP for mailbox retrieval	A	M
e-GIF TSC, Table 1 Directory	GSI Notice 1/2003 Information GSI Directory Schema.	e-GIF	LDAP v3 is to be used for general purpose directory user access	A	M
e-GIF TSC, Table 1 Domain name services	DNS (RFC 1035)	e-GIF	The UK Government domain naming guidelines define policy. GSI domain naming follows these guidelines as far as possible. GSI e-mail addressing specifications are defined in GNC Technical Notice 2/2001 (Domain Names, DNS and E-mail Addressing)	A	M
e-GIF TSC, Table 5 Identifier resolution system	A collection of standards aimed at providing identifiers.	e-GIF	Where information is provided electronically and the location is likely to change over time an identifier resolution system enables the information to always be accessible.	A	M
e-GIF TSC, Table 9 and Table 10 Assembly	ITU H .323 (07/03), V5 Standards for the assembly of Audio, Video, Data and Control (AVDC)	e-GIF	Where there is a need to support video and voice conferencing over an IP based network, for example, Voice over IP.	A	M

A.6 Service Interface and Integration Standards

Reference and Title	Summary	Source	Applicability	Classification	Status
Service Interface and Integration – Integration – Middleware					
ISO/IEC 9075:1992 Structured Query Language	A language used for accessing and manipulating databases.	I	Any RDBMS. This standard helps to ensure that applications can be ported from one database to another.	A	M
X/Open C193:1992 Distributed TP: The XA Specification	A model for Distributed Transaction Processing.	I	All distributed applications should consider the use of XA where relevant.	R	R
JMS 1.1 Java Message Service, Version 1.1	A messaging standard for creating, sending, receiving and reading messages on the J2EE platform.	I	All enterprise applications based on the J2EE platform should consider the use of JMS. All implementations of JMS must conform to version 1.1 of the standard.	A	M
e-GIF TSC, Table 2 WS-Transactions	Web Services Atomic Transaction (WS-AtomicTransaction).	e-GIF	When coordinating atomic transactions within the WS-Coordination specification, for example, short-lived transactions requiring agreement on the outcome of the transaction.	R	R
Service Interface and Integration – Interface – Service Description/Interface					
e-GIF TSC, Table 2 Web service description language	WSDL 1.1, Web Service Description Language.	e-GIF	To achieve reuse by describing the service offered, enabling others to select and use them in other solutions.	A	M
Service Interface and Integration – Interface – Service Discovery					
e-GIF TSC, Table 2 Web service request registry	UDDI v3.0	e-GIF	To provide Police Service and partner organisations visibility of available services via a central registry.	A	M
e-GIF TSC, Table 2 WS-Discovery	Web Services Dynamic Discovery (WS-Discovery).	e-GIF	To facilitate a dynamic discovery of services by applications based on the service type and scope.	F	N
Service Interface and Integration – Interoperability – Data Format/Classification					
Microsoft Office XML Schema	The XML schema for Microsoft Office documents.	I	Currently listed for information only.	U	G
Open Document Format	An open, XML-based file format for office applications. It covers the features required by text, spreadsheets, charts and graphical documents.	I	Currently listed for information only.	U	G

e-GIF TSC, Table 3 Data integration metadata/meta language	XML (Extensible Markup Language) Schemas	e-GIF	For all data that is to be exchanged between parties and, where appropriate within applications, to define structure and data types.	A	M
e-GIF TSC, Table 3 Data definition and schema standardisa-tion process	XML and XML Schemas	e-GIF	For all data that is to be exchanged between parties, and where appropriate within applications, to define structure and data types.	A	M
e-GIF TSC, Table 3 Minimum interoperable character set	8 bit UTF-8 (RFC 2279)	e-GIF	When there is a requirement to exchange data between different architecture platforms.	A	M
e-GIF TSC, Table 4 Subject element, category refinement	IPSV (Integrated Public Sector Vocabulary)	e-GIF	Where there is a requirement to populate the e-GMS Subject element for maximum metadata consistency across the public sector.	A	M
e-GIF TSC, Table 5 Persistent and unique logical identifiers	ANSI/NISO Z39.84	e-GIF	When a unique identification must be assigned to digital content.	U	G
e-GIF TSC, Table 5 Persistent identifiers	XRI (OASIS Extensible Resource Identifier)	e-GIF	When a resource location needs to be shared and is location, application and transport-independent.	F	N
e-GIF TSC, Table 5 Unique identifiers	GUID (Globally Unique Identifier)	e-GIF	When a guaranteed unique identifier is required	U	R
e-GIF TSC, Table 5 Identifiers for persistent URLs	A PURL (persistent URL) is a Persistent Uniform Resource Locator. Functionally, a PURL is a URL. However, instead of pointing directly to the location of an Internet resource, a PURL points to an intermediate resolution service	e-GIF	Where there is a requirement to perform a HTTP redirect type operation via a managed and controlled service.	A	M
e-GIF TSC, Table 5 Persistent name for URLs	A PURL (persistent URL) is a Persistent Uniform Resource Locator.	e-GIF		U	N
e-GIF TSC, Table 5 Registered namespaces	URI (Uniform Resource Identifier)	e-GIF	When there is a need to identify the resource type, for example http:, file:, mailto: etc.	R	G
e-GIF TSC, Table 5 Identifiers for digital objects using ASN.1	Object Identifier (OIDs) are used in ASN.1 based protocols.	e-GIF	When there is a need to define a unique identifier to a digital object.	R	N

Service Interface and Integration – Interoperability – Data Format/Classification					
e-GIF TSC, Table 5 Archival identifiers	IETF ARK (Archival Resource Key).	e-GIF	The persistent storage and retrieval of archived material.	F	N
e-GIF TSC, Table 5 Codes for physical objects as used in the retail industry	EAN.UCC (European Article Number/Uniform Code Council).	e-GIF	Bar coding.	R	G
Service Interface and Integration – Interoperability – Data Types/Validation					
e-GIF TSC, Table 3 Data integration metadata definition	XML Schema.	e-GIF	When defining the structure and data types of documentation.	A	M
e-GIF TSC, Table 3 Data transformation	XSL and XSL Transformations.	e-GIF	When required to transform data form one format to another.	A	M
e-GIF TSC, Table 4 Content management metadata definition	XML Schema.	e-GIF	When publishing XML Schema within the Police Service and publicly where appropriate.	A	M
e-GIF TSC, Table 4 Content management metadata elements and refinements	e-GMS.	e-GIF	When publishing metadata standards publicly.	A	M
e-GIF TSC, Table 4 Data definition	Government Data Standards Catalogue.	e-GIF	When defining data standards for use in the wider criminal justice community.	A	M
Service Interface and Integration – Supporting Platforms – Wireless / Mobile					
Airwave	The Airwave Trunk Radio mobile platform for voice and data.	PS	Airwave is mandated for all voice applications within the Police Service. Mobile data applications should use Airwave where not prevented by the TETRA data rate limitation.	A	M

A.7 Service Platform and Infrastructure Standards

Reference and Title	Summary	Source	Applicability	Classification	Status
Service Platform and Infrastructure – Database Storage – Storage					
Police Service Fileplan	The Police Service File Plan (PSFP) is a structured classification of Police business which can be implemented in information management systems.	PS	This standard should be considered when setting up a new electronic document management system. Current systems, network fileshares, filing cabinets, etc, should be migrated to the Fileplan, where possible.	A	R
Service Platform and Infrastructure – Hardware Infrastructure – RFID					
e-GIF TSC, Table 5 Radio Tracking Identification	Radio Frequency Identification (RFID)	e-GIF		R	G
Service Platform and Infrastructure – Hardware Infrastructure – Video Conferencing					
e-GIF TSC, Table 1 Real-time messaging services	A collection of standards pertaining to Real Time Messaging services.	e-GIF	At the current time there are numerous real time messaging protocols in use, largely as components of commercial instant messaging services (for example AIM, ICQ, MSN and Yahoo Messenger). Interoperability between services based on the various protocols is limited. A number of Internet drafts are currently in production to define common profiles and common services for gateways between real time messaging systems. In addition, end-user desktop-based utilities are available that combine the functionality of the commercial instant messaging services and support connectivity between users of the various commercial instant messaging services.	U	N
e-GIF TSC, Table 9 Audio	As a minimum ITU G.723.1 and G.722	e-GIF		R	G
e-GIF TSC, Table 9 Video	ITU H.261 and H.263	e-GIF	When there is a need to compress video.	R	G
e-GIF TSC, Table 9 Data	ITU T.120	e-GIF	When collaborative exchange of electronic data is required, for example, sharing whiteboard sessions with remote users.	R	G

Service Platform and Infrastructure – Hardware Infrastructure – Video Conferencing					
e-GIF TSC, Table 9 Control and signalling	ITU T.H.225 and H.245	e-GIF	When there is a need to provide solutions using bandwidth limited visual telephone services.	R	G
e-GIF TSC, Table 9 Call control signalling	ITU T.Q.931	e-GIF	To control call setup and termination.	R	G
Service Platform and Infrastructure – Hardware Infrastructure – Voice Communications					
e-GIF TSC, Table 10 Gateway control	A collection that defines standards for multimedia gateway.	e-GIF	Defines the standards for multimedia gateways.	R	N
e-GIF TSC, Table 10 Application layer signalling	Session Initiation Protocol (SIP): RFC 3261	e-GIF	Where there is a requirement to create, modify and control collaborative voice calls.	R	N
e-GIF TSC, Table 10 Resource setup	Resource ReSerVation Protocol (RSVP): RFC 2205 and RFC 2750	e-GIF	For providing a receiver based setup of resource reservations in multicast or unicast data flows.	R	N
e-GIF TSC, Table 10 Transport and control protocol	Real Time Protocol (RTP) and Real Time Control Protocol (RTCP): RFC 3550	e-GIF	RTP and RTCP provide end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services.	A	M
e-GIF TSC, Table 10 Delivery control	Real Time Streaming Protocol (RTSP): RFC 2326	e-GIF		R	N
e-GIF TSC, Table 10 Announcement protocol	Session Announcement Protocol (SAP): RFC 2974	e-GIF	For announcing the description of multicast sessions.	R	N
e-GIF TSC, Table 10 Session description	Session Description Protocol (SDP): RFC 2327	e-GIF	When providing a short textual description of a session.	R	N
e-GIF TSC, Table 10 Extended RTCP	RTP Control Protocol Extended Reports (RTCP XR): RFC 3611	e-GIF	For measuring VoIP performance enabling assessment of call quality.	R	N
Service Platform and Infrastructure – Supporting Platforms – Platform Dependent					
Windows XP Professional system requirements	The Microsoft Windows desktop operating system requirements.	I	All current and new desktop hardware platforms should meet or exceed the minimum requirements for running Windows XP Professional.	A	M
Windows Server 2003 system requirements	The Microsoft Windows server operating system requirements.	I	All current and new Wintel server hardware platforms should meet or exceed the minimum requirements for running Windows Server 2003. It is recommended that the Enterprise Edition is used.	A	M

Service Platform and Infrastructure – Supporting Platforms – Platform Independent

LSB 2.0 2004 Linux Standards Base 2.0	A set of standards designed to increase compatibility among Linux distributions. http://www.linuxbase.org/	I	The Linux Standards Base promotes software portability through binary compatibility. All Linux platforms should be LSB certified.	A	M

Annex B Actions and Guidance for IT Directors/Chief Officers

This annex outlines for IT Directors/Chief Officers and their staff the actions for Phase 1 of the ISS4PS. The annex is split into three sections: Priority activities for Phase 1, secondary activities for Phase 1 and guidance for Phase 1.

Phase 1 of the ISS4PS Roadmap covers a period of twelve months. The priority activities are those that are required to be completed as early as local resource commitments will allow. The secondary activities defined in the roadmap relate to actions that should be completed by the end of Phase 1 but are of lower priority in terms of timeframe. The final section of the annex provides guidance for Forces that is specific to the first phase of the ISS4PS.

Contents

B.1 Priority Activities for Phase 1

Force IS/ICT strategies aligned to ISS4PS

- Forces should review their local IS/ICT policies and standards to bring them into line with the ISS4PS.
- Local policies should be measured against the policies in Volume 1 and the principles established in Volume 2 of the ISS4PS.

Understanding the areas in which local policy differs from the ISS4PS will allow forces to produce their local migration plans.

Refer to action 42 in the main document for details.

Perform a Local Data Quality Audit and produce a local plan for improving the data quality

- Perform a local data quality audit in preparation for implementing a local data store. It is envisaged that this activity will need to be conducted throughout the migration to the ISS4PS.
- A local plan for improving data quality needs to be created by each Force. The plan will address issues including data integrity, accuracy and completeness.
- Guidance on how to perform such an audit will be produced during Phase 1.

Steps taken in auditing local data quality will inform the local migration plan for improving data quality.

Refer to actions 12 in the main document for details.

