



<b>Freedom of Information Act Publication Scheme</b>	
<b>Protective Marking</b>	NOT PROTECTIVELY MARKED
<b>Publication Scheme Y/N</b>	Y
<b>Title</b>	Information Management Strategy 2006 – 2011 Analysis and Supporting Material
<b>Version</b>	C
<b>Summary</b>	This paper supports the MPS Information Management Strategy, one of the supporting strategies for the MPS Information Strategy.
<b>Branch / OCU</b>	Dol2-2
<b>Date created</b>	8 April 2006
<b>Review date</b>	8 April 2010



## INFORMATION MANAGEMENT STEERING GROUP

# Information Management Strategy 2006 - 2011

## Analysis and Supporting Material

### Summary:

**This paper supports the MPS Information Management Strategy, one of the supporting strategies for the MPS Information Strategy.**

**Submitted for:** Approval

### Use of Content

The contents, concepts and models in this document must be acknowledged if used in other contexts.

Contact the author if clarification is needed.

<b>1. Introduction</b>	<b>5</b>
1.1 Scope and Purpose	5
1.2 Method	5
1.3 Information Strategy Family	5
1.3.1 Information Systems Strategy	5
1.3.2 Technology Strategy	5
<b>2. Management Summary</b>	<b>6</b>
2.1 Information is the Lifeblood of Policing	6
2.2 IM Vision: Information Management – from Control to Exploitation	7
2.3 Goals	8
2.3.1 Controlling Information to Meet Business Needs	8
2.3.2 Exploiting Information for Business Outcomes	9
2.3.3 Improving Data Quality	10
2.4 Vision – “One Whole View” – Standardised, Simplified, Corporate Information	11
2.4.1 Our policy must balance security of operations and rights and freedoms	11
2.4.2 Joining up policy to control information	12
2.4.4 Information Principles – describing where we want to be	14
2.5 What we are going to do	16
2.5.1 Marketing the MPS Information Management vision	16
2.5.2 Consolidating and developing new corporate capabilities supporting that vision	16
2.5.3 Business change to deliver the strategy goals	16
2.6 Terminology - Data, Information, Knowledge and Wisdom; Intelligence	17
<b>3. Where we are</b>	<b>18</b>
3.1 PESTLE Analysis	18
3.2 Political	18
3.2.1 National Policing Plan	18
3.2.2 Association of Chief Police Officers (ACPO)	18
3.2.3 National Police Improvement Agency (NPIA)	18
3.2.4 Closing the Gap	19
3.2.5 Modernising Government	19
3.2.6 Citizen Focus	19
3.2.7 London Public Authorities, Strategies and Executive Bodies	19
3.2.8 “Policing London” MPS Corporate Strategy 2006-2009 and the Met Modernisation Programme	20
3.3 Economic	20
3.3.1 MPS Organisational Context	20
3.3.2 ACPO / ACPOS Community Security Policy	21
3.3.3 Gershon and the Efficiency Agenda; MPS Service Review	22
3.3.4 Risk Management; Statement on Internal Control, Corporate Governance Framework	22
3.3.5 Audits and Best Value Reviews	22
3.3.6 UK and International Standards	22
3.3.7 Growth	23
3.4 Social	23
3.4.1 Safer Neighbourhoods, Step Change and MPS Demographics	23
3.4.2 Together	23
3.5 Technical	23
3.5.1 Transformational Government	23
3.5.2 ACPO Information Management Strategy	24
3.5.3 Information Systems Strategy for the Police Service (ISS4PS)	24
3.5.4 Home Office Police Science and Technology Strategy (HOPSATS)	24

3.5.5 Strategies for Metadata and Related Taxonomies (SMART) .....	25
3.6 Legal .....	25
3.6.1 Data Protection Act 1998 .....	25
3.6.2 Freedom of Information Act 2000 .....	25
3.6.3 Public Records Acts 1957 – 1959 .....	26
3.6.4 Crime and Disorder Act 1998.....	26
3.6.5 Regulation of Investigatory Powers Act 2000 / Human Rights Act 1998.....	26
3.6.6 Every Child Matters and the Children Act 2004 .....	26
3.6.7 Bichard Code of Practice (CoP) on the Management of Police Information and associated guidance (MoPI) .....	27
3.7 Environmental .....	27
3.7.1 MPS Environmental Strategy .....	27
3.7.2 MPS Estates Strategy.....	27
3.8 SWOT Analysis .....	27
3.9 Strengths .....	28
3.9.1 Sound technology base .....	28
3.9.2 Strong Partnership base .....	28
3.9.3 Importance of Information as an organisational asset .....	28
3.9.4 Organisational direction – MPS .....	28
3.9.5 Consolidated MPS IM Capability .....	28
3.9.6 Information Authority .....	29
3.9.7 IM Professional Specialism.....	29
3.9.8 Local Information Managers .....	29
3.10 Weaknesses .....	30
3.10.1 A sea of islands .....	30
3.10.2 Point solutions .....	30
3.10.3 Information re-capture.....	30
3.10.4 Inconsistency in information sharing.....	30
3.10.5 Disconnect to the paper legacy.....	31
3.10.6 Poor Data Quality.....	31
3.10.7 Culture of the broken loop.....	32
3.10.8 Governance in Information.....	32
3.10.9 Need for rationalisation of MPS “mapping” capabilities.....	33
3.11 Opportunities .....	33
3.11.1 Corporate Data Warehouse .....	33
3.11.2 Bichard Code of Practice on the Management of Police Information .....	33
3.11.3 National and International Standards.....	33
3.11.4 London Connects and the London Knowledge Network .....	34
3.11.5 Mapping Services Agreement.....	34
3.12 Threats .....	34
3.12.1 Benefits are real but diffuse .....	34
3.12.2 The Long Haul vs. Quick Wins.....	34
3.12.3 Ownership, Leadership and Airtime .....	34
3.13 Analysis of Where we Are .....	35
3.13.1 Legal obligations, operational risk and reputational risk accrue to poor information management .....	35
3.13.2 Information is a critical business asset and must be managed .....	35
3.13.3 Exploitation of information is key to effective policing .....	35
3.13.4 Effective controls enable exploitation.....	35
3.13.5 Information Sharing is now key to exploitation.....	36
3.13.6 Effective controls are key to information sharing .....	36
3.13.7 Common standards are key to information sharing.....	36

3.13.8 Business partners are combining into communities of interest and enabling those communities through standards .....	36
3.13.9 Not all of our partners respect the same standards .....	37
3.13.10 Good data quality is a major key control .....	37
3.13.11 Controls need to be applied to information regardless of format.....	37
3.13.12 Exploitation needs to be achieved regardless of format.....	38
3.13.13 Digitisation is a key enabler to control and exploitation.....	38
3.13.14 Standards and processes are key enablers for digitisation.....	38
3.13.15 Categorisation is a key enabler for control and exploitation of unstructured information .....	39
3.13.16 The paper legacy is significant and must be addressed .....	39
3.13.17 Re-use of information promotes efficiency and data quality.....	39
3.13.18 Operational staff are not experts in information management .....	40
3.13.19 Architecture is a key enabler for control and exploitation.....	40
<b>4. Where we need to be – Key Messages.....</b>	<b>41</b>
4.1 IM Vision: Information Management – from Control to Exploitation.....	41
4.2 Controlling Information to Meet Business Needs.....	42
4.3 Exploiting Information for Business Outcomes .....	43
4.4 Improving Data Quality .....	44
4.5 One Whole View – Standardising and Simplifying Information.....	45
4.5.1 Our policy must balance security of operations and rights and freedoms ...	45
4.6 IM Vision – Information Principles, Organisational Qualities, Behaviours .....	48
4.6.1 Information Principles .....	48
4.6.2 Organisational Qualities.....	50
4.6.3 Personal Behaviours.....	52
<b>5. How we get there – Enabling Information Quality.....</b>	<b>55</b>
5.1 IM Organisational Capabilities.....	55
5.1.1 IM Group.....	55
5.1.2 IM Professional Specialism.....	56
5.1.3 Information Managers.....	56
5.1.4 Information Authority and supporting Processes .....	56
5.1.5 Information Architecture.....	57
5.1.6 Master Reference Data.....	58
5.1.7 Information Policy Framework .....	59
5.1.8 Information Governance Framework.....	59
5.1.9 Data Modelling – Managed Information Team .....	59
5.1.10 Business Intelligence Capability .....	59
5.1.11 Information Assurance .....	60
5.1.12 Knowledge Management Capability.....	60
5.1.13 GIS Capability .....	60
5.1.14 Identity Management Capability.....	60
5.1.15 ACPO / ACPOS Community Security Policy Compliance.....	60
5.1.16 Information Sharing Capability .....	60
5.2 Business Change .....	60
5.2.1 Compliance with the Bichard Code on Management of Police Information..	60
5.2.2. Bichard IM Strategy and an Information Governance Framework .....	62
5.2.3 MPS Records Management Improvement, the move to Electronic Content Management and an Electronic Primary Record .....	62
5.2.4 Better Administration of the Paper Legacy.....	63
5.2.5 Data Quality Improvement Programme.....	63
5.2.6 ACPO / ACPOS CSP Compliance – Change Activities .....	64
<b>6. Glossary.....</b>	<b>65</b>

# 1. Introduction

## 1.1 Scope and Purpose

This is an MPS strategy which deals with management of *information* as an *essential business asset*. It provides the basis for business cases supporting investment for necessary IM business capabilities and business change; and informs other strategies dealing with the provisioning of business solutions and technology. This strategy updates the MPS Information Management Strategy 2005.

## 1.2 Method

The Information Management Strategy:-

- Analyses the current business context and proposes **goals\***;
- Describes a **vision** for an improved business environment;
- Describes the high level **enablers** necessary to achieve change.