Evaluations of data quality and load tools analysed

- Each force will need to provide to the technical authority their analysis and evaluations so that a coordinated set of tools can be established for Forces. Where economies of scale can be established, tools will be recommended to Forces.
- Guidance for developing a local plan will be produced during phase 1.

The next stage of implementing the local data store will be based on these tools. Lessons learned and, as necessary, economies of scale can be shared between forces.

Refer to actions 19, 20 and 21 in the main document for details.

Implement Local Data Store – Federated data store implemented in Forces

- The critical deliverable of phase one of ISS4PS is for Forces to implement a Federated data store as a stepping-stone to creating the Global Data Store.

A Federated data store provides the capability to make Force level data available nationally.

Refer to action 15 in the main document for details.

Include Conformance Criteria in All New Contracts and Developments

- A set of generic compliance criteria for use when procuring or developing systems or solutions has been provided in the ISS4PS annexes.
- Mandated standards from the relevant categories in Annex A should also be included along with their applicability statement.

Including these statements in all new tenders will assist in developing systems that are in line with the principles of the ISS4PS and follow the ISS4PS Technical Architecture.

Refer to Annex A Standards, and Annex C ISS4PS Compliance and action 37.

Review Current Roles and Responsibilities

- The ISS4PS requires that a Technical Authority (TA) role be established at local level. Forces should review their current responsibility structures and identify where the TA role can be placed within their organisation.
- Where they are not able to individually support a TA role, Forces should look to collaborate with others with a view to forming a group TA.

The Technical Authority is responsible for ensuring that systems are not developed in isolation from one another.

Refer to action 35 in the main document for details.

Implement the ACPO/ACPOS Information Systems Community Security Policy (CSP)

- The ISS4PS requires Forces to implement the Community Security Policy (CSP) as adopted by ACPO Council.
- Develop and Test a Response Plan – how each force will respond to an attempt to compromise their systems.
- Implement Proactive Monitoring of Systems – to pre-empt attacks and reduce the risk on the operational business.
- Update as necessary the 118 Directory – national directory of police workers.
- Reduce the number of local directories to support the migration to the CSP and Universal Police Security Architecture (UPSA).

The ISS4PS requires Forces to implement the CSP as adopted by ACPO Council. Forces should be putting the CSP into practice as soon as possible in order to achieve compliance. The CSP provides a framework for achieving information security. Complying with the CSP ensures that Police Service takes a consistent approach to information security.

Refer to actions 25 and 26 in the main document for details.

Data models harmonised with CorDM - Document Data Structures

- Forces should ensure that the data structures held in core business systems are fully documented and up to date.
- Correlation to CorDM established and the migration plan updated to show how alignment with CorDM will be achieved.

This will identify the core data held in local enterprise systems that will be shared between Forces.

Refer to action 17 in the main document for details.

B.2 Secondary Activities for Phase 1

Prepare for the ISS4PS Technical Architecture

- The ISS4PS Technical Architecture is based on the principles of service orientation and Service-Oriented Architecture.
- Forces should take the opportunity to bring all relevant personnel up to date with these current architectural trends through appropriate training and development.

The ISS4PS Technical Architecture provides the foundations for delivering services that are able to meet continually changing business requirements.

Refer to actions 3, 4 and 14 in the main document for details

Review Current Integration Solutions

- During phase 1 the Enterprise Architecture framework and tools will be selected.
- Guidelines on migration paths to an Enterprise Service Bus (ESB) will be provided. It is expected that Forces will begin to adopt common products and services during the later stage of phase 1 where appropriate. In some cases, vendors of the current EAI solutions may already provide a migration path to an ESB.

The Enterprise Service Bus is a recognised pattern for implementing Service-Oriented Architecture. It is much more scalable, flexible and reliable than traditional EAI solutions.

Refer to action 6 in the main document for details.

Review Applications Currently in Development – Legacy Applications Identified

- Applications that are currently being developed or specified should be assessed as to their compliance with the ISS4PS principles.
- A list of legacy applications can be produced and coordinated centrally. If required, and where possible, Forces should update their development projects to reflect the principles of ISS4PS.
- The Technical Authority will provide advice on whether applications that are in production need to be reengineered as part of Phase One.

Developing applications to the ISS4PS Technical Architecture will reduce the number of silos within the Police Service.

Refer to action 39 in the main document for details.

Force Networks analysed and a migration plan to meet minimum standards produced

- Each Force will need to define their existing network so that a gap analysis can be established for migrating to the minimum standards expected for the infrastructure.

A complete network analysis will help to inform the ISS4PS governance of the overall migration plan and assist with the compilation of an overall ISS4PS business case.

Refer to actions 9 and 27 in the main document for details.

Compile a List of All COTS/POTS Products

- An essential part of phase one is to establish the total number of COTS/POTS products in service. Each Force should compile a catalogue of COTS/POTS products in use.

This will help identify those products that will become core applications or services. A consolidated list of all COTS/POTS products is required to understand the number of products in service.

Refer to actions 9, 18 and 25 in the main document for details.

Migrate to the Minimum Standard Infrastructure

- The successful implementation of CRISP (or its equivalent) requires that Forces migrate to the minimum standard infrastructure during Phase 1.
- Forces are recommended that major changes should be avoided until the minimum standards have been established. The standards will be produced in the early stages of Phase 1. Any variations to the standards proposed by Forces will need to be reviewed by the technical authority.
- Forces should consider deferring significant changes to their infrastructure until phase 2, when the PNN3 contract is in place.

The minimum standard infrastructure ensures that Forces have the capability to share information.

Refer to action 9 in the main document for details.

B.3 Guidance for Phase 1

Selecting and Purchasing Products

During Phase One there will be procurement procedures and guidance written. However, in the absence of a defined set of common procedures, products and standards, Forces are advised not to make any strategic purchases in the short term. If this is not possible, Forces are advised to:

- Seek guidance from the technical authority.
- Look for products that have already been adopted by Forces. Such products are more likely to be accepted as a standard product when the TRM is established.
- Look for products with the widest support for industry and police standards. See below, 'Supporting Standards', for more information on standards use.
- Look to best-of-breed products.

Supporting Standards

Forces should look to those products with the widest support for industry standards. For both COTS and bespoke solutions, Forces should require vendors and developers to demonstrate the level of standards support by solutions.

Without the ISS4PS Standards Information Base (SIB) in place, Forces should refer to the provisional list of standards at Annex A and the e-GIF Technical Standards Catalogue[5] for guidance.

Implementing The ISS4PS Data Exchange and Interoperability Standards

The ISS4PS has been developed to assist the Police Service in eliminating silos of data. Any solution or product of strategic importance that is procured during Phase One should demonstrate that it is in keeping with this aim.

Forces should stipulate that all strategic applications expose data and services via a service interface or an open data layer, or provide another mechanism by which it can be interfaced.

Once established, interfaces should conform to the ISS4PS Data Exchange and Interoperability standards.

Selecting Integration Products

Forces should use an Enterprise Service Bus (ESB) for all new integration projects. Traditional Enterprise Application Integration (EAI) products will have ongoing tactical use within the overall ISS4PS architecture, although should be avoided for large-scale enterprise integration.

To select an ESB (or EAI) product before common Police Service product(s) are selected, Forces should choose one that provides the widest support for industry standards, as this is most likely to be compatible with the selected common products. Guidelines at Annexes A and C should be followed.

Service and Technology Library

Once released, system developers should familiarise themselves with the Service and Technology Library, the Service-wide resource for maintaining and sharing enterprise services and components. Once comfortable with the library, Forces should start to use, and contribute to the library.

Implementing ITIL

Forces should consider delaying investment in tools for implementing Information Technology Infrastructure Library (ITIL) until a common implementation approach has been established and a common toolset has been agreed. Forces should provide some ITIL training for operations staff in preparation for its introduction.

5 http://www.govtalk.gov.uk/schemasstandards/egif_document.asp?docnum=873

Digital Identities

The ISS4PS requires a common method of managing digital identities. This method has not yet been defined. It is likely that UPSA will define common products for use in this area.

Forces should avoid implementing new Force-specific ways of managing digital identities at present. Where a delay cannot be accepted, industry standards should be used, and products that are in common use within the Police Service should be adopted. This is likely to reduce the effort required to migrate to the common methods and products when a police standard is defined.

Where new applications that require digital identities are procured or built, it is recommended that the system adopts a modular approach to dealing with digital identities to enable integration to recommended products in the future.

Analyse Understanding of the Current Enterprise Architecture

In the period before the ISS4PS Technical Reference Model (TRM) is established, Forces should be taking the opportunity to analyse the degree to which their current architecture is understood and documented. Where significant gaps are revealed, Forces should seek to discover enough detail to give a complete overview of the enterprise.

With the absence of a Police-specific TRM, Forces may wish to use the established, though generic, TOGAF model as the basis for this discovery and documentation process. The scope can be restricted by developing a high-level view and giving priority to documenting those systems that feed CRISP.

As Service-wide Enterprise Architecture Framework (EAF) tools become available, training sessions and other events will be organised. Forces can take full advantage of the benefits offered by such tools by raising awareness of them internally.

Annex C ISS4PS Compliance

To achieve the benefits outlined in the ISS4PS strategy, assessment of both programmes and projects is required to establish the level of conformance to the architectural principles. The concept of conformance is evolving and the constraints on the implementation of the architecture will become tighter over time.

The nature of compliance to the ISS4PS is different to that of compliance to a standard.

Due to the nature of compliance, it is not a 'kite mark' for products or applications as the strategy has a broader reach. The nature of compliance is closer to a programme gateway review, in line with the OGC rather than a series of pass/fail questions.

This document defines the scope and architectural principles for conformance to the overall ISS4PS strategy as well as providing details on the assessment criteria across the three phases, the terms used to define levels of conformance, the timings and purpose of compliance assessment, and the governance details.

This document does not seek to provide the compliancy checklists, more to articulate what compliancy assessment entails. Checklists will be continuously evaluated and updated over the course of the strategy and will be available in electronic form. Whilst this annex is initially aimed at suppliers, as the various building blocks for in-house development become available (such as the Technical Reference Model), updates will be published to include detail for internal development routes to solutions architecture.

The ISS4PS focuses on technology, data and solutions architecture. The business view is recognised as an important enabler for the ISS4PS but is explicitly excluded from the scope of Volume 2. Once a baseline of the Police Service business architecture is delivered, compliance guidelines will be updated to cover more detailed guidance on the alignment of the IT solutions and the business.

Contents

C.1 Stages to Achieving Compliance

There are three phases to achieving compliance and they directly relate to the three phases that are discussed in section 3 of the main ISS4PS document. In summary, they are as follows:

- **Federating the data**

  Compliancy during this first phase will be largely assessed on the ability of local or national applications to express their data in a unified fashion via the Federated Data Store (FDS). The exact format for this interchange has yet to be decided but it is expected that it will be based around an amalgamation of both CorDM and CRISP XML.

  The Information Technology Infrastructure Library (ITIL) should be initiated and plans for the population of the policies relating to Configuration Management, Change management, Release management and Problem management should be in early draft form.

  Detailed plans should be in place covering the exposure of services to the Enterprise Service Bus as well as gap analysis between local Force applications and the Technical Reference Model and its associated implementation to enable migration to occur.

  Forces will have updated their infrastructure to meet the minimum level requirements, ensuring sufficient band width for the operation of the FDS and other national, centrally-hosted, browser-based applications.

  Initial plans for the cleansing and management of data should have been completed and submitted to the Enterprise Level Technical Authority (ELTA) for approval.

- **Globalising the data**

  Compliancy at Phase Two will be assessed on the basis that the Global Data Store (GDS) has been delivered. Data cleansing will have taken place, both nationally and locally and the cleansed data will be used to populate the GDS from the FDS established in Phase One.

  Interfaces supporting the querying of this data are in place at both local level and national level and applications are modified to take into consideration this capability.

  Migration from legacy applications to a service oriented approach using the Enterprise Service Bus for transport should have started and interface definitions should be published to the shared services library.

- **Globalising the architecture**

  Compliance in this final phase will be assessed on the basis of the use of the GDS coupled to the use of the common business services and components for all non-legacy applications or line of business functions. While the majority of change will have occurred prior to this phase, compliancy will focus on the adoption of ISS4PS for all applications and services as well as the relationships between the local force and suppliers in terms of the contracts required to be in place for both change requests and ongoing work.

  To be successful compliance will need to be embedded into an enterprise configuration management process.

C.2 Assessment Criteria

Compliance assessment can be broken down into discrete streams as outlined below. It is intended that compliance procedures are developed for each of these discrete areas with a view to combining the results to produce an overall compliance assessment.

When assessing compliance to the ISS4PS it is not always appropriate to utilise a numeric or linear assessment scale. Areas such as user interface design and application design are prime candidates where a non-linear scale should be used. Where a numeric or weighted scale is used then this will result in a direct and comparable score, enabling specific comparisons between products or technology solutions.

Scoring Mechanism

To assess compliance, a score or indicator will be used to determine the level of compliance. Concrete objective assessment metrics, where possible, will be used supported by a subjective assessment where appropriate. However, subjective assessments are to be kept to a minimum.

An action from the compliance assessment will be the identification of further studies and assessments of products and standards. The aim of this will be to establish concrete compliance questions that will result in a Boolean response. This will enable objective reporting of compliance at all levels of the enterprise and allow comparison of products or services.

All compliancy points will need to be assessed against a series of statements to gain a view on the level of compliancy that is being proposed. The following statements should be used as a guide to establishing the alignment levels of a particular application or programme, regardless of whether it is to be deployed at national, regional or Force level.

There is an important relationship between the defined architecture and its implementation, in the same way that there is a relationship between a logical and physical architecture model. This relationship stems from the definition of the terms used to define the level of compliance. Actual terms used may be different in differing areas of the business. The ISS4PS defines key terms to ensure that the concept articulated is consistent. Figure C1 illustrates the compliance terms. The compliance terms and their meanings are defined as follows:

- **Irrelevant**

  The implementation has features that do not impact the features outlined in Volume 2 and is not required to complywith any of the architectural principles or specifications. This category is reserved for true legacy applications that are not part of the wider ISS4PS architecture or infrastructure and have been approved for installation by the Technical Authority (an impact statement and the configuration records update to reflect the variation).

- **Consistent**

  The implementation has some features in common with the Technical Reference Model (TRM) (a mix of mandatory and desirable features). These features are in accordance with the architectural specification. However, there are some architectural specifications that are not aligned to either the strategy or the TRM.

- **Compliant**

  The implementation does not have all of the features outlined by the architectural TRM, but has all of the mandatory features covered by the architectural TRM.

- **Conformant**

  The implementation has all of the features outlined by the architectural TRM, but contains additional features that are not covered by the architectural TRM.

- **Fully Conformant**

  There is full compliance between the architectural TRM and the implementation. All specified features are implemented in accordance with the architectural TRM.

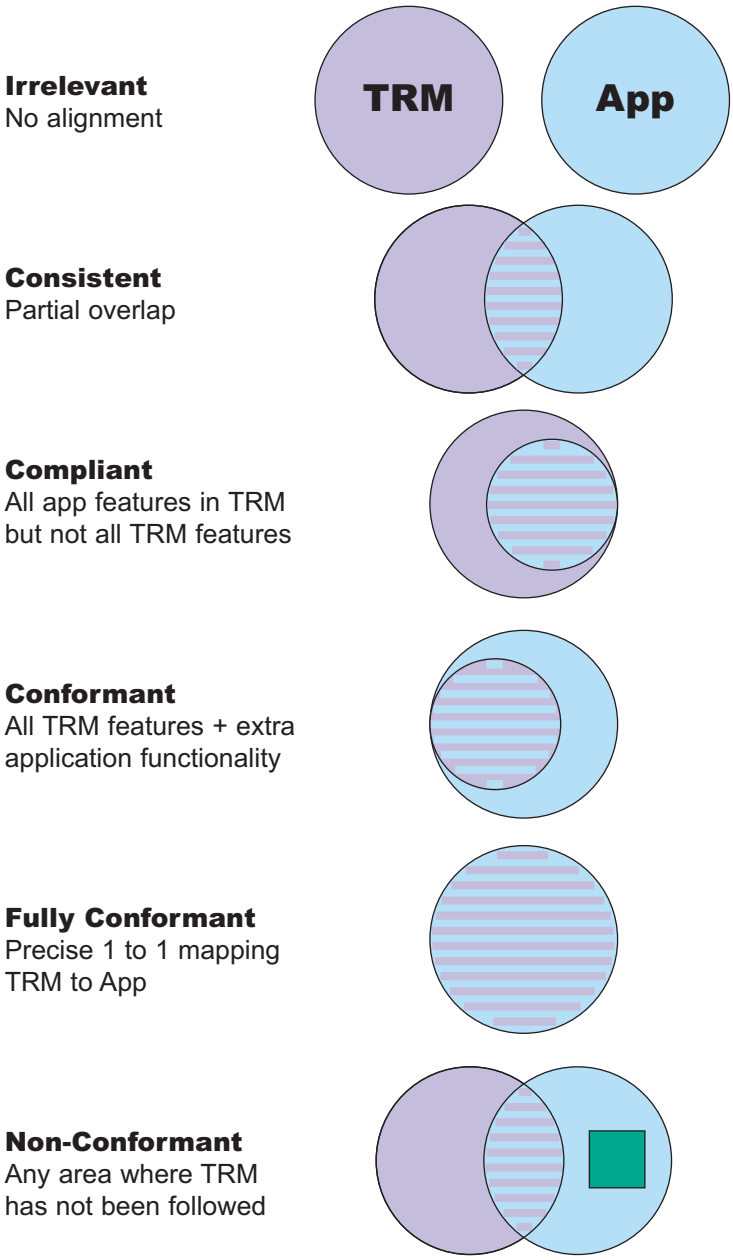
- **Non-Conformant**

  Any of the above statements where some of the features are not implemented in accordance with the architectural TRM.

In the compliance terms defined, the phrase “in accordance with” has the following meaning:

- Supports the strategy and future directions as outlined in ISS4PS Volume 2.
- Adheres to the standards as outlined in both the TRM and SIB.
- Provides the stated functionality as provided by the TRM.
- Adheres to the stated Enterprise Architectural Principles in the strategy.

Figure C1 – Illustration of compliance terms



C.3 Architecture Compliance Reviews

An architecture compliance review is a process to scrutinise the compliance of a specific programme/project or application against the established architectural criteria, principles, spirit and stated business objectives. A formal, documented process for compliance assessment reviews forms the core basis of the ISS4PS compliance and will produce an indicator as to the level of compliance achieved to the ISS4PS.

Purpose

The goals of an architecture compliance review are detailed as follows:

- To identify the level of divergence from the ISS4PS architecture, as early as possible, during development and implementation. This reduces the cost and risk of changes occurring later in the life cycle. This should reduce the risk of delivery creep within programme and projects to assure business benefit realisation is as fast as possible.
- Ensure that best practice is applied to all architectural design decisions.
- Provide an overview of the levels of compliance across the programme and project portfolio.
- Identify where the standards mandated in either the TRM or SIB need to be reviewed and updated.
- Identify potential services that may be application specific, but would make candidates for promotion to enterprise-wide services.
- Identify potential for collaboration, resource sharing and other synergies across the enterprise architecture.
- Take advantage of advances in technology and adapt the ISS4PS architecture accordingly.
- Communicate both the technical status and alignment to the ISS4PS of the IS/ICT plan to management and the SROs.
- Identify key criteria for a common procurement approach.

In addition to the quality assurance issues outlined, there are a number of management controls that need to be included in the compliancy assessment and review. These have been defined as the following:

- The architectural compliance review is a way of providing an impact assessment against the defined architecture. The assessment will enable a technical project risk to be raised to allow the Force to make a decision on the approach.
- The output of the technical assessment is a firm deliverable of the Technical Authority (TA).
- Architectural reviews provide the practical engagement approach for the TA with programmes and projects.
- The enterprise architecture and associated compliance provides additional avenues to assure alignment of technology projects to business objectives.
- Architectural compliance reviews examine the critical risk areas of a programme highlighting the main areas of risk for the SRO and, ultimately, the main governing body.

While compliance to the architecture is essential for both development and implementation, non-compliance provides a mechanism for highlighting areas that need to be addressed for realignment. The architecture assessment provides a level of assessment for projects with a feedback loop for the entire architectural process.

Areas of non-compliance are candidates for review at the enterprise level as new innovations for possible inclusion in the ISS4PS architecture model. To ensure flexibility the TA will be able to offer architectural waivers at the discretion of the ISS4PS architecture board. Waivers will be under stringent change control procedures and will require an impact assessment before approval can be given.

Timing

The timing of compliancy activities needs to be considered with regard to the development of programme and project architectures. Compliance reviews should be held at strategic points during the programme and project life cycle, such as:

- Programme definition phase.
- Programme or project initiation.
- Initial procurement activities (Invitation To Tender).
- Development of the solution architecture.
- Implementation of the architecture.
- Programme stage points.
- Publication of System Architecture Document (part of the ADS).
- Major design changes (linked into SAD review).
- Ad hoc assessment to gain a managerial insight into the architectural state of the project.

The output from these strategic review points will be fed to the TA for scrutiny and acceptance of the design. Without TA acceptance the programme or project cannot finalise its procurement phase.

There is an alternative compliancy model for the supplier. In effect the supplier states its level of compliance during Tender and if there is a discrepancy in compliance during testing or operation between the stated compliance and the implementation compliance then the supplier is responsible for any corrective rework. Therefore, the compliance framework will need to be an integral element of all ITTs. To reduce supplier non-compliance there will be a predefined number of reviews conducted by the TA during the design and implementation phase. The timings and scope will feature in the ITT and will be published by the TA.

C.4 Governance

One of the core streams of work that enables a coherent and coordinated architecture to be developed is compliance. Within the overall governance of the ISS4PS the responsibility for measuring compliance forms a key role of the Enterprise Level TA (ELTA). At this level the overall compliance assessment to ISS4PS is of interest and the mechanism for either waiving a particular programme compliance criterion or establishing the solution that delivers compliance across the portfolio is determined. The ELTA focuses on the whole programme portfolio compliance to the ISS4PS and will determine critical activity that needs to be put in place in existing programmes or form key activity in new programmes of work. Ultimately it is the ISS4PS architecture board that determines the suitability of any assessments that it reviews. If an assessment is rejected by the board and it will result in significant work at programme, level then the portfolio board will take ownership of the action to redirect activity.

At the programme level the TA will collate and assess each of the lower level project compliance statements and develop a programme perspective on compliance. It is this assessment that forms the key input to the ELTA overall assessment of programme compliance. Any issues that will impact the delivery of compliance to the ISS4PS at the enterprise level will be escalated for action by the board.

At the project level, compliance forms part of the TA role. At this level, it is essential to ensure that the supplier is complying with the ISS4PS. At this level, there is a degree of compliance for design and delivery. Any assessments that will impact the wider benefits of delivering the ISS4PS will be escalated to the ISS4PS Implementation Programme Board.

C.5 ISS4PS Policy Alignment

Each section in the following paragraphs outlines how each Architectural Principle maps back to the policies of ISS4PS as detailed in Volume 1 of the strategy.

Policy 1 - Define governance

"The Home Office, in conjunction with ACPO and APA, will define governance arrangements for police IT as part of police reform."

Architectural Principles Applied: Governance
Technical Assurance
Adopt Formal Methodologies

Policy 2 - Securing alignment across the Forces

"Chief Constables, in partnership with their Police Authority, will ensure that local IS/ICT strategies are guided by ISS4PS and are compliant with it."

Policy 3 - Make national programmes accountable

"Senior Responsible Owners for national programmes, in partnership with their Programme Board, will adopt ISS4PS and oversee compliance with it."

Policy 4 - Creating an assurance function

"The Home Office will establish an assurance function for police IS and ICT as part of police reform."

Architectural Principles Applied: Governance

Policy 5 - Delivering national initiatives

"All national programmes will use a common programme management framework and approach that complies with the ISS4PS Guidelines for National Solutions and the OGC Gateway Process."

Architectural Principles Applied: Business Agility
Business Event Driven Systems
Common Use Applications
Ease of Use
Total Cost of Ownership (TCO)

Policy 6 - Engaging with industry

"The Police Service will establish a service-wide approach for engaging with industry and suppliers, approving products and procuring solutions."

Architectural Principles Applied: Control Technical Diversity
Proven Standards and Technology

Policy 7 - Sharing information and services

"The Police Service will create a joined-up service for information sharing across all Forces and appropriate partner agencies."

Architectural Principles Applied: Common Vocabulary and Data Definitions
Data is Accessible
Data is Shared
Data Assurance
Data Stewardship
Extended Information and Service Environment

Policy 8 - Managing information

"The Police Service will define common information management processes to ensure that information is created, reviewed, retained, deleted, owned and shared in a consistent way across Forces."

Architectural Principles Applied: Common Vocabulary and Data Definitions
Reduce Integration complexity

Policy 9 - Empowering police officers and staff

"All ICT-based initiatives, both national and local, will make full and detailed provision for the needs of Police Officers and staff in the professional fulfilment of their work."

Architectural Principles Applied: Presentation
Ease of Use

Policy 10 - Deploying common services to citizens

"Police Forces will deploy common services for the public that provide a consistent experience and level of service for all citizens, as far as possible, irrespective of location."

Architectural Principles Applied: Business Agility
Resilience

Policy 11- Shaping the future of police ICT

"The Police Service will harmonise policing business processes and champion the development of new solutions, making best use of local and national innovation."

Architectural Principles Applied: Proven Standards and Technology
Common Use Applications
Control Technical Diversity
Ease of Use
Interoperability
Maximisation of Overall Business Benefit
Proven Standards and Technology
Technology Independence
Total Cost of Ownership (TCO)

Policy 12 - Adopting a common architecture

"The Police Service will define and adopt a common technical architecture using common standards and products where appropiate."