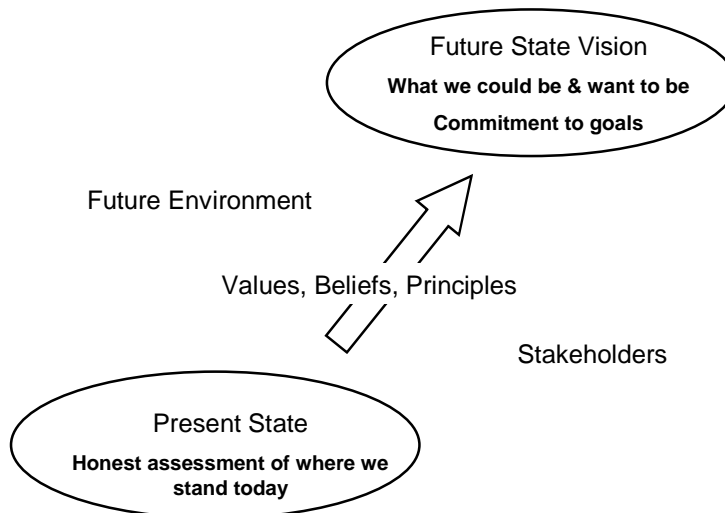


Figure 1 – Strategy Journey

## 1.3 Information Strategy Family

This strategy is one of three strategies which underpin the MPS Information Strategy. The Information Strategy provides a high level bridge between the MPS Corporate Strategy and the strategic business issues relating to information. Supporting this strategy are two other strategies which deal with how we organise information in systems and how technical standards can make its delivery efficient and effective. See the other strategies in this “family” for:-

### 1.3.1 Information Systems Strategy

Enabling the information requirements of MPS strategic priorities, outcomes and Met Modernisation Programme (MMP) critical components; requirements and benefits identification supporting information capture, analysis and enquiry; portfolio, programme and project management; process management.

### 1.3.2 Technology Strategy

A framework for smooth and transparent implementation of new and enhanced technology; technology strategies, architectures and standards.

## 2. Management Summary

### 2.1 Information is the Lifeblood of Policing

Use of information is vital to almost every activity in delivering a policing service to the capital. Along with our people, information is our most critical resource. Efficiency improvements in handling information can yield huge benefits. Conversely, under-performance severely impacts effectiveness. Information and how we use it is first and foremost a *business issue* rather than one of technology, but sound and innovative use of technology to get the right information to the right people at the right time, place and cost is critical to the effective use of information.

Strategy and policy on information management issues is set in the MPS by the Directorate of Information (DoI).

This strategy holds that the current MPS approach to information management is not sustainable.

Our information is a sea of islands, which is not capable of being controlled or exploited corporately and lack of confidence in its quality is a critical impediment.

This exposes us to risks such as:-

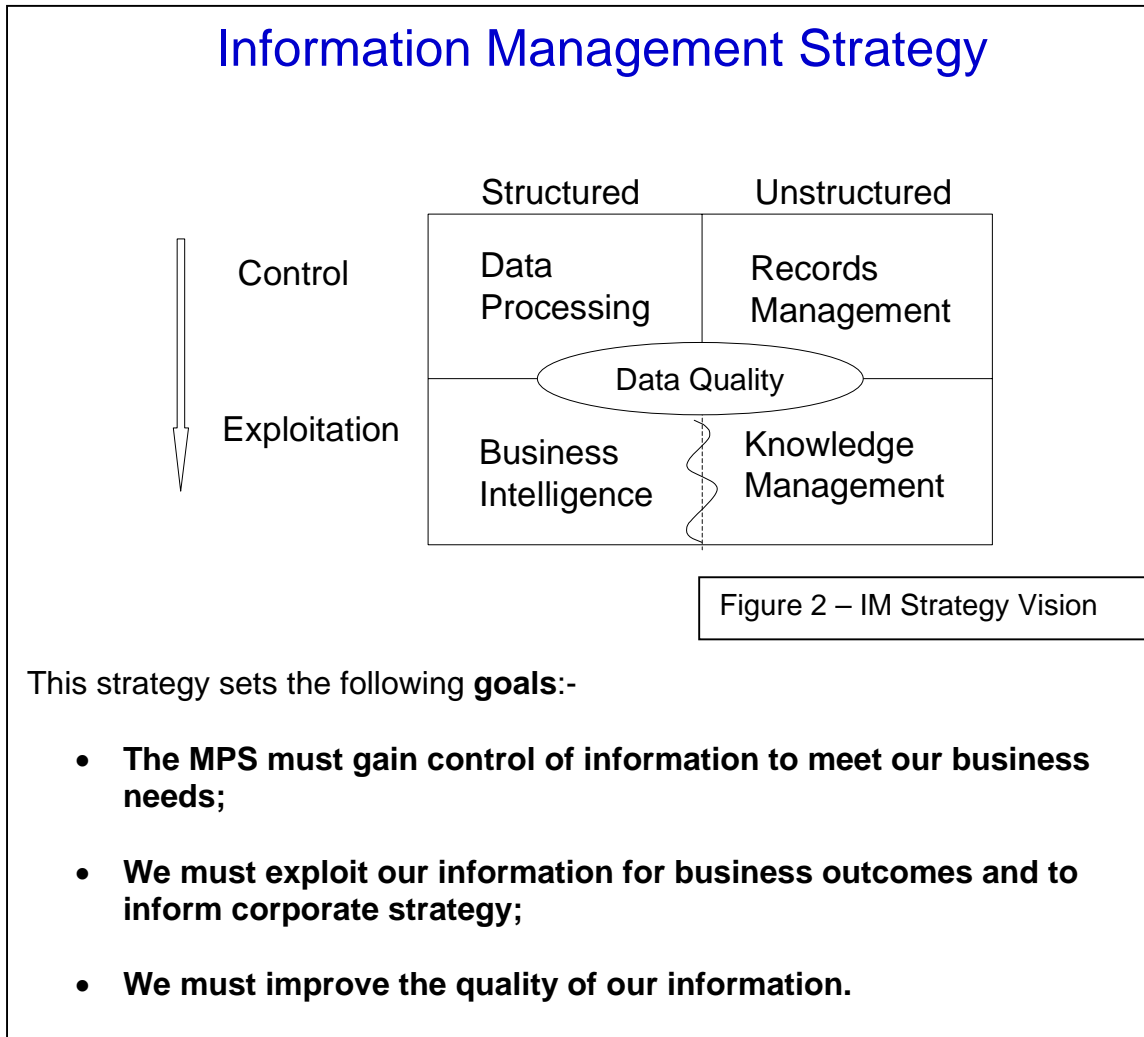
- Failure to exploit information to effect necessary policing outcomes;
- Failure to share information to the same ends;
- Compromise to police operations through poor quality or poor control;
- Litigation.

Increasingly, these issues are the subject of inspection and statutory control.

Acts and policies have been introduced as enablers and together with our partners we are expected to take up these enablers and to use them to deliver effective and efficient joint working. To do this we need a level of business sophistication, investment and culture which is not present in the MPS today. As we have introduced business infrastructures to manage finances and people better, so we now need the necessary business infrastructure to manage *information* adequately. This is not the same as managing *information technology*. We are currently *technology rich* and yet we are *information poor*.

We need a vision of an MPS better able to meet these challenges; and to build new capabilities and to change our organisation to reflect that vision.

## 2.2 IM Vision: Information Management – from Control to Exploitation



A **vision** must be adopted to achieve these goals. These involves:-

- Obtaining “one whole view” of information through:-
  - Joining up our policies to reflect real-world issues;
  - Joining up formats and sources of information.
- Using principles to describe how our information, organisation and behaviours need to change and which give us a vision of the goals.

The **enablers** for the strategy are:-

- Marketing the MPS Information Management vision, internally and externally;
- Consolidating and developing new corporate capabilities supporting that vision;
- Business change to deliver the strategy goals.

## 2.3 Goals

### 2.3.1 Controlling Information to Meet Business Needs

Statutory, strategic, and policy drivers along with productivity issues demand that we exploit *new markets* for our information from which substantial benefits may be derived. The key enabler for these new markets is the effective *sharing* of our information assets.

But unless we apply appropriate **controls** to achieve confidence in sharing, involving effective *security* and *quality* improvements we will expose ourselves to unacceptable *cost* and *risk*.

*Information and organisation growth exacerbate quality issues and introduce liabilities.*