Architectural Principles Applied: Proven Standards and Technology
Business Agility
Common Use Applications
Control Technical Diversity
Ease of Use
Interoperability
Maximisation of Overall Business Benefit
Technology Independence
Total Cost of Ownership (TCO)

Policy 13 - Deploying corporate solutions

"Police Forces will implement corporate solutions wherever they have been approved."

Architectural Principles Applied: Presentation
Proven Standards and Technology
Resilience
Technology Independence
Total Cost of Ownership (TCO)

Policy 14 - Coordinating service management

"Police Forces will adopt and implement a common approach to service management, based on the IT Infrastructure Library (ITIL) model."

Architectural Principles Applied: Service Management and Service Delivery

C.6 Compliance Checklists

The following checklists provide a series of questions that will need to be complied with for each programme or project supplier that seeks to gain ISS4PS compliancy. The checklists are not exhaustive and it is anticipated that these will evolve over time.

There are five major elements to achieving the ISS4PS compliance that need to be considered as an integral part of developing a programme or project:

- **Business led development**

  The ISS4PS is not an end in itself but is specifically designed to support the police business and ensure that the IT support is as effective as possible. Hence IT solutions must support operational policing and be considered as part of an overall business process.

- **Use of standards**

  The ISS4PS mandates a common technical architecture based on the use of open standards and a common infrastructure. Programmes and projects must be developed and implemented to ensure that applications can be accessed in a standard way and corporate solutions can be implemented.

- **Architectural compliance**

  The ISS4PS promotes the use of a service-oriented enterprise and architecture using new technologies and principles. The application architecture and supporting infrastructure must be designed to achieve compliance.

- **Information sharing**

  The way that data is structured, stored and accessed must enable end-users both within Forces, CJOs and external agencies to access the correct information required at the point of use.

- **Delivery**

  Programmes and projects must be focussed and organised to achieve their business objectives. This implies governance, management and product assurance must be properly applied.

Although not directly relating to the provision of deliverables other than software within the Police Enterprise (such as networks or other forms of infrastructure), there will be a series of compliance checklists developed to consider these areas. While the Architectural Principles and checklists outlined below are predominantly aimed at software, there are numerous Architectural Principles that should and will apply to non-software based deliverables.

The practical implications of these elements are considered in more detail below. The checklists are directly related to the underlying enterprise architecture.

Business Led Development

The underlying purpose of both programmes and projects is to enable business objectives to be satisfied. There are five compliancy checklists defined as follows, in addition to the alignment of business processes across the Forces:

- Defined Business Requirements.
- Maximisation of Overall Business Benefits.
- Ease of Use.
- Business Agility.
- Business Continuity.

Defined Business Requirements

Architectural Principle:	Business Requirements
Statement:	Clear measurable business requirements must be established and maintained throughout the life cycle of a programme or project.
Implications:	Clear definitions of functional and non-functional requirements are essential to successful delivery of any programme or project. Each requirement must be specified in a manner which is unambiguous, measurable and achievable. The requirements must include compliance to the ISS4PS and compliance to relevant legislation (wherever applicable). There is no direct mention of either performance or scalability within this Architectural Principle as it is envisioned that the requirements for these aspects will vary too much between programmes. Thus, the details concerning performance and scalability should be dealt with in the project or programme definition. Police business is subject to a continual process of change (eg, mandatory legislative changes). The requirements specification must be placed under configuration management control. Change management processes must be developed and implemented in a manner, which enables legitimate business needs to be addressed responsively.
Compliancy Assessment:	It is recognised that requirements can be documented using different methods and formats. What is best for a small project is different from that of a large programme. Compliancy will not be assessed against a specific standard but must illustrate fitness for purpose. Requirements documentation must be approved by users through a QA review process compliant with PRINCE2. This documentation must be kept up to date through use of a formal change control process. Reviewers must also include technical assurance.
Compliance Checklist:	✔ Approved and current requirements documentation. ✔ Requirements documentation reviewed and under configuration management control.

Maximisation of Overall Business Benefit

Architectural Principle:	Maximise Overall Benefit to both the Business and Enterprise
Statement:	Information management decisions are made to provide maximum benefit to both the police business and the Enterprise.
Implications:	Programmes and projects are developed using a business-lead approach to ensure requirements are met. Benefits management must be applied throughout the life cycle of the programme or project. The preferred business solution and technical infrastructure should be considered as the 'global optimum' of possible solutions. That is, the overall solution may not be the best in certain areas ('local optima') but be the best overall to achieve clear business benefits. A framework must be implemented which not only identifies such a globally optimum solution from all of the options that must be considered, but also manages this solution at an Enterprise level. The required framework is not a passive role which monitors reviews and audits the work undertaken, but an active role of determining the solution for the programme or project.
Compliancy Assessment:	Programmes and projects will be assessed on their ability to deliver benefits to the users and the enterprise. Further collateral investment must be made during the early programmes. These will produce the services that will enable cost savings to be made further down the line. Local and national programmes and projects need to be aware of work that is either planned or completed to ensure that maximum reuse is made, where appropriate. To this end, compliance must encompass the establishment of the CIO functions as outlined in Volume 1.
Compliance Checklist:	✔ Benefits management is carried out in accordance with MSP (Management of Successful Programmes). ✔ Proactive technical assurance is applied in support of an optimum solution. ✔ Programmes and projects must provide collateral investment to the Enterprise where applicable. ✔ Design and document the application to achieve maximum reuse. ✔ Ensure that services and interfaces can be provided to the enterprise, where appropriate.

Ease of Use

Architectural Principle:	Ease Of Use – standardisation of the Human Computer Interface
Statement:	Applications must be easy to use. The underlying technology is transparent to users, so they can concentrate on tasks at hand.
Implications:	There is a need for a standard presentation to users which gives a similar 'look and feel' to applications and minimises training requirements. All applications must be compliant to the ISS4PS Style Guide. All local and national applications should be designed making specific reference to the style guide.
Compliancy Assessment:	All user interfaces must comply with the ISS4PS Style Guide version 3.1 or later.
Compliance Checklist:	✔ Design documentation approved as compliant by ETA. ✔ Implementation signed off as acceptable by users and ETA.

Business Agility

Architectural Principle:	Business Agility
Statement:	Police systems need to be able to adapt to change. Each discrete business function needs to be made up of a series of coarse-grained services that allow procedural changes to be implemented easily.
Implications:	Systems need to be designed and built to be able to adapt to changes. This implies separation and modelling of business processes such that composite applications can be built from existing business services and components. Coarse-grained services should be used which are linked to form a single business process, thereby allowing changes in the workflow to be implemented with minimal technical work. These services must be published in the ISS4PS Service and Technology library.
Compliancy Assessment:	Attention needs to be paid to the design of components, which are assembled to provide reusable services not just within the application but also in the wider enterprise. Service interfaces must be defined and published in a Service and Technology Library to enable intelligent design and integration decisions to be made.
Compliance Checklist:	✔ System design will be reviewed by the Technical Authority. ✔ Service interfaces defined and published in a service library.

Business Continuity

Architectural Principle:	Business Continuity
Statement:	Police Enterprise operations need to be maintained while experiencing system interruptions.
Implications:	The risk of business interruption, together with criticality and impact on the overall Police Enterprise, must be established in advance to determine what level of continuity is required and identify an appropriate recovery plan. This must be managed in accordance with BS15000 (ITIL) standards. Recoverability, redundancy and maintainability should be addressed at the time of design.
Compliancy Assessment:	Systems will be assessed on their business continuity plans and how these interface with the wider business continuity plans. Other aspects that require assessment will be the ability to restore the system to a known state following a system outage or loss of function or other withdrawal of service. Further work will be completed to establish the format and best practice that is applicable to highly available systems.
Compliance Checklist:	✔ Agreed Business Continuity documentation in accordance with BS15000 (ITIL) standards. ✔ Transition of services during the implementation phase to show how the transition supports business continuity. ✔ Testing to include business continuity plan and procedures.

Use of Standards

By adopting and utilising standards across the enterprise, greater understanding and interoperability can be achieved. There are four compliancy checklists to meet this condition:

- Proven Standards and Technology.
- Adopt Standard Methodologies.
- Control Technical Diversity.
- Interoperability.

Proven Standards and Technology

Architectural Principle:	Proven Standards and Technology
Statement:	Products must, wherever possible, use commercially viable standards based on those found in the SIB.
Implications:	The Police Service and more importantly local Forces who control their own budget must ensure that they do not adopt a 'technology for technology's sake' attitude. It is more important to produce robustness and reliability than to have systems produced with cutting-edge technology. In the long term, keeping about a year behind current development technologies is a safe way of offsetting the technology risk but at the same time being able to adopt new, proven techniques.
Compliancy Assessment:	Assessment will be based on a product list (issued following a future study) and the SIB, both of which will undergo regular reviews to ensure that the Police Service as a whole is getting the maximum benefit from the technology that is available. The SIB will predominantly consist of open standards and protocols as this will remove the potential for vendor lock-in.
Compliance Checklist:	✔ The project or programme must comply with the standards and protocols listed in the SIB. ✔ Where a need is established to use either a piece of technology or emerging standard for a particular application, approval must be sought from the Enterprise TA.

Adopt Formal Methodologies

Architectural Principle:	Adopt Formal Methodologies
Statement:	The Police Service will employ formal practices, methods and tools for all stages of a business-led programme and project. This will include the design, construction and implementation of ICT systems.
Implications:	Adoption of formal processes for design and development will result in a high level of consistency. Where improvements to the process are made these will be reflected across all aspects of the design cycle.

Compliancy Assessment:	In association with the TRM, further work should establish both best practice in terms of development work and project and programme frameworks. Programme and project best practice will be mandatory.
Compliance Checklist:	✔ Programmes use OGC MSP. ✔ Projects adopt PRINCE2. ✔ All development must show compliance to a formal design method.

Control Technical Diversity

Architectural Principle:	**Control Technical Diversity**
Statement:	Technological diversity is controlled to minimise unnecessary cost of maintaining expertise in and integration between different environments.
Implications:	Policies, standards, and procedures that govern acquisition of technology must be tied directly to this Architectural Principle. Technology choices will be constrained by the flexibility of the technology blueprint. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be established. The technology baseline is not being frozen. Technology advances will be incorporated into the technology blueprint if they are compatible with the current infrastructure, if it provides an improvement in operational efficiency, or if it is a required capability that has been successfully demonstrated.
Compliancy Assessment:	Ensure that the proposed application or service conforms to the standards as listed in the Standards Information Base. Until the SIB is developed, use the list of standards provided in Annex A.
Compliance Checklist:	✔ Products and services must conform to the standards defined in either the SIB or the list of standards provided in Annex A.

Interoperability

Architectural Principle:	**Interoperability**
Statement:	Software and hardware should conform to defined standards that promote interoperability for data, applications and technology.
Implications:	Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution. The use of open standards as opposed to vendor specific standards provides a mechanism that prevents 'vendor lock-in', enabling change to platforms to occur. A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established. Existing IT platforms must be identified and appropriately documented and plans put in place for a migration to the Enterprise Service Bus.

Compliancy Assessment:

Assessment will be based on the ability for systems to interact with each another. Particular focus will be given to the technology and standards used to provide interfaces to external systems or to expose functionality across the Enterprise Service Bus.

Reviews must be conducted at appropriate points to establish the potential to reuse the information contained in other systems or business processes.

The use of common industry-wide standards that exist in the SIB must also be assessed and any non-compliance must be approved by the Enterprise TA.

Compliance Checklist:

- ✔ All interchange information must be compliant with CorXML and CorDM.
- ✔ The use of proprietary standards both within the application and as transport must be reviewed and approved by the Enterprise TA.
- ✔ All ICT systems and their purpose must be documented to enable the potential for data or component reuse.
- ✔ System design will be reviewed by the Technical Authority.

Architectural compliance

Compliance at the architectural level is crucial to ensure that solutions are consistent and available across the enterprise. There are six compliancy checklists defined as follows:

- Presentation.
- Business Event Driven Systems.
- Common Use Applications.
- Resilience.
- Reduce Integration Complexity.
- Technology Independence.

Presentation

Architectural Principle:	**Multiple delivery channels and devices**
Statement:	Information systems must support multiple delivery channels and devices to the wider community.
Implications:	As the blurring of the classic channels of delivery occurs there is an overwhelming need to encompass these potential delivery mechanisms as early as possible. Investigation into the various Force developments as well as suitable technologies will be completed prior to recommendations being made.
Compliancy Assessment:	To enable the deployment of applications to devices other than a ‘standard’ desktop browser-based design, and techniques must be adopted at the presentation layer. Whatever technology is adopted, there must be a separation between the content and the style to enable redevelopment of the user interface to occur without impact on the underlying application.
Compliance Checklist:	✔ Adopt the techniques outlined in the ISS4PS Style Guide until further research into the device types has been completed. ✔ Applications must ensure that there is a separation between the presentation and content of an application.

Business Event Driven Systems on a Service-Oriented Architecture

Architectural Principle:	Business Event Driven Systems Implemented Using a Service-Oriented Architecture (SOA)
Statement:	Information systems must be designed to be business event driven via a series of well-defined business processes within a Service-Oriented Architecture.
Implications:	Allows easier development and maintenance of large-scale, distributed applications and services involving unpredictable and/or asynchronous occurrences. Allows new and existing applications and services to be assembled, reassembled, and reconfigured easily and inexpensively. Promotes component and service reuse, therefore enabling a more agile and bug-free development environment. Short-term benefits: Allows easier customization because the design is more responsive to dynamic processes. Long-term benefits: Allows system to become more accurate and synchronized closer to real-time changes.
Compliancy Assessment:	Systems must be designed based on the use of Service-Oriented Architecture. Integration between services and applications will use an Enterprise Service Bus (ESB). This must be documented and reviewed to show underlying business services and processes. Without adequate documentation, the interaction between the associated functions within a process cannot be matched. This must include details of error handling.
Compliance Checklist:	✔ Design based on the use of an SOA and ESB. ✔ Architecture approved by TA. ✔ Documentation produced describing the end-to-end business process, including exceptions and manual overrides. ✔ Documentation produced detailing the escalation and delegation procedures to ensure that data / information is not trapped waiting for interaction or approval to occur. ✔ Test scripts produced for each event and error conditions.

Common Use Applications

Architectural Principle:	Common Use Applications
Statement:	Development of common components used across the Police Enterprise is preferred over the development of similar to, or duplicate components used within different applications.
Implications:	Organisations or groups will not be allowed to develop capabilities for their own use that are similar to or duplicates of Enterprise-wide capabilities. Data and information used to support the Police Enterprise decision making body will be standardised. Use of existing common components, together with development of potential common components, must be considered as an integral part of the design process. The TA must identify candidate components for inclusion in the wider Enterprise. A business case may need to be made to support collateral investment. The resulting capability will become part of the Police Enterprise-wide system, and the data it produces will be shared across the Enterprise. If there is a specific need within the Application to develop a variant to an existing common component, this must be approved and documented.

Compliancy Assessment:	Particular focus needs to be put on the analysis of both existing and future applications with a view to identifying common functionality to be implemented as accessible services as early as possible. Further criteria such as the adoption of existing force-based or centrally-provided services to maximise the reuse that can occur from a single implementation are in line with this Architectural Principle.
Compliance Checklist:	✔ New applications and programmes to identify common services during design. ✔ Collateral investment approved to provide common services to other applications. ✔ Common services provided centrally (security model, software factories) at either local Force or enterprise level. ✔ Any Force non-compliance approved by Enterprise TA within a compliance review.

Resilience

Architectural Principle:	**Resilience**
Statement:	Information systems that support business activities must be resilient robust, responsive and reliable, with the appropriate redundancy to protect against failure.
Implications:	Resilience, as opposed to Business Continuity, focuses upon the inherent system features which provide high availability as opposed to environment. Resilience can be effectively split into four main areas: • Business Resilience, which is the degree to which the enterprise continues to function properly under abnormal conditions or circumstances. • Application Resilience, which is the degree to which an application continues to function properly under abnormal conditions or circumstances. • Hardware Resilience, which is the degree to which a hardware component continues to function properly under abnormal conditions or circumstances. • Software Resilience, which is the degree to which a software component continues to function properly under abnormal conditions or circumstances. These four areas need to have mechanisms in place to address the issue of Resilience.
Compliancy Assessment:	Assessment will be based on the ability of an application to fulfil the four areas outlined above.
Compliance Checklist:	✔ Applications must be designed with mechanisms to deal with the four major areas listed above. ✔ The implementation of these mechanisms should be designed so that there is the minimum of inconvenience to a user when an abnormal condition occurs. ✔ Design to be reviewed and approved by TA. ✔ Where systems are redundant by design, testing must specifically include such features and illustrate recovery from failure.

Reduce Integration Complexity

Architectural Principle:	Reduce Integration Complexity
Statement:	Reducing integration complexity will enable integration and interoperability of information systems, not only across Forces but also across other government agencies.
Implications:	Systems must adopt standard interface techniques and parameters to ensure that the language of the enterprise is driven by standards rather than ad hoc interfaces.
Compliancy Assessment:	Assessment will be based on the steps taken by programmes and projects to ensure that the maximum level of reuse can be achieved, either at the framework or data level within the specific application.
Compliance Checklist:	Further assessment will be made on the internal architecture of a specific product with a view to the ease of replacement of individual components or services during the anticipated lifetime of the project – (eg, replacing inbuilt security model with UPSA). ✔ The project or programme must document the internal system architecture in terms of process flow and application architecture. ✔ The project or programme must express all external interfaces in CorXML. ✔ Formal compliance reviews held and documented.

Technology Independence

Architectural Principle:	Technology Independence
Statement:	Applications are independent of specific technology choices and therefore can operate on a variety of technology platforms.
Implications:	Independence of applications from the underlying technology allows applications to be developed, upgraded, and operated in the most cost-effective and timely way The intent of this Architectural Principle is to ensure that applications software is not dependent on specific hardware and operating systems software. This Architectural Principle is dependent on compliance with standards that support portability. For COTS and POTS applications, there may be limited current choices, as many of these applications are technology and platform dependent. Application Programming Interfaces (APIs) will need to be developed to enable legacy applications to interoperate with applications and operating environments developed under the Enterprise architecture. Middleware should be used to decouple applications from specific software solutions.
Compliancy Assessment:	Applications need to be developed to support the broadest possible reach of standards. This should enable a high degree of data portability due to the rejection of proprietary standards.
Compliance Checklist:	✔ Applications must use the Enterprise Service Bus for data exchange between the various tiers of the architecture. ✔ Where possible, development should be based around interpreted code rather than compiled code.

Data Sharing

Data must be shared and exchanged within Forces, between Forces and between the Police Service and other government agencies. Successful data/information sharing relies on a common meaning, syntax, definition and delivery mechanism. It also assumes a sufficient degree of data quality to ensure that accuracy, currency and relevance of information are maintained.

The ISS4PS 'End Game' has a single Global Data Store (GDS) providing a master transactional data store for all data of national importance. This is considered as the most practical way to meet the goals of improved data management, quality and sharing at a national level.

The Architectural Principles of data sharing and management apply to all areas within the Police Service and leads to the following six checklists:

- Common Vocabulary and Data Definitions.
- Data is Accessible.
- Data is Shared.
- Information Assurance.
- Data Stewardship.
- Extended Information and Service Environment.

Common Vocabulary and Data Definitions

Architectural Principle:	**Common Vocabulary and Data Definitions**
Statement:	Data is defined consistently throughout the Police Enterprise, and the definitions are understandable and available to all users.
Implications:	The Police Service CorDM is used to express both the meaning and the data properties for the majority of the data items in the police domain. All programmes and applications will use these definitions for their data requirements. While CorDM contains structural information relating to data clusters, the standards are derived from a logical model and represent all data items that are permissible within a data object.
Compliancy Assessment:	All data models for programmes and applications must be based around CorDM to ensure that common data definitions are used throughout the enterprise. In terms of establishing a common data vocabulary, a data dictionary is being established that will provide the semantic definition for data attributes.
Compliance Checklist:	✔ Each programme or project must establish a logical data model that provides a one-to-one mapping to the CorDM logical model. ✔ Each programme or application must establish a data dictionary that provides semantic definitions for all data attributes used within the product. ✔ The CorDM compliance framework must be completed by all programmes and projects.

Data is Accessible

Architectural Principle:	Data is Accessible
Statement:	Data is accessible for users to perform their functions.
Implications:	Accessibility involves the ease with which users obtain information. The way data is accessed and displayed must be sufficiently adaptable to meet a wide range of Enterprise users and their corresponding methods of access. Data held in different locations must be capable of being combined to provide a complete composite picture of the data. This will rely on a duplicate match service which must resolve potential duplicate data items according to business rules. Services are also required to inform users when specific data is updated or removed. For example a stolen car reported in Force A may be used in a robbery in Force B. Access to data does not constitute understanding of the data. Personnel should take caution not to misinterpret information. Access to data does not necessarily grant the user access rights to modify or disclose the data.
Compliancy Assessment:	Data which is of 'National Interest' must be made accessible via the CorDM-compliant integrated data store, identified by the phase 1 actions. Additionally, Forces can take this opportunity to align some of their other systems to the CorDM specifications as a precursor to the next phase of ISS4PS strategy.
Compliance Checklist:	✔ Logical data models must be created for all programmes and applications. This must include ownership information. ✔ Mapping must occur between the application logical model and CorDM, highlighting both conformance and non-conformance to the CorDM logical model. ✔ Interfaces must be defined and implemented to allow both query and read-only access to the underlying data. ✔ Services must be provided which allow users to access required data regardless of location and to identify changes to data items.

Data is Shared

Architectural Principle:	Data is Shared
Statement:	Users have access to the data necessary to perform their duties. Therefore, data of a known quality is shared across Police Enterprise functions and organisations.
Implications:	This is one of three closely-related Architectural Principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all organizations within the Enterprise understand the relationship between the value of data, sharing of data, and accessibility to data. To enable data sharing we must develop and abide by a common set of policies, procedures and standards governing data management and access for both the short and the long term. For the short term, to preserve significant investment in legacy systems, there must be an investment in software capable of migrating legacy system data into a shared data environment. There is a need to develop standard data models, data elements, and other metadata that defines this shared environment. In addition, there is a need to develop a repository system for storing this metadata to make it accessible.

	For the long term, as legacy systems are replaced, there is a need to adopt and enforce common data access policies and guidelines for new application developers to ensure that data in new applications remains available to the shared environment, and that data in the shared environment can continue to be used by the new applications. For both the short term and the long term we must adopt common methods and tools for creating, maintaining and accessing the data shared across the Enterprise. This Architectural Principle of data sharing will continually impact the principle of data security. Under no circumstances will the data sharing principle cause the security framework to be compromised. Data made available for sharing will have to be relied upon by all users to execute their respective tasks. This will ensure that the most accurate and timely data is relied upon for decision making. Shared data will become the Enterprise-wide 'virtual single source' of data.
Compliancy Assessment:	In line with the phases of the strategy, data must be made accessible to other applications. During phase 1, data must be fed via a series of ETLs to the Federated Data Store. In Phases 2 and 3 data must be available via the GDS. There is no enforcement for data other than data of national interest being made available to the query mechanisms in the early phases of the strategy, but there is a process of strong encouragement for Forces to maximise the reuse of data within their own Force boundary.
Compliance Checklist:	✔ Data of national interest must be available from the integrated data store. ✔ The integrated data store must be capable of expressing the data in the CorDM format irrespective of the internal structure. ✔ The integrated data store must support the defined mechanism for queries. ✔ If the integrated data store is not available for whatever reason, the interface which services the request must be capable of responding to requests with a predefined error message indicating that the service is not currently available. ✔ The interface must respect fully any security restrictions associated with either the request or the aggregation of data in a cluster. ✔ The interface must provide a full audit log of both requests received and responses given.

Data Assurance

Architectural Principle:	**Data Assurance**
Statement:	Data is protected from unauthorized use and disclosure. This includes, but is not limited to, protection of pre-decisional, sensitive, source selection sensitive and proprietary information.
Implications:	To provide the required level of assurance, it is necessary to be confident of user identity as well as providing safeguards that users can only access data to which they are entitled. A global approach to security based upon compliance to the Community Security Policy (CSP) and the Unified Police Security Architecture (UPSA) is essential. This will provide a federated approach for identity management, authentication and local and global directory facilities. In order to adequately provide access to open information while maintaining secure information, security needs must be identified and developed at the data level, not the application level. Security must be designed into data elements from the beginning; it cannot be added later. Data security safeguards are required to be put in place to restrict access at the appropriate level. Data owners and/or functional users must determine if data aggregation results in an increased classification level. There is a need for an appropriate policy and procedure to handle this review and variation in classification level.

	All services provided need to ensure that the same level of security is applied to similar data sets. The requirement for security may conflict with other requirements. The associated risks must be balanced against the potential impact where a conflict may arise.
Compliancy Assessment:	A definition of compliancy and Compliancy Matrix for the CSP has been developed. 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'. UPSA will provide a reference implementation for Forces which should be used as the basis of the security model. To support the design process the data security and access requirements must be analysed and documented. This must include the level of access which must be supported for each user role taking into account aggregation of data into data clusters. Programmes must ensure that security is developed in a modular fashion based on common service calls enabling the underlying security model to change and evolve over time.
Compliance Checklist:	✔ Compliancy to CSP. ✔ Implementation of UPSA. ✔ Data security requirements and access documented and baselined. ✔ The correct level of security applied to both individual data items and data clusters. ✔ Security developed using common service calls.