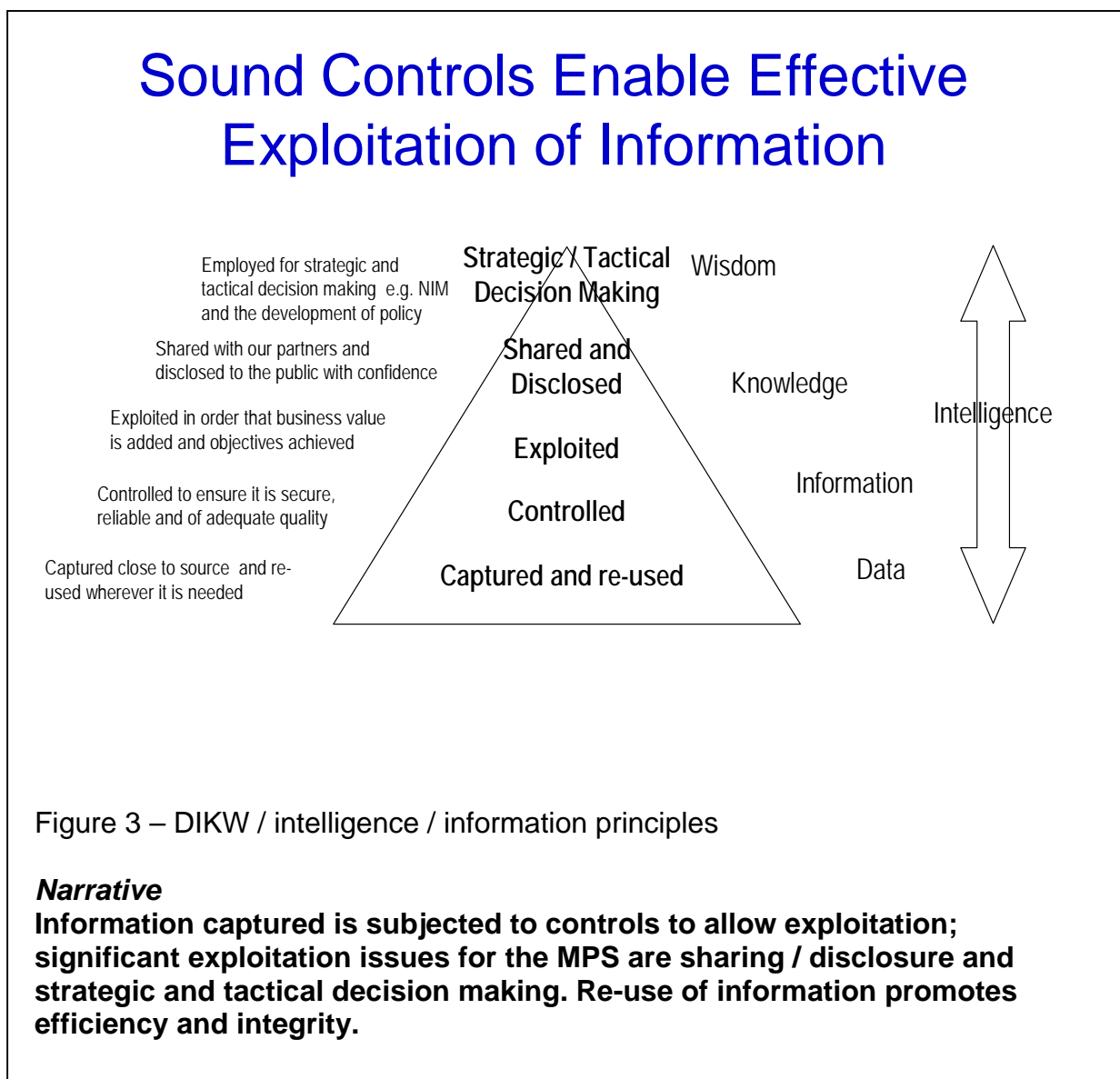


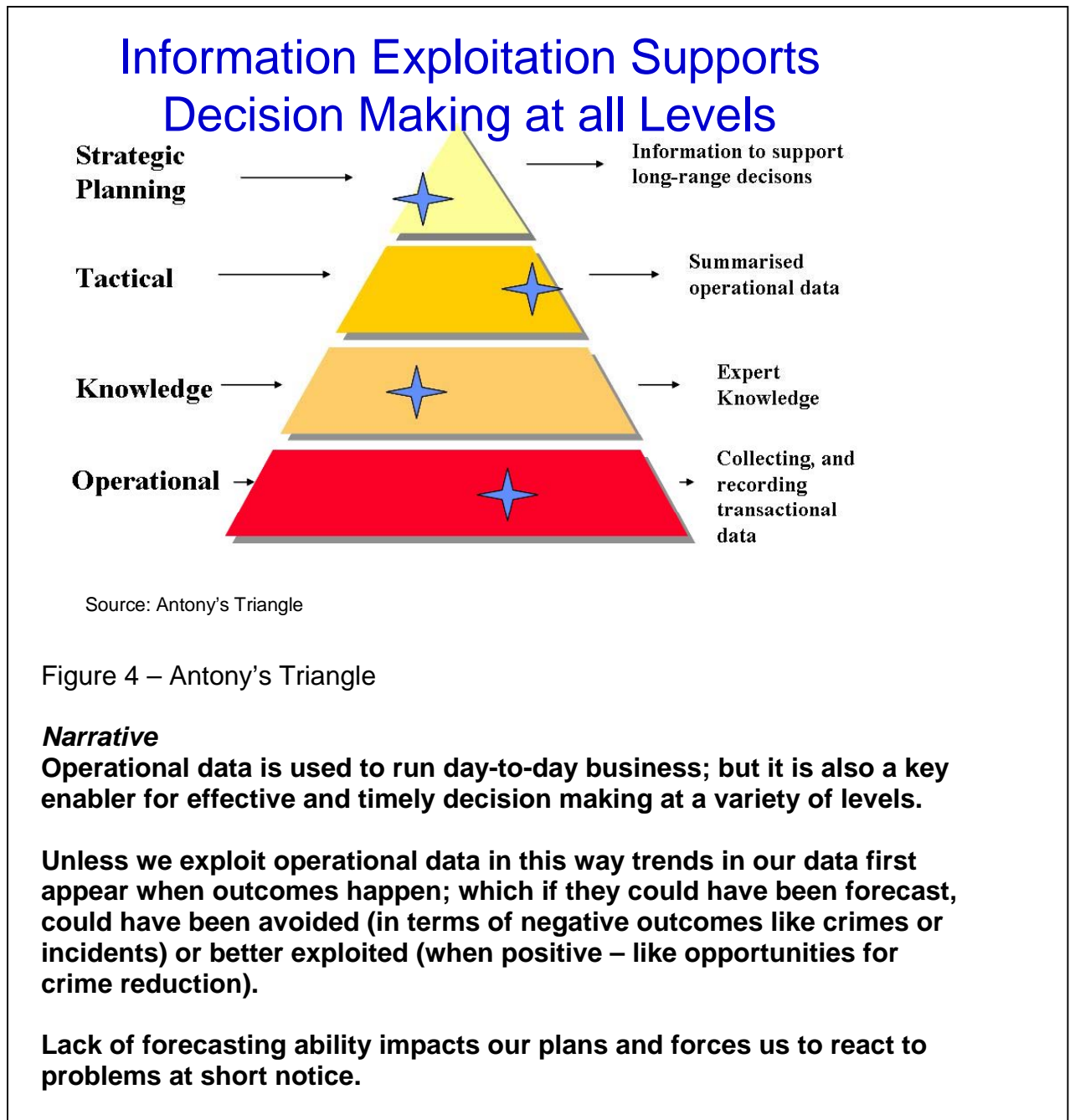
Figure 3 – DIKW / intelligence / information principles

#### **Narrative**

**Information captured is subjected to controls to allow exploitation; significant exploitation issues for the MPS are sharing / disclosure and strategic and tactical decision making. Re-use of information promotes efficiency and integrity.**

### 2.3.2 Exploiting Information for Business Outcomes

We must build *new capabilities* to **exploit** the information resources we already have through the re-use of *experience* and better *analysis* of recorded information.



### 2.3.3 Improving Data Quality

## Data Quality is a Necessary Enabler for Effective Exploitation of Information

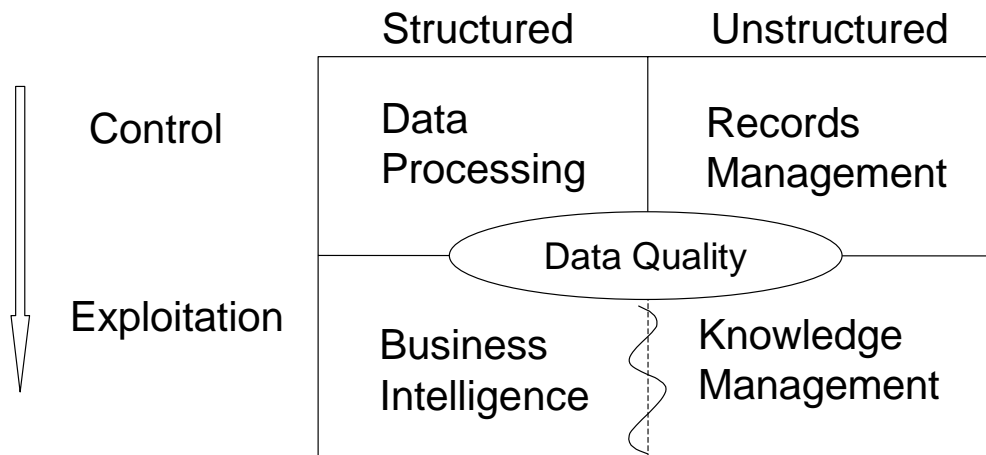


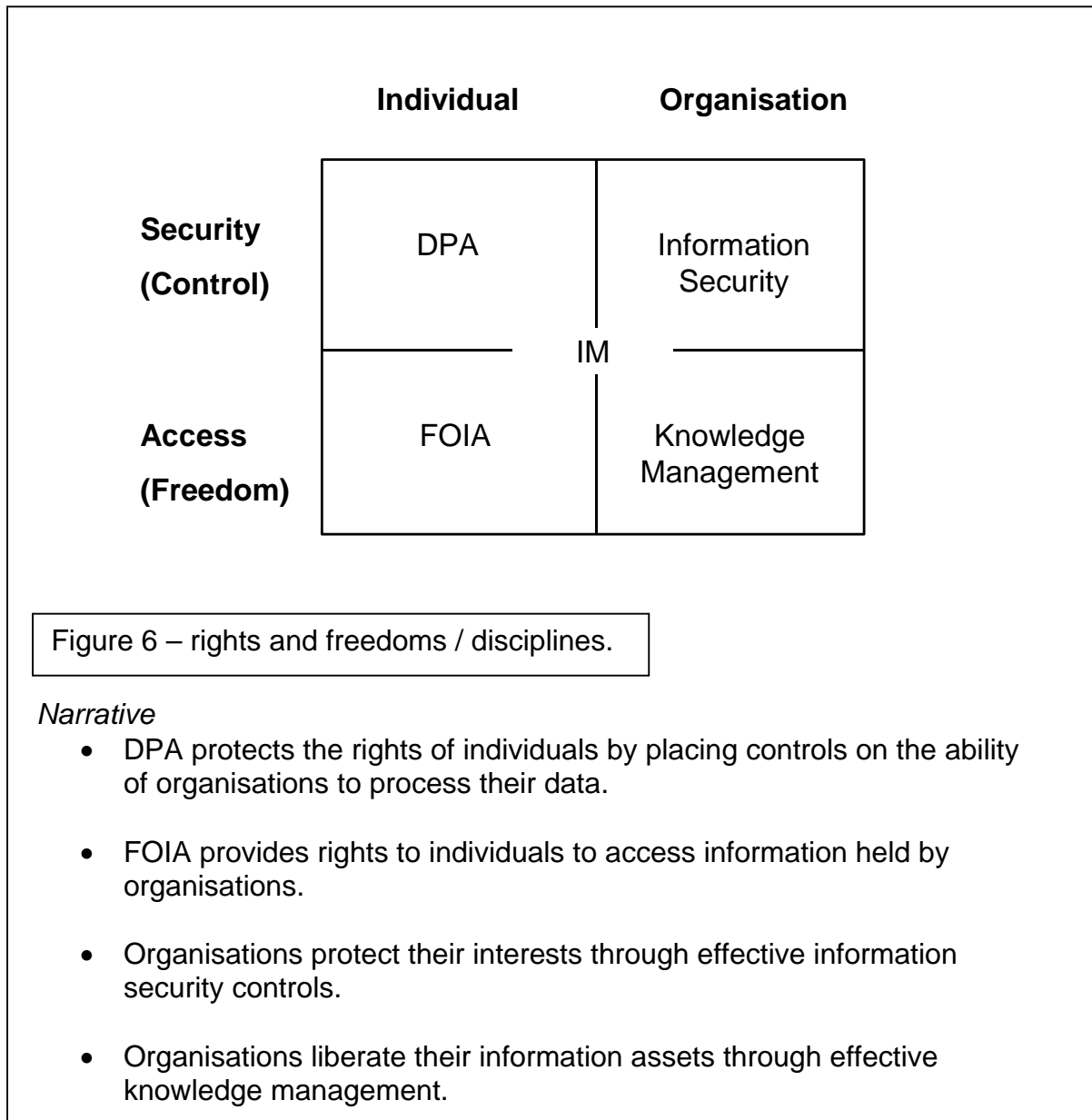
Figure 5 – Data Quality supports control to exploitation

***Narrative:***

**In order to exploit information effectively it is critical that the issue of data quality is addressed. Seeking improved exploitation without addressing data quality is likely to result in poorly informed decision making. Data quality is therefore a key enabler to allow effective exploitation of information.**

## 2.4 Vision – “One Whole View” – Standardised, Simplified, Corporate Information

2.4.1 Our policy must balance security of operations and rights and freedoms  
 Information must be **trusted, accessible** and **usable (see vision)**. *Whose interests are protected, who may be granted access, and how information may be used* are issues which provide UK public sector organisations with some challenges.



**There is a balance to be struck between the rights and freedoms of individuals and the effectiveness of organisations in delivering effective IM. IM organisations in the UK public sector need to reconcile these interests. The relationships between the issues / disciplines shown need to be understood. Only by bringing our policy development and supporting disciplines together can we achieve joined up thinking – a “whole view”.**

### 2.4.2 Joining up policy to control information

When applying controls, the real world is not conveniently divided into separate problems of data protection, information security, freedom of information or records management.

These issues are generally interlinked in any real situation. So must be our thinking.

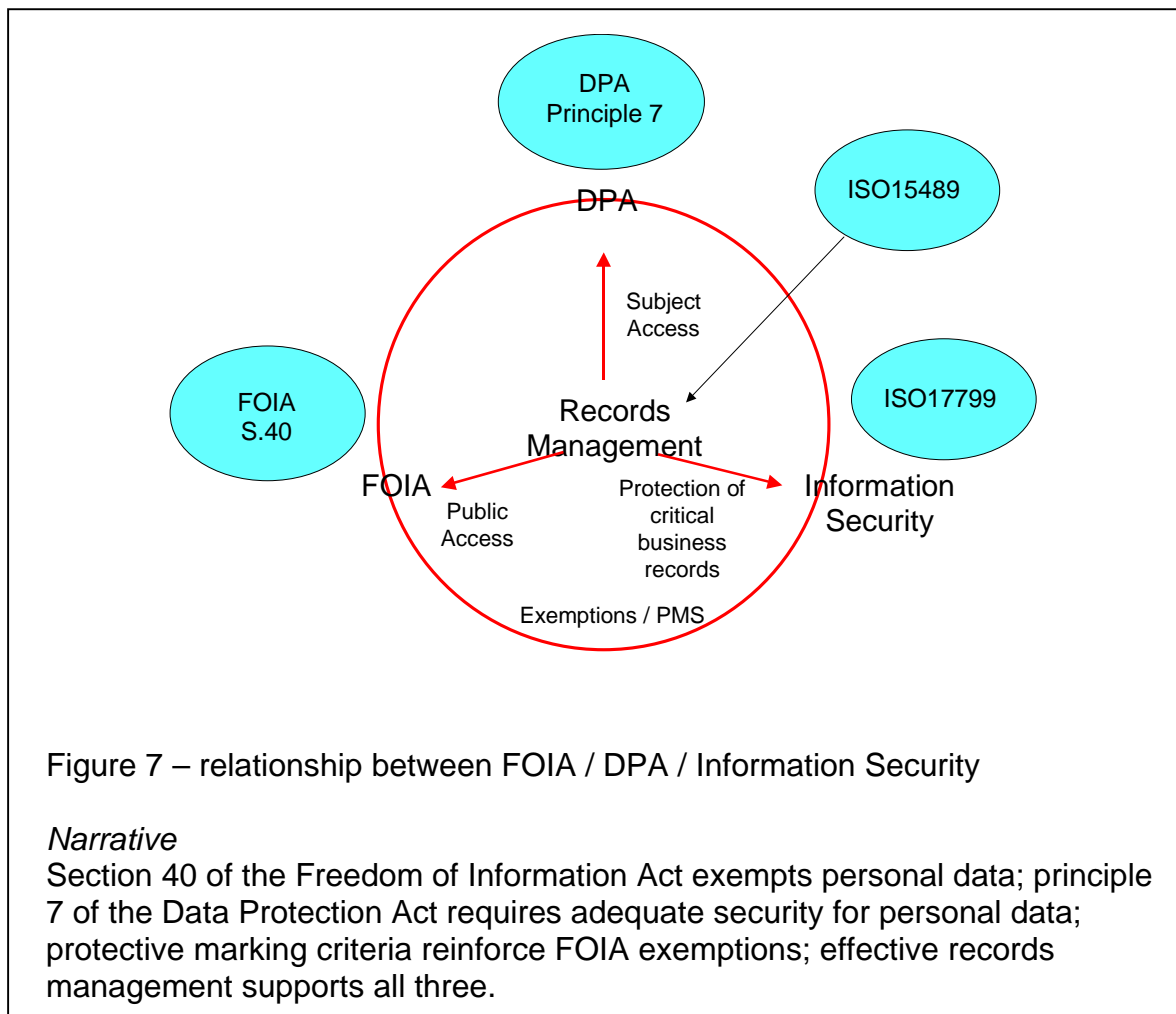


Figure 7 – relationship between FOIA / DPA / Information Security

#### *Narrative*

Section 40 of the Freedom of Information Act exempts personal data; principle 7 of the Data Protection Act requires adequate security for personal data; protective marking criteria reinforce FOIA exemptions; effective records management supports all three.

**All of these issues are interdependent and will need to be brought to bear on real world issues together. We must obtain a “whole view” - understand these relationships and find whole answers to real world problems.**

The relationship between these Acts and standards can be complicated. We need to introduce tools and processes which make them easier to apply, and to manage circumstances where their demands conflict.

#### Notes –

DPA = Data Protection Act 1998

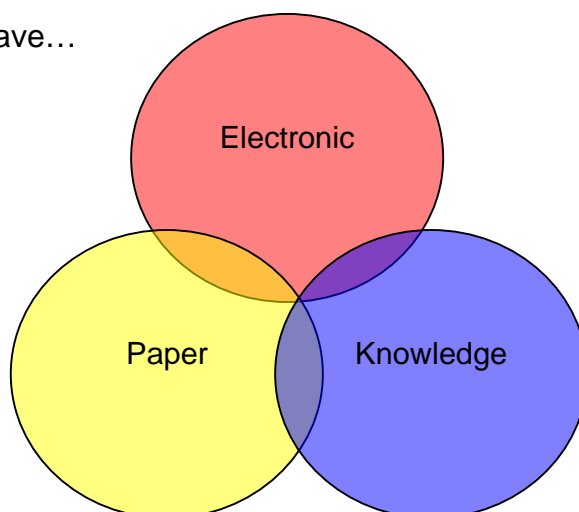
FOIA = Freedom of Information Act 2000

ISO 15489 = International Standard for Records Management

ISO 17799 = Code of Practice for Information Security Management

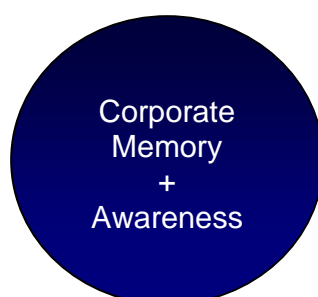
### 2.4.3. Joining up formats and sources of information

At present we have...



...three separate views of information depending on format. In control terms we also need to apply policies consistently across these formats.

**We need to overlay these views as far as possible, achieving one view...**



We need clear “whole view” policies to apply to this “one view” environment; the ability to apply those policies consistently; and to be able to access the information we need regardless of format.

*Narrative*

**To build “one whole view” we must introduce a new *architecture* for MPS information, supporting the corporate memory and awareness; we need the organisational *capability* to build it; and will need to exercise *authority* to maintain it.**

Figure 8 – Converging Formats

#### 2.4.4 Information Principles – describing where we want to be

We can use principles to describe how our information, organisation and behaviours need to change and which give us a vision of the goal. We must be able to see:-

*MPS **information** as trusted, accessible and usable via a set of information principles;*

##### *Trusted*

- One version, captured once and re-used;
- Appropriate quality information for action;
- Compliant with policy and the law;
- Protected from loss or misuse.

##### *Accessible*

- Managed according to its cost and its worth;
- Captured close to source, available when and where it is needed;
- Shared with our partners and disclosed to the public with confidence, in an open and accountable manner.

##### *Usable*

- Easy to find and deploy with agility;
- Presented in context, in the best way possible;
- Used and understood by a skilled workforce.

*An MPS **organisation** which:-*

- knows what it knows and how to find it;
- promotes openness and accountability;
- protects information proportionately, according to its worth;
- exploits information effectively and efficiently;
- manages information in accordance with business need, policy and the law;
- shares information with others.

*The **behaviours** which we need our staff to adopt:-*

- S**ecure and protect valuable information;
- O**ne version of the truth;
- R**evue information over time;
- T**hink of finding when storing;
- E**xpect to share information;
- D**ispose of redundant information.

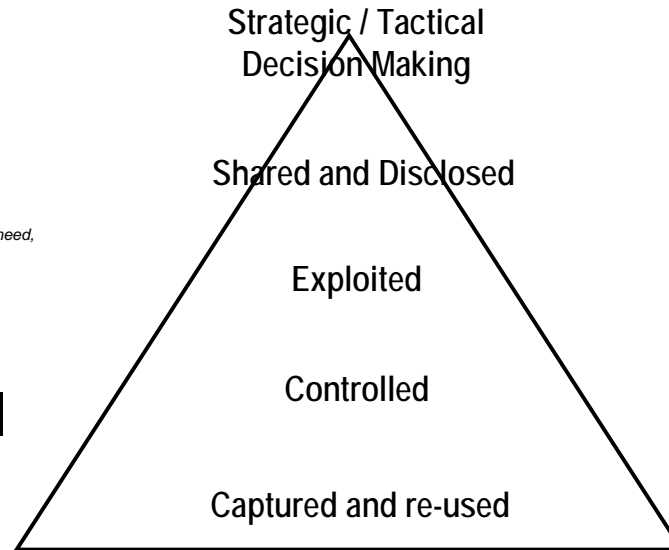
Together, our principles describe the information, organisation and behaviours we need for a better MPS

# IM Vision - Principles

## Organisational Vision

- Know what we know and how to find it;
- Promote openness and accountability;
- Protect our information proportionately, according to its worth;
- Exploit our information effectively and efficiently;
- Manage the information we need in accordance with business need, policy and the law;
- Share our information with others.