Data Stewardship

Architectural Principle:	**Data Stewardship**
Statement:	Data is an asset that has value to the Enterprise and must be managed accordingly.
Implications:	Stewardship devolves the data 'ownership' issues and allows the data to be available to meet all user needs. This implies that a cultural change from data 'ownership' to data 'stewardship'. Stewards must have the authority and means to manage the data for which they are accountable. The steward is accountable and responsible for the accuracy and currency of their designated data element(s). The role of the data steward is to maintain data quality. This is critical because obsolete, incorrect, or inconsistent data could be passed to enterprise level personnel and adversely affect decisions across the Enterprise. Procedures must be developed and used to prevent and correct errors in the information and to improve those processes that produce flawed data. Data quality will need to be measured and steps taken to improve it. A forum with comprehensive Enterprise-wide representation should decide on process changes suggested by the steward. Since data is an asset of value to the entire Enterprise, data stewards accountable for properly managing the data must be assigned at the Enterprise level.

Compliancy Assessment:	A data steward must be established to ensure that data quality, security and access is given a high enough priority within the Forces. There must be documentation to show the procedures used to establish both the quality and the provenance of the data and source. The data trustee must be involved in the establishment of all data-related requirements and must identify and establish data re-use to promote a holistic approach to data.
Compliance Checklist:	✔ Establish the role of the data steward with agreed Terms of Reference. This must include the authority to force changes on existing business processes where appropriate and establish the overall provision and reuse of data. ✔ Procedures documented to assess both the data quality and the evaluation of the source material. ✔ Evidence of the process available to ensure consistent data quality of the exposed data. ✔ Procedures documented to correct data on submission of a request.

Extended Information and Service Environment

Architectural Principle:	**Extended Information and Service Environment**
Statement:	Information systems should enable and enhance the provision of information to other government services and initiatives to both the public and other agencies.
Implications:	This ability to conduct ‘straight through processing’ (STP) to partner agencies will result in efficiencies of scale and reduction in the man-hours spent exchanging information with government partners.
Compliancy Assessment:	Compliancy is based on the establishment of the integrated data store in phase 1 and the continued development of the following phases. Identification of the external agencies that need to communicate with the Police Service. This will require the establishment of a schema/repository of information required to be exchanged.
Compliance Checklist:	✔ Establish the integrated data store as outlined in phase 1 and drive the business applications from it. ✔ Data identified to be exchanged between the Forces and the external parties. ✔ Adapters provided to translate between CorDM and external schema with integration achieved through an Enterprise Service Bus.

Delivery

The Office of Government Commerce (OGC) recognises the importance of supporting programme and project delivery. Recommendations are embedded within Managing Successful Programmes. A programme requires active management of the changes in business operations and integration of programme deliverables.

This section of the checklist focuses on the management activities and products required for compliance to the ISS4PS. There are five compliancy checklists to achieve successful programme and/or project delivery:

- Governance.
- Protection of Intellectual Property Rights.
- Technical Assurance.
- Service Management and Service Delivery.
- Total Cost of Ownership.

Governance

Architectural Principle:	Governance
Statement:	The strategic level board is responsible for the priorities of capability to meet the enterprise portfolio plan and assure coherent delivery of the corporate level solutions.
Implications:	Effective governance ensures that the programmes and projects can coordinate delivery of multiple objectives, even when there are competing priorities and conflicting goals. An overall accountable body needs to be appointed to assure the delivery of programmes across the enterprise. Governance policies are required that document a set of rules that govern the provision of services and related assets through the stages of identification, planning, development, implementation, operation and review.
Compliancy Assessment:	The recommendations at Annex D require implementing at both the enterprise and local level to ensure suitable governance structures are in place. Senior management must have clearly defined and documented roles and responsibilities that highlight their responsibility to maintain cohesion at an enterprise level. Policies are required to ensure that resources are provided and allocated effectively to meet the demands of the Police Service.
Compliance Checklist:	✔ The governance structures as outlined at Annex D must be adopted and put in place to ensure effective alignment to the ISS4PS strategy. ✔ Terms of reference must be documented and agreed for every role within the programme/project structure. ✔ Governance policies must be specified with documented evidence of compliance. Compliance with these policies will be assured by an effective programme assurance function.

Technical Assurance

Architectural Principle:	Technical Assurance
Statement:	Assurance must be provided that the technical solution supports the required business objectives. This will reinforce the programme or project goals for meeting fit for purpose.
Implications:	An appropriate level of technical assurance must be provided within the programme or project to ensure the solution is not only fit for purpose but fully contributes to and exploits the wider strategic technical environment for Police Service modernisation. Technical assurance will: • Enable the linkage between the top-level strategic direction and the activities required to achieve the strategic objectives. • Ensure that a consistent and coherent system of business policies and procedures, supported by the best possible use of technology, is defined and implemented.
Compliancy Assessment:	A single 'Enterprise Level Technical Authority' (ELTA) has been assigned to define the enterprise technical architecture to be adopted by all Police programmes and projects. Every programme or project is required to include the function of 'Technical Authority' (TA). For small projects a single individual may be sufficient resource to discharge the responsibilities of a TA. In most programmes or projects the TA will lead a team to discharge these responsibilities. The TA will manage a strand of project work with adequate resources for the discharge of the TA function provided by all programmes and projects.
Compliance Checklist:	✔ Agreed Memorandum of Understanding between the ELTA and the Programme SRO. ✔ Technical Authority appointed in accordance with Terms of Reference agreed by the ELTA. ✔ Formal compliance reviews conducted at enterprise and programme level.

Service Management and Service Delivery

Architectural Principle:	Service Management and Service Delivery
Statement:	Service Management and Service Delivery services must be implemented at programme/ project initiation in alignment with IS20000 (ITIL) standards.
Implications:	As the complexity of information systems has increased, together with the importance of their availability to the organisation, it is no longer acceptable to adopt a piecemeal approach to service management and delivery. The Police Service must now take a corporate view of service management. Successful adoption of ITIL based upon the IS20000 (ITIL) standards requires the definition of the processes and tools that will be used to meet best practice. It is essential that future support services are staffed with experienced trained resources.

Compliancy Assessment:	It is recognised that there are different levels of support for ITIL throughout the Police Service and work needs to be undertaken at an Enterprise Level to define common processes and support tools. When these are available, compliance will be required. In the interim, compliancy will be measured directly against ITIL requirements. As a minimum, programme and projects must implement configuration management, change management, release management and problem management. Programmes and projects must illustrate how availability management and capacity management have been addressed. Service Level Agreements (SLAs) must be agreed prior to implementation that support an end-to-end response time for the end-user, the required level of system availability, and application support.
Compliance Checklist:	✔ Configuration management, change management, release management and problem management procedures which are supported by automated tools. ✔ Formal compliance review of availability and capacity management products. ✔ Evidence of compliance to agreed procedures. ✔ Agreed SLAs in place prior to live operation.

Protection of Intellectual Property

Architectural Principle:	**Protection of Intellectual Property Rights (IPR)**
Statement:	The Enterprise IPR must be protected. This protection must be reflected in the ICT Architecture, Implementation, and Governance processes.
Implications:	While protection of IPR assets is the responsibility of all, much of the actual protection is implemented in the ICT domain. Even trust in non-IT processes can be managed by ICT processes (e-mail, mandatory notes, etc.).
Compliancy Assessment:	For in-house developed applications the Police Service will own the intellectual property surrounding both the development and processes that the system fulfils. Where applications are developed externally, the contract should contain provision for the retention of the IPR by the Police Service.
Compliance Checklist:	✔ Tenders for programmes or projects must contain provision for the IPR of the solution to remain within the Service.

Total Cost of Ownership (TCO)

Architectural Principle:	**Total Cost of Ownership (TCO)**
Statement:	TCO for ICT must balance development, support, disaster recovery and retirement costs alongside the costs for flexibility, scalability, ease of use/support over the life cycle of the technology or application.
Implications:	TCO is an assessment that helps an Enterprise to understand how much financial resource will be eaten up if a new piece of technology is brought into the business. A TCO study shows the direct and indirect costs of owning and using any ICT component throughout its life cycle. TCO data attempts to cover all the phases such as acquiring, installing, and managing a company's computers, networks, and applications.
Compliancy Assessment:	All deployments, regardless of the area, should be assessed on the return on investment/total cost of ownership. These figures should form part of the business case used in justifying the financial spend.
Compliance Checklist:	✔ Business cases must include reference to the TCO for a project or programme prior to funding being released.

Annex D Guidelines for National Programmes

Volume 1 defined 14 policies and three phases that relate to the successful delivery of the ISS4PS. This annex focuses on the needs of the two policy groups 'Establishing the Foundations' and 'Delivering Joined-up Services', with specific reference to Policy 5, 'Delivering national initiatives'.

Contents

D.1 Issues

National programmes are managed as specific programmes of work. This does not provide an easy mechanism for managing cross programme interdependencies. This, coupled with a lack of coordination and control across the portfolio, often leads to an increased level of corporate risk within national programmes.

Identifying and providing the right level of resource is a frequent problem when managing programmes. Poor coordination and incorrect resource profiling can result in programme slippage which, in turn, will impact the ability to deliver the expected business benefits.

D.2 Aim

These guidelines aim to provide a framework that reduces the likelihood of programme failure. The OGC quotes the following key reasons for programme failure:

- Not linking the programme delivery to clear strategic priorities.
- Unclear senior management ownership.
- Evaluation of proposals based on price alone.

Tackling these issues is the focus of these guidelines.

D.3 Summary of Approach

The approach used by national programmes is summarised as:

- OGC Managing Successful Programmes (MSP) and PRINCE2 should be used.
- A Portfolio[6] approach will be used to manage the Police Service programmes in order to provide coherent end-to-end alignment of priorities, plans, delivery and roll-out, as well as coordinated business requirements, service levels and end-user requirements.
- An overall Portfolio Responsible Owner will be appointed, possibly in conjunction with a portfolio strategy board, to be accountable for the portfolio and provide an escalation path for SROs of national programmes.
- Enterprise Level Technical Authority (ELTA), Programme Technical Authority and Project Technical Authority roles will be established to ensure technical leadership and guide programmes in meeting the requirements of the ISS4PS.
- A Service Level Authority will be put in place to manage the introduction and operation of ITIL.
- A Procurement Authority will be established to coordinate and provide procurement best practice for national programmes.
- A Programme Assurance and Support Office will be put in place to provide support to national programme SROs and provide best practice advice to Forces.
- When assessing programmes, the whole life cycle costs, including force-level resources, should be taken into account.
- The management regime should include measurable gateway criteria that enforce engagement at the local level and drive through best practice and alignment with the ISS4PS[7].

The roles defined in these guidelines identify the activity that is considered to be essential for the ISS4PS compliance. It is accepted that each of the roles will evolve and be refined by the project and programme using MSP and PRINCE2 frameworks to suit the nature of the programme or project. These are not definitive lists.

6 The definition of portfolio management presented by OGC is used: “Portfolio management is a corporate, strategic level process for coordinating successful delivery across an organisation’s entire set of programmes and projects”.

7 This is covered in more detail in Annex C: ISS4PS Compliance

D.4 Portfolio Responsible Owner

Portfolio Responsible Owner

The Portfolio Responsible Owner role provides the strategic level guidance for all national programmes. It is at this level that the overall investment to deliver the portfolio will be agreed and the priorities for delivery established. The authority for this role could be vested through the portfolio strategy board.

Within MSP this role can be equated to the sponsoring group for national programmes. It retains the overall accountability for all national programmes.

Establish common framework for portfolio management

- Create the right programme environment in terms of commitment from resource providers that enables the capability plan to be delivered.
- Provide a consistent approach to the issue of national programme mandates.
- Provide continued support to the SROs.
- Provide communication support as required by the SROs.
- Provide appropriate endorsement to the SROs in terms of sign-off of key stages.
- Define the scope of business process harmonisation.
- Define and implement a benefits realisation plan aligned to the strategic priorities.

Support the programme assurance function for the portfolio

- Provide the authority for establishing programme interdependencies.
- Provide the leadership and authority required to manage a corporate configuration management process for national programmes.
- Provide support and authority required to enable the prioritisation of resources for national programmes by the assurance office.
- Endorse the approach and provide leadership to determine the right level of programme communication.

Support a corporate risk manager for national programme SROs

- Endorse the corporate risk plan.
- Provide SROs with a prioritised list of risks and advice on the action to manage national risk in national programmes.
- Provide a corporate view on business continuity planning to enable SROs to develop their transition plans.

Support a Technical Authority role at all levels to drive coherence and consistency

- Provide leadership support as necessary to ensure that the global architecture remains cognisant of the business strategy and objectives.
- Approve the investment required to deliver a Technical Reference Model.
- Approve the capabilities that meet the business strategy and objectives.
- Champion the ISS4PS.