## Organisational Qualities



## Information Strategy Principles

### Trusted

- One version, captured once and re-used
- Appropriate quality information for action
- Compliant with policy and the law
- Protected from loss or misuse

### Accessible

- Managed according to its cost and its worth
- Captured close to source, available when and where it is needed
- Shared with our partners and disclosed to the public with confidence, in an open and accountable manner

### Usable

- Easy to find and deploy
- Presented in context, in the best way possible
- Used and understood by a skilled workforce

## Design Principles

**SORTED**

- **S**ecure and protect valuable information
- **O**ne version of the truth
- **R**eview information over time
- **T**hink of finding when storing
- **E**xpect to share information
- **D**ispose of redundant information

## Behaviours

## **2.5 Enablers - What we are going to do**

Information Management Group (part of the Directorate of Information) will drive delivery of this strategy.

### 2.5.1 Marketing the MPS Information Management vision

We will set out the vision for MPS IM and communicate it to our staff and partners. We will use it to define our end-game and to inform our progress toward our goals. Specifically we will use:-

- Information principles to design our business solutions;
- Organisation principles to organise and champion business change
- Behaviours to modify culture and inform policy and processes.

### 2.5.2 Evolving new corporate capabilities supporting that vision

We will:-

1. Develop an IM professional specialism with industry leaders and seek to provide thought leadership on IM issues;
2. Consolidate the MPS Information Authority, champion good IM practice including reduced re-keying, data quality improvement and records management improvement, extending over time to all MPS information;
3. Review the role of MPS local Information Managers to ensure the capability meets MPS business needs and good practice;
4. Build an MPS information architecture to enable effective use of MPS information and the application of policy;
5. Define / refine a model of legal and policy issues which apply to MPS information;
6. Introduce a governance framework for information;
7. Build a capability to model MPS information, enabling reduced re-keying and sharing;
8. Develop MPS business intelligence capabilities;
9. Build on the establishment of the new information sharing capability, market it to the MPS and ensure that it is sustainable;
10. Build on the DoI Knowledge Management strategy and introduce an MPS-wide KM capability;
11. Introduce capabilities for management of master reference data including identity and spatially referenced data;
12. Introduce measures to ensure compliance with the full breadth of MPS information policy issues;
13. Comply with the ACPO / ACPOS Community Security Policy.

### 2.5.3 Business change to deliver the strategy goals

We will

1. Deliver a major business change programme to introduce the Bichard Management of Police Information (MoPI);
2. Move MPS records management from current reliance on paper records to electronic content management, preserving integrity of processes and maintaining necessary evidential weight;
3. Introduce improvements to manage the legacy of paper records;
4. Deliver a programme of targeted data quality improvements;
5. Introduce IM awareness and infrastructure improvements.

## 2.6 Terminology - Data, Information, Knowledge and Wisdom; Intelligence

The word “information” is used throughout this strategy to mean a range of ideas summarised in the table below. Without realising it, we translate the “material” we use between **data**, **information**, **knowledge** and **wisdom**.

Typically we move a commodity called **data** in vast quantities around our organisation; it is presented in context to our workforce as **information**; they apply their experience and know-how to deploy **knowledge** in the service of policing outcomes; and from time to time we aggregate this together to derive principles, policies, strategic and tactical decisions as **wisdom**. As a police service we also trade in **intelligence**. While there is no nationally agreed definition of the term, we tacitly agree that intelligence is “information fit for action”. A more detailed description is given in the table below. At different times intelligence may meet any of the criteria for **data**, **information**, **knowledge** or **wisdom**.

In order that material can be moved around	Description	Concept	Intelligence – information processed for analysis which has a predictive value and may be of evidential worth.  All information can become intelligence when it is developed as part of an evaluation process to inform tactical and strategic decision making	Policing example	In order that material can be exploited
	Raw material; symbols, numbers, letters – without context or specific meaning	<b>Data</b>		10 Acacia Avenue	
	Data with context; potential material for action	<b>Information</b>		10 Acacia Avenue, address of John Smith, informant	
	Information with added experiential references	<b>Knowledge</b>		John Smith bears a grudge against David Jones from previous circumstances and will make false allegations against him	
Underlying truth on which tactical or strategic decisions may be made	<b>Wisdom</b>	Use of informants must be made in the context of their likely motivation to supply information to Police			

Figure 10 – DIKW and Intelligence

### Information Management

*“The associated people, policies, processes, structures and tools necessary to meet the information needs of the organisation”*

- Policies – rules for managing information;
- Structures – a hierarchy of concepts which allow information to be stored, retrieved and policy to be applied;
- Processes – activities which apply the rules to the structures;
- Tools – aids to enforce policies, structures and processes.

### Knowledge Management

We define Information Management as dealing with explicit information and Knowledge Management as covering tacit information.

Knowledge Management is *“The re-use of experience for the benefit of the organisation”*

## **3. Where we are**

### **3.1 PESTLE Analysis**

This section provides an appraisal of the position of the MPS in the context of major business drivers relating to information at the time of writing. The PESTLE (political, economic, social, technological, legal and environmental) method has been employed.

### **3.2 Political**

#### 3.2.1 National Policing Plan

The National Policing Plan (NPP) is a three-year rolling strategy document designed to provide a single point of definition for the Government's priorities for the Police service, performance indicators by which that service is assessed and new developments planned to enable priorities to be met. The Government's 5 key priorities for the police service, identified in NPP (2005-2009), incorporated into the National Community Safety Plan, are to:

- Reduce overall crime by 15% by 2007-08 and more in high crime areas
- Bring more offences to justice within the Government's Public Service Agreement (PSA)
- Provide Every area in England and Wales with dedicated, visible, accessible and responsive neighbourhood policing teams; and reduce public perception of anti-social behaviour
- Tackle serious and organised crime, including through improved intelligence and information sharing between partners
- Protect the country from both terrorism and domestic extremism

A number of actions are set out within the NPP describing how these national priorities can be delivered at a local level.

The NPP is updated on a yearly basis.

#### 3.2.2 Association of Chief Police Officers (ACPO)

ACPO is a caucus of senior police management interests in England and Wales. Collectively ACPO provides a voice for the police service both to government / rest of the public sector and to the public. ACPO has been active in the information, IS and ICT contexts, commissioning the Valiant Programme and subsequent Information Systems Strategy for the Police Service (ISS4PS). ACPO maintains a forum dealing specifically with information management issues, the IM Business Area (IMBA). MPS Director Dol has recently become chair of this forum and as a result the MPS is well placed to exert influence nationally. Our strategic aim (see MPS Information Strategy) is to increase this influence.

#### 3.2.3 National Police Improvement Agency (NPIA)

The NPIA, a Home Office body, will be formed in 2006/07 by the integration of the Police IT Organisation (PITO) and the National Centre for Policing Excellence (NCPE). The resulting agency will be of great significance in information and IS terms as it will contain capabilities to develop Codes of

Practice affecting police information and *business processes* which can be mandated on Chief Officers with legislative effect; and the executive capability to enshrine these developments in IS / ICT.

#### 3.2.4 Closing the Gap

Her Majesty's Inspectorate of Constabulary (HMIC) released "*Closing the Gap*" in September 2005. This report proposes the rationalisation of Police Forces in England and Wales to a smaller number with minimum personnel levels of 4,000. Forces are in negotiation with the Home Office on mergers to this end. In information terms this suggests the opportunity to *standardise* in a variety of ways, including *business processes*. It also suggests the disparity in size between MPS and other UK forces may reduce. This disparity has in the past been responsible for "poor fit" between solutions designed and implemented in small Forces and MPS implementations.

#### 3.2.5 Modernising Government

*Partnership* has shaped policing since the 1990s. *Modernising Government* (Cabinet Office 1999) and subsequently the *e-Government / e-Policing* agendas set out the principles that public services should be shaped around citizens rather than the public sector; that *channels* of choice for the provision of services directly to citizens and between government agencies should be enabled through *electronic service delivery*. A number of standard frameworks have been developed, for example for authentication, security, interoperability (*e-GIF*) and metadata (*e-GMF / e-GMS*). These are significant enablers for the extension of information beyond the MPS organisational boundary.

#### 3.2.6 Citizen Focus

The themes in *Modernising Government* have been continued into the *Policing Performance Assessment Framework* (PPAF) – by which progress can be measured, and most recently into *Citizen Focused Policing*. All of these drivers suggest *new markets* for police information – blurring boundaries between organisations to share information across the public sector and beyond to the *citizen*; and *new channels* – both electronic and in more traditional forms.

*Building Communities, Beating Crime* takes up these themes and suggests new and greater engagement with the public to provide more responsiveness and accountability. Provision of information on performance (e.g. National Crime Recording Standard (NCRS) and National Incident Recording Standard (NIRS)) and additional communication channels are implicit in this.

#### 3.2.7 London Public Authorities, Strategies and Executive Bodies

Since 2000, the Metropolitan Police Service has been one of the functional bodies of the Greater London Authority (GLA), and reports status and progress to the Metropolitan Police Authority, (MPA). The Mayor has set out ambitions for London in "the London Plan" and various related strategies on subjects such as digital inclusion and broadband access. An executive body providing support for technology-enabled partnership working has been created by GLA and the Association of London Government (ALG) with input from the London Branch of the Society of IT Managers (SocITM), called

London Connects. MPS is a signatory to the London Connects concordat since 2001 and is an active participant in that organisation; Director DoI is a member of London Connects Board. London Connects has promoted co-ordination of issues such as pan-London information sharing, Freedom of Information Act (FOIA) compliance and a London Public Services Network.

### 3.2.8 “Policing London” MPS Corporate Strategy 2006-2009 and the Met Modernisation Programme

The MPS Corporate Strategy 2006-2009 seeks to make London the safest major city in the world. This is described by four outcomes:-

- Communities are engaged with, confident in and satisfied with our police service
- Security is improved and the public feel reassured
- Crime, disorder, vulnerability and harm are prevented and reduced
- More offenders are brought to justice

Seven strategic priorities are intended to deliver these outcomes, titled:-

- Safer Neighbourhoods;
- Counter Terrorism, Protection and Security;
- Criminal Networks;
- Capital City Policing;
- Information Quality;
- Citizen Focus;
- Together.

These are supported by corporate values and enablers titled:-

- A modern and diverse workforce;
- Enabled staff;
- Better use of resources;
- Cohesive partnership working;
- Clear communication.

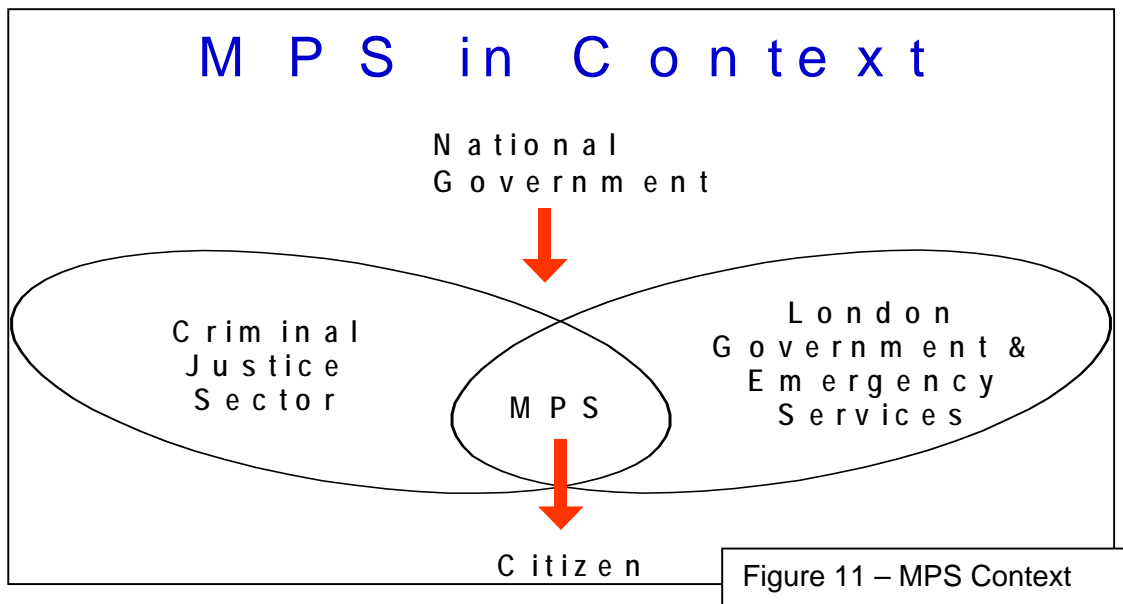
Delivery of the corporate strategy will be co-ordinated by the Met Modernisation Programme. Measurement of achievement will be via public service agreements and the PPAF.

## **3.3 Economic**

### 3.3.1 MPS Organisational Context

The MPS is on the cusp between the Criminal Justice Sector and the various agencies representing London Government and the delivery of public services in the capital. This bi-directional focus affects MPS information in three ways:-

- The need to respect *strategy* and *policy* set in both these communities;
- The need to align *processes* at the interfaces;
- The need to *share* information with partners in both of these markets.



The MPS is a *large and diverse* organisation. It is the single biggest employer in London and virtually all its employees are engaged in gathering, controlling or exploiting information. Our size means that the sources and destinations of information are often widely separated. There may be no contact between the officer who enters a CRIS (Crime Report Information System) record and the analyst who uses it to produce crime statistics for hot spot mapping. The inertia common to most large organisations makes change slow and difficult and magnifies its cost. In common with other organisations the business is split along functional lines. This has contributed to the fragmentation of our information and impacts on the effectiveness of our business processes.

The MPS is an *emergency service*. Our information is relied upon for serious outcomes and must be accessible to our people. It needs to be acquired and deployed quickly and securely, possibly in locations that are difficult to reach. It also requires us to interact with the public in a variety of ways.

The MPS is a *public service* operating in both the Criminal Justice and the Local Government sectors. This means maintaining high standards of information security; dealing with tensions that arise from the need to share information into environments that do not meet our security standards; and at the same time meeting the standards of openness and integrity which are rightly expected of us by the public. Statutory and policy drivers are high in focus and political and social changes provide drivers, often at short notice. In common with other public bodies we are constrained by our budgets and resources are finite.

### 3.3.2 ACPO / ACPOS Community Security Policy

The *ACPO / ACPOS Community Security Policy (CSP)* sets out standards for business and technical assurance of Police information. It provides a “level playing field” where signatories align their investment in information assurance based on an assessment of risk. Practical benefits include access to shared services such as Police National Computer (PNC) and the Criminal Justice Extranet (CJX).

### 3.3.3 Gershon and the Efficiency Agenda; MPS Service Review

The review by Sir Peter Gershon: *Releasing Resources for the Front Line; Independent Review of Public Sector Efficiency*, in July 2004 set the ambition to achieve £20Bn savings in public sector spending by 2007/08 to allow these savings to be redirected to “front line” services. Police feature twice in this issue, both as subjects of scrutiny and redirection in resource management and as potential beneficiaries of savings from elsewhere in the public sector. This theme was echoed within the MPS by the Service Review in 2005. The Gershon report also, significantly, supported investment in the *Causeway* project relating to shared information and processes in criminal justice organisations (CJOs) reporting to the Northern Ireland Office (NIO) as a cross-cutting enabler.

### 3.3.4 Risk Management; Statement on Internal Control, Corporate Governance Framework

MPS introduced a formal risk management and governance structure following the review by Willis in 2001. Of the table of major corporate risks MPS Corporate Risk No 7 is “*Inadequate management of MPS information (including information security)*”. More recently these themes have been carried forward into other corporate controls such as the Statement on Internal Control (SIC), signed annually by the Commissioner and the Chair of the Metropolitan Police Authority (MPA) and the MPS Corporate Governance Framework.

### 3.3.5 Audits and Best Value Reviews

- The *Records Management Best Value Review (RMBVR)* identifies shortcomings in the relationship between our *corporate memory* and our *policies* and investment choices, proposing policy and business change to address this.
- The *Demand Management Best Value Review* and *Demand Resolution Strategy* seek *new channels* for MPS information in order to realise business efficiencies.
- *On the Record* highlights shortcomings in the quality of critical police information sources.

### 3.3.6 UK and International Standards

Certain UK and international standards are becoming key to the management of information;

- *BIP0008 - Code of Practice for Legal Admissibility of Electronic Records* defines the considerations necessary to assure the integrity of processes involving electronic records (as opposed to paper records) through maintenance of *evidential weight*.
- *ISO15489 International Standard for Records Management* defines the organisational measures necessary for effective management of essential corporate records.

- *ISO17799 Code of Practice for Information Security Management* defines the means for systematic assurance of information assets.

### 3.3.7 Growth

Like most modern organisations the MPS is experiencing exponential *information growth*, driven simultaneously by a move towards electronic information and access to massive external information sources. Information superfluous to business need is increasingly becoming a *liability*. Not only are there new statutory (FOIA) and policy (Bichard) obligations to ensure it is managed, but redundant information increasingly obscures the presence of useful data.

## **3.4 Social**

### 3.4.1 Safer Neighbourhoods, Step Change and MPS Demographics

The MPS is already on average one of the youngest and most inexperienced police services in the UK. *Organisational growth* (Step Change) – the increase in police numbers from 30,000 officers to 35,000 and overall numbers to reach 52,000 – will accelerate this trend.

Safer Neighbourhoods (and *Safety in Neighbourhoods*) will extend MPS information resources to new and challenging environments and will prompt sharing of information resources still wider.

### 3.4.2 Together

The Together initiative seeks to champion the efforts of MPS personnel as a collective through an appropriate and consistent values and behaviours, supporting the Commissioner's mission of working *together* for a safer London. Information aspects of this issue are

- Information *sharing* –internally, with business partners and *disclosure* to the public
- Effective *collaboration*
- Effective *communication*

## **3.5 Technical**

### 3.5.1 Transformational Government

Transformational Government (Cabinet Office, November 2005) sets a strategic vision for government enabled by technology where:-

- IT is designed around the citizen or business (echoing Modernising Government and Citizen Focus);
- Government rationalises and shares services (echoing Gershon and the efficiency agenda) using *standardised, simplified* information and infrastructure;
- Capabilities are broadened and deepened in respect of professionalism in planning, delivery, management, skills and governance of IT enabled change.

### 3.5.2 ACPO Information Management Strategy

The *ACPO IM Strategy (Exploiting Information for an Enhanced Police Service, 1999)* defines the ambition of the Police Service nationally to see Police information as a *shared* national resource. It proposes a shift from management of information in functional silos to a “whole” view of information as a business resource and that this will enable benefits in relation to efficiency, effectiveness and public confidence, and would address challenges such as:-

- Improving quality and performance;
- Delivery in a broader public safety context;
- Improving front line policing;
- Meeting the needs of the public; and
- Enhancing co-operation with other criminal justice agencies.

### 3.5.3 Information Systems Strategy for the Police Service (ISS4PS)

The *ACPO Information Systems Strategy for the Police Service (ISS4PS)*, based on previous work called *Programme Valiant*, seeks to deliver the ambitions of the ACPO IM Strategy through the development of congruous business and technical capabilities in the UK Police Service.

*Valiant* foresaw the need to develop specific capabilities “in-Force” supporting information and knowledge management (in contrast to technology capabilities) in recognition of a capability shortfall in this area.

Of specific significance to this strategy are the Enterprise Architecture Framework for the Police Service (EAF4PS) and Corporate Data Model (CorDM). These are enablers for interworking with the police service nationally.

### 3.5.4 Home Office Police Science and Technology Strategy (HOPSATS)

One means of delivering the priorities outlined in the NPP is through the effective use of ICT. HOPSATS is a five-year strategy (currently 2004-2009) aimed at providing a framework to guide the planning and delivery of valuable science and technology services to frontline policing. PITO, along with the Forensic Science Service (FSS), the Police Scientific Development Branch (PSDB), and the ICT divisions within the nation’s individual Police Forces are expected to use the HOPSATS as a guide for their deployment and development plans for 2003/04 and beyond.

The purpose of the HOPSATS is defined as:

*‘to ensure the Police Service is equipped to exploit the opportunities in science and technology to deliver effective policing as part of a modern and respected criminal justice system.’*

In order to achieve this purpose, the HOPSATS aims to:

- Establish priorities for current and future science and technology applications and research

- Co-ordinate the development and implementation of technology between users and suppliers to ensure a coherent and effective process
- Implement processes for future scanning to ensure that the Police Service can exploit new technology at the earliest opportunity and is prepared for new technology based threats.