Define an investment approvals process that identifies how national programmes will obtain financial commitment from the Police Service and its partners

- Provide a level of assurance that the benefits realisation plan for the National programme portfolio is ade quately budgeted.
- Confirm the programme whole life cycle investment presented by national level SROs is appropriate to meet the benefits realisation plan for the National programme portfolio.
- Provide leadership in resolving investment conflicts between programmes against the priorities set by the National Portfolio to ensure that the benefits realisation plan remains achievable.
- Confirm the relevant approval stages for national programmes with appropriate decision points based around the benefits realisation stages for the National programme portfolio.

Support the national procurement authority role

- Endorse the principles to be deployed nationally.

Support the ISS4PS architecture board

- Provide leadership and direction in terms of architecture decisions that maintain ISS4PS.
- Endorse waivers to the ISS4PS as necessary.
- Endorse the core application and capability presented in the ISS4PS.
- Endorse the overall safety case for the portfolio.

Support the service level authority

- Provide leadership and advice in the provision of variations to ITIL.
- Provide support in terms of endorsing the investment required to meet ITIL by Forces.
- Provide the authority for the Service authority to define the overall Force Service structure and levels required to move to a corporate approach.

D.5 Enterprise Level Technical Authority

Enterprise Level Technical Authority

The Enterprise Level Technical Authority role provides the leadership necessary to ensure that the global architecture remains coherent and aligned with the Capability plan and the Police National ICT Plan. It has the overall accountability for the enterprise architecture that delivers the portfolio.

Maintenance of the ISS4PS procedures, principles and policies

- Provides national level programmes and local Forces with up-to-date procedures and principles and policies to ensure capability delivery.
- Define and refine common technical standards and products – policy 12.

Provide best practice advice and guidance to national programmes and local Forces on implementation of the ISS4PS

- Provide TA resource to programmes for best practice advice.
- Provide guidelines on procurement practices for ISS4PS.

Manage the Technical Reference model implementation

- Provide support for national and local programmes to ensure compliance to ISS4PS.
- Provide assessment of architecture compliance for ISS4PS.
- Provide guidance on the requirements to ensure performance of the national service.

Service support and contracts comply with ISS4PS

- Provide a framework for assessing service support contracts against the requirements of the ISS4PS.
- Provide an audit and review service to national programmes and local Forces.

Disaster recovery plans and guidelines

- Provide the compliance assessment framework to ensure disaster recovery for national services is coherent across all Forces.
- Provide the technical requirements baseline for national programmes.

Infrastructure footprint for the architecture

- Manage the requirements for the national technical footprint across the Police Service estate.
- Determine the life cycle cost for the infrastructure footprint for the architecture.

Architecture board

- Operate and manage the architecture board process and policies.
- Provide best practice guidance to local Forces and national programmes on compliance criteria and tolerance levels.
- Manage the convergence planning to the ISS4PS.
- Assess the level of ISS4PS compliance for all national programmes.
- Maintain and update the definition of ISS4PS compliance.

D.6 Programme Level Technical Authority

Programme Level Technical Authority

For each programme, a programme level technical authority provides the leadership necessary to ensure that national programmes deliver technical solutions that are aligned with the ISS4PS. The role also provides the overall technical lead for the programme.

Implement a Technical interface management process and structure

- Define and implement the interface requirements management policy and procedures between programme projects.
- Ensure that the interface plan complies with the needs of the ISS4PS and the Enterprise Level Technical Authority (ELTA) requirements.
- Audit and review project level interface plans.

Implement best practice advice and guidance

- Provide TA advice to suppliers and ensure compliance with requirements.
- Provide guidelines on procurement practices for the ISS4PS.

Endorse the Technical Reference Model implementation requirements

- Liaise with suppliers to develop a requirement for verification of solution against the Technical Reference Model.
- Ensure compliance against the approved design.

Service support and contracts comply with ISS4PS

- Ensure service support is cognisant of the demands of ISS4PS.
- Ensure that service support is kept abreast of capability development and define the transition to service.

Disaster recovery plans

- Develop appropriate disaster recovery plans for the programme that integrate to the business continuity plans.
- Comply with the national requirements.

Infrastructure footprint for the architecture

- Establish the requirement for the infrastructure required to support the technical footprint from the blue print and ensure sufficient capacity to meet the needs of the programme.

Technical Assurance

- Provide an overall programme approval of the technical elements of the Safety Case.
- Provide an independent review of suppliers.
- Provide an independent view of the compliance with the ISS4PS.

D.7 Project Level Technical Authority

Project Level Technical Authority

For each project, a project level technical authority provides the leadership necessary to ensure that it delivers technical solutions that are aligned with the ISS4PS. The role also provides the overall technical lead for the project.

Ensure that the architecture meets the needs of the ISS4PS

- Corporate Data Model (CorDM) is complied with and as necessary deviation from the standard is clearly noted and approved by the programme board.

Ensure the technical elements of the Safety Case are necessary and sufficient to meet the needs of the business

- Provide an assessment of the supplier Safety Cases and produce a single case for the project.

Establish a technical audit programme that assures the delivery of the supplier service and products

- Existing service providers' migration plans for the technical architecture.
- Programme and project interdependencies have been acknowledged and being managed.
- Business continuity planning to ensure that the business can operate during service migration.
- Compliance criteria for the ISS4PS have been applied and an assessment endorsed by the programme board.

Ensure that the test plan meets the needs of suppliers and complies with the programme standards

- Business resources required to support the test plan can be delivered by the business and are in the business plans.
- Appropriate User Acceptance Tests and System Acceptance Tests are included.
- Compliance with test procedures has been verified.

Implements best practice advice and guidance

- Provide TA advice to project suppliers and ensure compliance to requirements.
- Provide guidelines on procurement for project procurement.

Service support and contracts comply with ISS4PS

- Ensure the project service needs are articulated to the programme service liaison.

Disaster recovery plans

- Develop the technical elements of disaster recovery, taking note of the business needs.
- Comply and verify compliance with the programme requirements.

Infrastructure footprint for the architecture

- Ensure the technical footprint needs are articulated to the programme level.

D.8 Service Level Authority

Service Level Authority

The Service Level Authority provides the overall coordination in defining the common approach to service management, coordinates the implementation of ITIL at the enterprise level, and provides best practice guidance to Forces.

Ensure coherence between the introduction of ITIL at Force level

- Maintain the overall configuration management for ITIL.
- Provide a consistent view of the Force adoption of ITIL.
- Provide common process for ITIL implementation.

Establish the benefits of adopting IS20000

- Provide an independent audit function for Forces to assure implementation of best practice.
- Provide criteria for the implementation of ITIL across Forces.

Provide coherent approach to the implementation of tools to support ITIL

- Define the common toolset, national service management tools and processes.
- Define the common training approach.
- Coordinate national IT service continuity plans.

Develop the integration approach for Forces to enable economies of scale through service improvement

- Determine the disciplines that need to be adopted centrally.
- Provide guidance to Forces.

Manage the national infrastructure service

- Define the SLAs and MOUs for Force service management interfaces.

D.9 Procurement Authority

Procurement Authority

The Procurement Authority provides the leadership necessary to deliver a service-wide approach to engaging with industry, and provides the overall authority for information system procurement practices within the Police Service.

Develop national procurement practices for the delivery of capability

- Provide best practice and advice to Local Forces.
- Provide support and advice to national suppliers on standards.
- Provide the guidelines for engaging with industry.

Provide a national perspective or the procurement of resources to support national programmes

- Where individual programmes are procuring resources for specific disciplines in silos a central body may gain economies of scale from resourcing centrally.

Identify differing procurement options to ensure the delivery of joined-up services

- Identify the best practices from across the Police Service and align procurement principles.

Service-wide approach to engaging with industry

- Establish common procurement standards across the Police Service.
- Provide Common Terms and Conditions and approach to Intellectual Property Rights.
- Adoption of consistent evaluation criteria tools enabling like-for-like evaluations to be made.

D.10 Programme Assurance and Support Office

Programme Assurance and Support Office

The Programme Assurance and Support Office provides the leadership and support that enables coordination and coherency between all national programmes. It delivers the guidance and advice to local programmes on best practice and acts as the assurance and support office for all national programme implementation.

Board coordination

- Provide central resource management for procurement to identify economies of scale from single procurement action.
- Provide guidance and advice to enterprise level boards on the progress of national programmes.
- Provide an audit and assurance process for all programmes.
- Creation and management of a national implementation plan.
- Provide a programme communication plan for the keeping programmes and Forces up to date on the programme portfolio.

Programme support

- Provide support functions defined in MSP and PRINCE2.
- Risk and issues overview for all national programmes.
- Identify and manage the coordination of all national programme interdependencies.
- Provide key audit reports to national programmes.
- Provide support to the procurement authority in terms of national programme procurement strategies and approaches.
- Coordinate and assure the right level of support for national programmes (provide an escalation path to local Forces).

Configuration management

- Provide advice and guidance to all parties on best practice for change management.
- Ensure that the configuration management process of service and delivery remain complementary.
- Provide the master change log for all national programmes.
- Provide the master configuration management reference library for national programmes.
- Provide guidelines for national and Force configuration management best practice.
- Provide and manage a national compliance plan for the ISS4PS.

Technical assurance

- Assess compliance to the ISS4PS.
- Ensure capability solutions meet the business plan.
- Assure the quality of services.
- Verify supplier Safety Cases.
- Manage the configuration plans for the Enterprise architecture board.
- Ensure national programmes comply with requirements and safety cases.
- Ensure data stewardship is correctly managed within programmes and projects.
- Assurance of suppliers.
- Provide a technical risk assessment of national programmes.

Business assurance

- Coherence between the core business processes that cut across CJIT, CPDG boundaries and Police Forces.
- Independent view of the transition planning to ensure business continuity.
- Coordinate the resource requirements at national programme level.
- Assure the delivery of the Enterprise business benefit realisation plans.
- Assure that the transition planning can be sustained by the business.
- Ensure correct level of SLA and MOUs are in place and maintained.
- Coordinate and ensure control of the business requirements for national level programmes.
- Ensure that the programme capabilities are linked to benefits that deliver the overall portfolio benefits.

D.11 Steps to Adopt a Portfolio Approach

To move towards a portfolio approach requires specific activities to be conducted across the enterprise. The following steps are prerequisites to using a portfolio approach:

Step 1 – Ensure that MSP is implemented in all programmes and PRINCE2 is implemented in all projects. This will enable a common standard and framework on which all levels of the organisation can communicate effectively.

Step 2 – Each Force implements a single programme assurance/programme support office to act as the focal point for the programme assurance and support function.

- Each Force establishes a single programme support office.
- Programme assurance and support established and guidelines developed for management.
- Central resource view established.

Step 3 – Establish a first draft portfolio

- Each Force compiles a portfolio of programmes.
- Combined Police Delivery Groups agree which Force-level programmes should be considered local, and which national.
- PITO/NPIA confirm what enterprise-wide programmes exist and ensure SROs are appointed for each.
- Align Force-level and enterprise programmes.
- Establish a consolidated list of benefits for the portfolio.
- Determine the portfolio investment.
- The Enterprise Level Technical Authority (once appointed) assesses technical risk.
- The Portfolio is aligned against risk and finance.

Step 4 – Assess the enterprise business strategy against needs

- Align existing portfolio to business strategy.
- Establish delivery profile timeframe.
- Compile a risk profile for the portfolio.
- Turn off programmes that do not meet the enterprise needs.
- Assess the level of risk for acceptability.
- Assess the benefit of continuing some programmes that do not support the business strategy.
- Confirm the financial assessment of enterprise portfolio.
- Implement a financial and strategic assessment scrutiny process for all programmes.
- Confirm the level of investment for the portfolio.
- Determine the allocation of budgets.

Step 5 – Prioritise the portfolio

- Assess all programmes and realign to deliver the portfolio.
- Determine the level of resource required to deliver and gain agreement from Forces and programmes.
- Evaluate the level of risk for the portfolio in terms of delivery.
- Reallocate Force IS/ICT budgets based on their portfolios and the overall portfolio.

Annex E Criteria for Corporate Solutions

ISS4PS Policy 13 concerns corporate solutions; national solutions that have been developed or procured by the Police Service to be used by Forces. Corporate solutions would be provided through central or local services that are rolled out to appropriate Forces to meet a business need. Corporate solutions may be:

1. **Procured products or bespoke developments.**

2. **Applications or infrastructure.**

3. **Products that include standardisation of business processes as well as technology.**

Contents

E.1 Benefit Justification

Policy 13: Deploying corporate solutions
Police Forces will implement corporate solutions wherever they have been approved.

Before implementing or procuring corporate solutions, they must be justified by a business case that identifies costs and benefits to both the Police Service as a whole and the individual Force. All business cases relating to corporate solutions need to be approved by ACPO/NPIA and, if necessary, the portfolio planning board[8]. The implementation of the corporate solution may involve more than one Force and/or CPDG[9].

In addition to the usual content of a business case, a corporate level business case needs to quantify the impact on the Police Service, as a whole, if an individual Force does not implement the corporate solution. This impact statement needs to consider the business impact and the compliance to ISS4PS.