### 3.5.5 Strategies for Metadata and Related Taxonomies (SMART)

Strategies for Metadata and Related Taxonomies (SMART) is a PITO initiative which has developed a range of products for the consistent treatment of unstructured and semi-structured information (information which does not carry its own definition of context e.g. emails, documents). These include a UK corporate police file plan, metadata standard, and a thesaurus of policing terms. FOIA has provided the initial driver for Force adoption of this content but the Bichard Manual of Police Information (MoPI) provides another significant business driver going forward; requiring the effective application of policy to information in both structured and unstructured contexts.

## **3.6 Legal**

### 3.6.1 Data Protection Act 1998

The Data Protection Act (DPA) governs the processing of information on living individuals in the UK. Since 1<sup>st</sup> January 2005 this includes unindexed, unstructured paper collections; this is of significance for the estimated 36 linear Km of MPS paper legacy.

Legal gateways are necessary to enable sharing of information within the remit of the DPA. Some of the most significant gateways are found in the Acts which follow in this section.

The principles enshrine in law the requirements of good information lifecycle management. Principle 7 of the Data Protection Act has the effect of making “appropriate” security measures a legal requirement.

Section 55 creates an offence when personal data is knowingly misused.

### 3.6.2 Freedom of Information Act 2000

The Freedom of Information Act (FOIA) provides legal powers for citizens to request information held by public authorities, who must honour this obligation unless an exemption can be quoted. Even in these circumstances a challenge can be mounted to release information if the public interest is held to outweigh the exemption. The Act also requires public authorities to pro-actively publish information likely to be of interest to the public.

Section 40 of the FOIA refers requests for information requested by the data subject to be addressed by the DPA.

Sections 45 and 46 enable Codes of Practice which require the necessary business infrastructure to be put in place to meet the needs of the public authorities’ obligations to the citizen and to manage corporate records adequately to that end.

Section 77 creates a criminal offence of deleting information which may have been of relevance to a received request.

### 3.6.3 Public Records Acts 1957 – 1959

The PRA set out the requirements for maintenance of essential business records in Government. The MPS has not been subject to the PRA for new records since the formation of the GLA in July 2000 but has obligations to meet the requirements of the Act for legacy records and has made a policy decision to apply these standards to new records as good practice.

### 3.6.4 Crime and Disorder Act 1998

Section 115 creates the legal gateway for the sharing of personal information between certain partner agencies including police for the reduction or prevention of crime and disorder.

### 3.6.5 Regulation of Investigatory Powers Act 2000 / Human Rights Act 1998

Acts control the relationship between law enforcement agencies and the public and between employers and their employees in respect of the interception of communications.

Regulation of Investigatory Powers Act 2000 (RIPA) is most commonly applied in the police domain to the former relationship and the Human Rights Act 1998 (HRA) to the latter.

Chief among the HRA articles of relevance to information issues is article eight, which grants individuals the *“right to respect for private and family life, home and correspondence...”*. Article eight is a qualified right but interference with it by public authorities must be *“in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”*.

RIPA constraints are to some degree mitigated by the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000* which authorises interceptions for most necessary business purposes.

In both domains clarity of communication of policy and subsequent adherence to that policy are key enablers.

### 3.6.6 Every Child Matters and the Children Act 2004

The Children Act 2004 places a responsibility on all partner agencies to ensure that every child and young person is able to succeed in life by achieving five key outcomes; an implication is the introduction of the national Information Sharing (IS) Index that will record details of all children under the age of 19. This will in conjunction with improved guidance on information sharing increase the requirements to share information between the partner agencies including the police. The sensitivity of some of the material being shared will also push into high focus the tensions between enabling the

provision of care to vulnerable individuals and the duty of care to protect their information.

### 3.6.7 Bichard Code of Practice (CoP) on the Management of Police Information and associated guidance (MoPI)

The Bichard CoP and MoPI arise from recommendations 8 – 11 of the Bichard Inquiry Report (June 2004) into the systematic failures of police information management leading to the murders in Soham in 2003. Both are mandated on Chief Officers under s39 / s39a Police Act 1996 and s2 Police Reform Act 2002. The CoP and MoPI complement a major national ICT-enabled business change activity called IMPACT which will enable the sharing of intelligence between police agencies in England and Wales.

A national infrastructure to support implementation is being assembled by the National Centre for Policing Excellence (NCPE), shortly to be subsumed into the National Police Improvement Agency (NPIA). Implementation will occur in phases, over time. An implementation methodology based on that used to introduce the National Intelligence Model (NIM) is being developed in parallel.

The MoPI proposes a model for the governance of police information assets and specific processes for assessment / retention / disposal of information based on risk and business need. A model for the sharing of information is also proposed.

MoPI will have the general effect of standardising / aligning strategy, policy and processes for information management in England and Wales.

## **3.7 Environmental**

### 3.7.1 MPS Environmental Strategy

The MPS Environmental Strategy promotes reduction in consumption of / impact to natural resources in MPS business practice. Issues for information implicit in the strategy include the reduction in generation of paper output and consumption of electricity by technology enablers.

### 3.7.2 MPS Estates Strategy

The MPS Estates Strategy proposes a more flexible approach to the provisioning of accommodation to meet MPS business needs. Implications for information are

- Introduction of greater variety in the domains containing MPS information assets, including new / greater threats to confidentiality;
- Requirement for more cost-efficient management of paper material.

## **3.8 SWOT Analysis**

This section provides an appraisal of the strengths, weaknesses, opportunities and threats obtaining to MPS information at the time of writing.

## **3.9 Strengths**

### 3.9.1 Sound technology base

MPS has a sound if heterogeneous technology infrastructure which is reliable, maintainable and cost efficient. This infrastructure is based on de facto industry standards. Mechanisms exist to ensure a good fit between business need and provisioning and the identification and realisation of benefits.

### 3.9.2 Strong Partnership base

MPS has engaged in partnership working since the early 1990s and has incorporated this mode of working into everyday business practice, with some notable successes. For example,

- Crime Reduction Units
- Youth Offending Teams
- Community Safety Units

have all been implemented successfully, and Safer Neighbourhoods / Safety In Neighbourhoods is extending this integration.

Some initiatives have incorporated specific information enablers, some novel in nature – for example:-

- Karrot smart card / reward card model (Southwark – winner of Invest to Save award 2003);
- North London Strategic Alliance initiatives involving abandoned vehicles, environmental crime, local intelligence, public reassurance;
- CASWeb community advice online.

### 3.9.3 Importance of Information as an organisational asset

The importance of information to the business of policing is widely recognised by MPS management, and several high profile initiatives have sought to address information shortfalls (e.g. Operation Asgard, Operation Baseline Success). There is however a disconnect between this acceptance and the prevailing MPS culture (see culture of the broken loop).

### 3.9.4 Organisational direction – MPS

MPS has in recent times started to reposition itself toward a more centralised organisational structure. In information terms this will assist in the promotion of values such as corporacy and help to enable the view of information as a corporate rather than a local asset. A greater emphasis on alignment of local priorities toward corporate goals and investment controls to that end will also assist.

### 3.9.5 Consolidated MPS IM Capability

A central IM function has been built from MPS business functions representing:-

- Records Management;
- Library Services;
- Information and Knowledge Management;
- e-Government / e-Policing;

- Data Protection;
- Freedom of Information;
- Information Security;
- Data Quality;
- Data Modelling;
- Intranet management.

This represents practical recognition of the business value of information by combining the disciplines involved in its management, to give a coherent “joined-up” service to the organisation as a whole.

### 3.9.6 Information Authority

An “Information Authority” has been established to question the development of both point solutions and re-capture situations. Supporting processes have been defined and implemented to inform the decisions of the Information Authority and all DoI solutions in development have been inspected for compliance with MPS principles for information design (see Information Principles).

### 3.9.7 IM Professional Specialism

A professional specialism of “Information Management” has been constructed involving the disciplines of records management, information security and legal governance of information (e.g. DPA, FOIA etc).

The Police Service employs a competency framework to define job roles (the National Integrated Competency Framework or NICF):- an activity of “Managing Information” has been introduced by the MPS IM Group with the following parameters:-

Summary: *Manage information in accordance with information legislation, policy and business requirements*

Effective Performance will include the following:

1. Ensuring information is managed in accordance with Force policy, operating procedures and the information life-cycle – creation to disposal;
2. Ensuring compliance with relevant information legislation;
3. Ensuring information security policies and operating procedures are applied to achieve confidentiality, integrity and availability.

This activity is of relevance not only to those whose “professional home” is information management, but can be applied to a range of roles with information management aspects, making this intervention powerful.

### 3.9.8 Local Information Managers

Information Managers have been recruited into positions distributed throughout MPS business functions to improve MPS information

management; the driver at the time being the Freedom of Information Act, the next being the Bichard CoP / MoPI. A professional development programme for this cadre has been constituted in conjunction with a private sector IM consultancy.

### **3.10 Weaknesses**

#### **3.10.1 A sea of islands**

Five years ago the MPS corporate network, OTIS, was many local networks, joined together; this was hard to maintain, inconsistent, costly and inefficient. In AWARE MPS technology has been re-organised so that it is corporate, consistently built and optimal. However our information is still a sea of islands, of variable quality. We have 50,000 inboxes and home directories; and about 130 corporate and local applications. This is not sustainable. We need to extend the reform of our technology into how our information is organised. We need the same trust and accessibility in our information, and to use it in ways which help us, together, make London safer.

#### **3.10.2 Point solutions**

MPS has a tendency to seek specific solutions to problems rather than to seek general enablers and to apply them to a variety of circumstances. It has, for example, not one enterprise resource management tool, but two; and six document management systems. None of these interoperate well.

#### **3.10.3 Information re-capture**

Another organisational tendency is to construct answers to information problems which involve the capture of information where this information is already held elsewhere in the service. This results in:-

- Inefficiency (multiple keying);
- Integrity and data quality problems (through multiple copies of the same data).

This can be because the solutions are MPS implementations of national products; but often is the result of the need for “quick answers” to urgent problems.

#### **3.10.4 Inconsistency in information sharing**

Whilst MPS has embraced partnership working and has done much to augment its processes and change culture to accommodate its needs, this has happened on a devolved basis and as a result the arrangements for sharing information are not consistent between different parts of the MPS. Many examples of good practice exist but these standards are not reflected in all parts of the organisation.