Example:
If one Police Force does not implement a corporate payroll system, it is unlikely that the national impact in terms of operations will be huge. However, it may have future investment costs and considerations. Whereas, if one Police Force does not implement a corporate solution that supports a national database, other Police Forces may not have access to the complete set of national data. The impact to the Police Service as a whole could be significant. This assessment becomes a corporate level risk when the business case has been accepted and needs to be managed appropriately at the enterprise level.

Forces will adopt corporate solutions unless one of the criteria listed in the following table is applicable. If the criterion is applicable, the Force should conduct a formal impact assessment that can be submitted to the Enterprise portfolio planning board for action. The table lists the criteria to be used when deciding not to adopt a corporate solution within a Force.

8 The Enterprise portfolio management board is the overall accountable body that is responsible for the successful delivery of the enterprise portfolio. The CIO appointment at the enterprise level is responsible for the IS/ICT portfolio which forms a sub-set of the overall enterprise portfolio.
9 Combined Police Delivery Group.

E.2 Criteria

Domain	Criteria	Additional Actions
1. Disruption to business	Will impact the Force's delivery of its PPAF targets.	Issue to be raised and a full impact assessment presented to ACPO or the Enterprise portfolio planning board for action as appropriate.
	Will adversely impact the Force service contracts.	Issue to be raised and a full impact assessment presented to the Programme SRO or ACPO as appropriate.
2. Resources	There are insufficient resources available to implement the corporate solution.	Issue to be raised and a full impact assessment presented to the Enterprise portfolio planning Board.
	The cost to the Force of hiring temporary resources is outside the approved Force investment plan.	Issue to be raised and a full impact assessment presented to the programme SRO or ACPO as appropriate.
3. Prerequisites not met	The prerequisites that a Force requires in order to implement the corporate solution have not been met.	The Programme SRO will escalate the issues to the Enterprise portfolio planning board for action.
4. Incompatible architecture	The technical architecture for the corporate solution is incompatible with the architecture of existing Force IS/ICT.	The ISS4PS architecture board will assess the impact of achieving the overall ISS4PS architecture and present the assessment to the Portfolio planning board for a decision on how to manage the implementation Plan.
5. Existing solution	There is an existing solution that already meets the business requirements offered by the corporate solution, including meeting national requirements.	The ISS4PS architecture board will assess the impact against the ISS4PS compliance standards and make a recommendation to the Enterprise portfolio of an expected migration plan.
6. High cost of implementation	The cost of implementation in the Force is significantly higher than the cost in the programme business case.	The SRO to raise an issue for escalation to ACPO or the enterprise portfolio planning board for action.
	The cost of implementing the corporate solution cannot be funded from the approved Force investment plan.	Issue to be raised and a full impact assessment presented to the Programme SRO or ACPO as appropriate. If not an active programme the variations are to be raised to ACPO and, as appropriate, assessed by the ISS4PS architecture board.
7. Business requirements not met	Business requirements have changed in the Force and the corporate solution no longer meets the full requirement.	Issue raised to the programme SRO for action. It may be necessary to amend the scope of the programme.
	The level of performance offered by the corporate solution does not meet the demands of the Force.	Full impact assessment raised to the enterprise portfolio planning board for action. If this is not an active programme then the changes need to be raised via ACPO.

Domain	Criteria	Additional Actions
8. Alternative solution	There is another solution available that meets the full business requirements, including national requirements, providing more than the minimum requirements set. (Alternative corporate solutions on a like-for-like basis are the responsibility of the ISS4PS architecture board to approve).	ISS4PS architecture board will make a formal assessment of the solutions and, if applicable, include the product on the approved products list.
9. Minimal business benefits	The business benefits identified are minimal for the Force.	Issue raised to the programme SRO for action. There may be justification to halt the implementation at a specific Force.

Annex F Principles & Actions

This Annex provides a summary of all the Principles and actions defined in Volume 2 of the ISS4PS, Version 3.

Contents

F.1 Frameworks, References and Standards

Policy	Principle	Action/ Deliverable	Action On	Action number	Effort		
					Phase 1	Phase 2	Phase 3
12	An ISS4PS Enterprise Architecture Framework will be used to understand, plan and document the business and technology landscape.	Deliver and populate the ISS4PS EAF tool/ Operational and fully populated EAF implementation.	PITO/NPIA and the Forces	1	✔	✔	
12	A freely available SIB will be created, published and maintained to support the implementation and procurement of ISS4PS compliant systems.	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.	PITO/NPIA	2	✔		
12	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.	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.	Technical Authority	3	✔	✔	
12	A reference implementation of the ISS4PS technical architecture will be provided.	Develop the ISS4PS reference implementation/A full implementation of the ISS4PS Technical Architecture End-Game and a set of best practices and guidance.	PITO/NPIA	4	✔	✔	
12	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.	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.	PITO/NPIA	5	✔	✔	

F.2 Application Architecture

Policy	Principle	Action/ Deliverable	Action On	Action number	Effort		
					Phase 1	Phase 2	Phase 3
12	The architectural basis for new applications will be shared services using a Service-Oriented Architecture. New initiatives requiring integration between services and applications will use an Enterprise Service Bus (ESB).	Select one or more ESB products suitable for the Police Service at local and national levels/ A list of recommended Enterprise Service Bus products.	Technical Authority	6		✔	
12	New applications will be built from services, wherever an applicable component or service has been identified as a police standard.	Identify, build 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.	Technical Authority	7	✔	✔	
13	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. New applications will allow for access from a range of client devices.	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.	Technical Authority	8	✔ ✔	✔ ✔	

F.3 Infrastructure

Policy	Principle	Action/ Deliverable	Action On	Action number	Effort		
					Phase 1	Phase 2	Phase 3
7	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 simply across all Forces.	Identify, agree and implement minimum standards for Police Service infrastructure/A master list of common infrastructure products, standards and processes.	PITO/NPIA and the Technical Authority	9	✔		
12	The Police Service will implement high performance, scalable, rugged and flexible networks that will meet a minimum set of standards.	Agree requirements and implement national network/ PNN3 National Network.	PITO/NPIA	10	✔	✔	
		Agree requirements for Force networks, assess Force network against requirements and upgrade where necessary/ Force network assessments and Force networks upgraded.	PITO/NPIA	11	✔		
12	The ISS4PS will support mobile working for the Police Service throughout the stepwise migration to the 'End Game'.	Develop standards to be applied to the use of mobile information/ Standards for the use of mobile information.	PITO/NPIA	12	✔		
		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 in the use of mobile services.	PITO/NPIA	13	✔		
		Develop technology demonstrators for proof of concept of proposed technology/ Technology demonstrators to form part of the technical reference model.	PITO/NPIA	14	✔	✔	

F.4 Information

Policy	Principle	Action/ Deliverable	Action On	Action number	Effort		
					Phase 1	Phase 2	Phase 3
12	Forces will implement a Force-level integrated data store as a stepping-stone to using a Global Data Store. A Global Data Store will be used as a national data store for all core data within the Police Service.	Implement integrated data stores/ A definition of Core Data, GDS data model and a populated and operational GDS.	Forces	15	✔		
		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.	PITO/NPIA and Technical Authority	16	✔	✔	
		Perform detailed technical analysis for the GDS, initiate procurement and begin to populate the GDS in conjunction with an existing major national programme/A definition of core data, GDS data model and a populated and operational GDS.	PITO/NPIA	17	✔	✔	
8	The Police Service will implement intelligent services that provide unstructured and semi-structured data as a source of actionable, time-critical business intelligence.	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.	PITO/NPIA	18		✔	✔
8	The new Code of Practice for Police Information Management will be used as the basis for continuous improvement in data quality.	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.	PITO/NPIA and Central Customer	19	✔	✔	
		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.	PITO/NPIA and Central Customer	20		✔	
		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.	PITO/NPIA and Central Customer	21		✔	
7 & 8	Data exchange and interoperability standards will be used throughout the Police Service based on open standards technologies.	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.	PITO/NPIA	22		✔	✔

F.5 Information Assurance

Policy	Principle	Action/ Deliverable	Action On	Action number	Effort Phase 1	Effort Phase 2	Effort Phase 3
11	The Community Security Policy (CSP) will be implemented throughout the Police Service. As part of the CSP, a community security architecture will be adopted.	Forces and national services will implement the Community Security Policy by the end of 2005/ A compliancy matrix measuring compliance against the Community Security Architecture.	Forces and PITO/NPIA	23	✔		
7 & 8	A standard method of managing the digital identities and roles of police officers and staff will be implemented throughout the Police Service.	Implement tools and central infrastructure for managing digital identities and roles (currently within the UPSA project)/ An identity and access management infrastructure.	PITO/NPIA	24	✔		
		Consolidate local directories into an enterprise directory(ies). Implement the enterprise directory using the Police Schema/ A consolidation of Force directories to a manageable number.	Forces	25	✔	✔	
		Implement national 118 Directory/ The Police 118 Directory populated with details of staff from all Forces.	PITO/NPIA and Forces	26	✔	✔	
11	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.	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.	Forces and PITO/NPIA	27	✔		
		Develop and test response plans at Force and national levels/ Validate response plans.	Forces and PITO/NPIA	28	✔		
		Develop mechanism for coordinating incidents to provide a Service-wide view of threats/ Agreed and validated plans for responding to an information assurance incident.	PITO/NPIA	29	✔		

F.6 Governance for ISS4PS Delivery

Policy	Principle	Action/ Deliverable	Action On	Action number	Effort		
					Phase 1	Phase 2	Phase 3
1 & 5	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. 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.	Produce Police Service IS/ICT plan as part of the programme portfolio plan/ Police National IS/ICT Plan as part of the enterprise portfolio.	ACPO/NPIA	30	✔	✔	
		Produce Police Service IS/ICT plan as part of the programme portfolio plan/ Police National IS/ICT Plan as part of the enterprise portfolio.	Forces	31	✔	✔	✔
		Produce Capability Plan as part of the overall police strategic plan/ Police National IS/ICT Plan as part of the enterprise portfolio.	NPIA/Central Customer	32	✔	✔	
5		Appoint a national level Programme Assurance function/ The Programme assurance structure to support all national programmes.	ACPO/NPIA	33	✔	✔	
		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.	Programme Assurance	34	✔	✔	
		Appoint an overarching TA role for national programmes/ ISS4PS coordination and coherency framework produced.	PITO/NPIA	35	✔	✔	

F.7 Integration

Policy	Principle	Action/ Deliverable	Action On	Action number	Effort Phase 1	Effort Phase 2	Effort Phase 3
8 & 12	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.	Develop and maintain conformance requirements for products and developments/ ISS4PS conformance criteria.	PITO/NPIA and Technical Authority	36	✔	✔	
5 & 6	The Police Service will take ownership of all key points in the life cycle.	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.	PITO/NPIA	37	✔	✔	
6 & 14	The Police Service will act corporately in its dealings with suppliers in order to achieve value for money and drive industry into providing ISS4PS conformant and compliant products.	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.	Home Office/ NPIA	38	✔	✔	✔
12	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 (GDS). Forces and national service providers should plan for a migration so that their systems become increasingly conformant to the ISS4PS.	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.	PITO/NPIA and Force	39	✔	✔	✔

F.8 National Planning for Convergence

Policy	Principle	Action/ Deliverable	Action On	Action number	Effort		
					Phase 1	Phase 2	Phase 3
5 & 11	Migration progresses in a coordinated, controlled and non-disruptive manner and documented in national and local level migration plans that are continuously monitored and maintained.	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 Global Data Store seeded with data from the national applications.	PITO/NPIA	40		✔	✔
		Develop and implement a migration plan for national services/A National Migration Plan that clearly identifies a practical roadmap to convergence at a national level supported by a Global Data Store seeded with data from the national applications.	PITO/NPIA	41	✔	✔	✔
		Coordinate national and local migration plans with regular reviews of progress and comparison with national and local priorities/A National Migration Plan that clearly identifies a practical roadmap to convergence at a national level supported by a Global Data Store seeded with data from the national applications.	PITO/NPIA	42	✔	✔	✔

F.9 Service Management

Policy	Principle	Action/ Deliverable	Action On	Action number	Effort		
					Phase 1	Phase 2	Phase 3
14	The Police Service will develop a consistent and holistic implementation of the ITIL framework.	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.	PITO/NPIA	43	✔	✔	✔
		Agree and procure common tools for implementing ITIL/ The Police Service will develop, implement and migrate to a consistent and holistic implementation of the ITIL framework.	PITO/NPIA	44	✔	✔	
		Migrate Forces and Central services in concert to the agreed standard processes and tools/ The Police Service will develop, implement and migrate to a consistent and holistic implementation of the ITIL framework.	PITO/NPIA	45		✔	✔
14	In order for the whole service management function to remain cohesive, it 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.	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.	PITO/NPIA	46		✔	✔
11 & 14	The Police Service will coordinate a migration to ITIL ensuring a consolidated approach is adopted.	Appoint a central coordination authority/ A central service management coordination authority.	PITO/NPIA	47	✔	✔	

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