There is also still uncertainty amongst practitioners over the rules for sharing information and the scope for discretion in sharing as a process. Standards and terminology which allow risk issues to be communicated internally and to business partners (such as the Protective Marking System and handling code 4) are not yet consistently understood or embedded in MPS culture.

This inconsistency and uncertainty may manifest itself as risks for the MPS, either through information not being shared which needs to be for operational outcomes, or information being shared inappropriately causing impacts on operations or the subjects of the data themselves.

Much has been done in this area but there is still much to do. A joint initiative between the Directorate of Information and Territorial Policing (TP) has introduced a rational, standardised corporate model for the development of information sharing agreements (ISAs) and training undertaken. A business function has been set up to support this process (the Information Sharing Support Unit) and this approach has been marketed successfully to NCPE as a model for Bichard MoPI; but marketing of this process, function and capability needs to be pursued further with the MPS and it needs to be made sustainable.

### 3.10.5 Disconnect to the paper legacy

The MPS has been estimated to hold approximately 36 linear Km of paper. Of this the Records Management Branch (RMB) administers a central registry system for paper files, including the management of a central record archive containing 17 linear Km of paper records.

There are approximately 750,000 registered files held either at Hendon repository or by TNT under contract.

The paper records in these repositories should represent a core resource, containing the “gold standard” of information – papers containing accountable decisions, information of sufficient quality and authenticity to be presented as evidence in a court of law - essential business records.

The MPS has however become disconnected from this “corporate memory” and essential business decisions / material involving substantial corporate risk / cost are now routinely recorded in no consistent manner – most frequently as email content. Where local paper records are kept these are also of variable quality and in questionable conditions.

Work in 2004 / 05 has sought to address both the alignment of the categories for recording in the corporate memory and to champion the submission of this material to RMB from across the MPS. There is however much still to do in respect of both activities and of moving the MPS to a position where critical business records can be kept electronically under adequate control. It is apparent that our corporate memory is substantially a centralised manual process based on paper, in an organisation which is widely distributed, and technology enabled.

### 3.10.6 Poor Data Quality

Information is essential to the business goals of the MPS. If that information is poor quality the MPS will fail to identify wrongdoers, connect them to their actions or locate them.

- Policing actions are taken on the basis of false information, wasting time and undermining the reputation of the MPS.

- People are arrested on the basis of false information and the MPS is frequently sued for it.
- Priority offenders are not identified because their names and details are not recorded accurately and a full picture of their activities cannot be obtained.
- Prosecutions fail because the facts cannot be presented in a complete and convincing fashion.

### 3.10.7 Culture of the broken loop

As suggested in the PESTLE analysis:-

*“The MPS is a large and diverse organisation. It is the single biggest employer in London and virtually all its employees are engaged in gathering, controlling or exploiting information. Our size means that the sources and destinations of information are often widely separated. There may be no contact between the officer who enters a CRIS record and the analyst who uses it to produce crime statistics for hot spot mapping...”*

At a working level information is often not valued and this is reinforced by a service that refers to recording of information supporting the reporting of crimes and arrests as “bureaucracy”. There is a disconnect between the act of recording information and its subsequent re-use for important outcomes. This is the loop which is “broken”, and poor data quality leading to risk and cost is the result.

### 3.10.8 Governance in Information

The Commissioner of the Metropolitan Police is the owner of all MPS information. As such he is vicariously liable for shortcomings arising from this information and how it is used; most obviously in relation to the provisions of the Data Protection and Freedom of Information Acts.

Clearly the Commissioner cannot by himself discharge his obligations in this respect; he expects his staff to exercise delegated authority on his behalf.

It is at this point that the current arrangements cease to provide adequate corporate governance. Whilst there is a general understanding that certain collections of information are notionally owned by certain parts of the MPS business – usually represented by the names of IT applications (CRIS) or business themes (crime), there is currently no unequivocal source which describes “who” is responsible for managing “what” MPS information. Whilst ownership of some information is clearly known (albeit not formalised in most cases), some information may be claimed by more than one source; other information may be disowned by a range of potential business interests. There is also a lack of clarity around what these responsibilities mean in practice. What is needed is a governance framework for MPS information; to allow corporate policy to be applied to specific collections of information.

### 3.10.9 Need for rationalisation of MPS “mapping” capabilities

Whilst progress has been made in developing corporate tools for capturing information about location and licenses for spatially referenced data obtained (see “Mapping Services Agreement” (Opportunities)), MPS business functions and solutions which apply spatially referenced data to maps are disconnected from these strategic developments and need to be rationalised. At present they may deliver out of date data, are hard to maintain and are not cost-effective.

## **3.11 Opportunities**

### 3.11.1 Corporate Data Warehouse

MPS is progressing the implementation of a data warehouse; this will provide a capability to join MPS datasets and produce marts for a variety of purposes including intelligence, performance management / management information and strategic and tactical decision making. This will highlight, however, situations where poor data quality is an impediment. It will also highlight the dependency on clarity around governance of information assets.

### 3.11.2 Bichard Code of Practice on the Management of Police Information

Bichard CoP and MoPI provides a statutory driver complementing DPA, FOIA and the Secretary of State’s / Lord Chancellors’ Codes for sound management of information. The Commissioner is required to “have regard to” Codes of Practice made under the Police Act 1996.

The MoPI will drive the introduction of a range of business controls promoting:-

- Clear governance controls for MPS information;
- Processes for the management of collections of information pertaining to high risk offenders or potential offenders;
- Technology investment to enable the above;
- Training and awareness on information issues;
- A compliance regime.

The MoPI will drive the construction of an MPS Bichard “Information Management Strategy” which specifically addresses these requirements. That document should not be confused with this strategy which oversees the whole information environment which applies to the MPS. MoPI will provide a strong business driver to introduce the measures proposed in the analysis / vision sections of this strategy.

### 3.11.3 National and International Standards

A range of standards now exist which are essential enablers for working in partnership with other organisations and for forming / assuring internal developments.

- BIP0008 - Code of Practice for Legal Admissibility of Electronic Records;
- BIP0025 (DIRKS – Developing and Implementing Record Keeping Systems)
- ISO15489 International Standard for Records Management;

- ISO17799 Code of Practice for Information Security Management;
- e-GIF, e-GMS;
- CorDM
- TNA 2002

#### 3.11.4 London Connects and the London Knowledge Network

MPS has engaged with agencies promoting information and knowledge issues in London and is an active partner in both. Opportunities include the development of business and technical infrastructures for information sharing, multi-agency channels for electronic service delivery and exchange of knowledge management best practice.

#### 3.11.5 Mapping Services Agreement

The MPS has engaged with 558 local, police, fire and allied authorities to pool their purchasing power for the supply of digital map, address and height data. Data supplied under the Mapping Services Agreement (MSA), whilst widely distributed, is not yet fully exploited within the MPS. Location is a key element of MPS held information. The MPS will need to develop its capability to utilise spatial information to maximise its effectiveness across a wide spectrum of policing activities.

### **3.12 Threats**

#### 3.12.1 Benefits are real but diffuse

The threats, opportunities and issues described in this paper, whilst real, are in the main abstract; other demands have more obvious operational effects. Benefits, anticipated to be major from a corporate perspective, will be difficult to measure, as much other change will be underway in the same environment; and the benefits which accrue will tend to be corporate rather than local.

#### 3.12.2 The Long Haul vs. Quick Wins

Few of the outcomes proposed in this strategy provide benefits in the short term. Such benefits will however need to be sought in order to provide “pump priming” to enable long term gain. A robust benefits realisation plan will be necessary to support business cases for investment supporting improvements in the “How we Get There” section of this strategy.

#### 3.12.3 Ownership, Leadership and Airtime

This strategy involves, amongst other things, widespread cultural change.

Change is difficult; a great deal of change for other purposes is already going on. Airtime is limited, and contended for. MPS resources are finite. Best value and value for money must be achieved in what we do; evidence of this must be presented.

Ownership of this strategy at the highest level will be fundamental if its goals are to be achieved; and in order to effect the changes necessary this ownership and leadership must come from the top.

### **3.13 Analysis of Where we Are**

This section analyses the “Where we are” section of the strategy and proposes findings which can be concluded from it. This then becomes the basis for the vision explored in “Where we need to be”.

#### 3.13.1 Legal obligations, operational risk and reputational risk accrue to poor information management

The current MPS approach to information management is not sustainable. Our information resources are fragmented and are not capable of being controlled or exploited corporately and lack of confidence in their quality is a critical impediment.

This exposes us to risks such as

- Failure to exploit information to effect necessary policing outcomes;
- Failure to share information to the same ends;
- Compromise to police operations through poor quality or poor control;
- Litigation.

Increasingly, these issues are the subject of inspection and statutory control.

#### 3.13.2 Information is a critical business asset and must be managed

Acts and policies have been introduced as enablers and we are expected to take up these enablers and to use them to deliver effective and efficient joint working. To do this we need a level of business sophistication, investment and culture which is not present in the MPS today. As we have introduced business infrastructures to better manage finances and people, so we now need the necessary business infrastructure to manage *information* adequately. This is not the same as managing *information technology*. We are currently *technology rich* and yet we are *information poor*.

#### 3.13.3 Exploitation of information is key to effective policing

We are familiar with the need to serve the information needs of our major processes to arrive at essential policing outcomes – for example reporting and management of crime, responding to incidents, processing cases to court.

All these examples are reacting to demand. Few of our processes – intelligence and performance management excepted – make the journey to pro-activity through the exploitation of such information.

A focus on the exploitation of information to deploy resources, make tactical and strategic decisions, and to re-use experience is an essential enabler for effective policing. This focus will require new organisational *capabilities* - people, processes and tools.

#### 3.13.4 Effective controls enable exploitation

Effective controls – for example controls on retention against business need, timeliness, quality, and confidentiality - provide confidence in the information needed for exploitation. Without this confidence we are inhibited from taking

the steps necessary to exploit our information for the outcomes we are seeking.

#### 3.13.5 Information Sharing is now key to exploitation

Few successful outcomes are achieved nowadays in isolation from our partners in the London public sector and the criminal justice system. Achieving the outcomes we need by exploiting information with our partners whilst mitigating risks arising from sharing that information is therefore a key enabler.

#### 3.13.6 Effective controls are key to information sharing

Mitigating risks in the sharing of information relies on effective and demonstrable controls – if the controls are not demonstrable they are probably not effective.

The controls necessary to achieve effective sharing of information can be categorised as

- Legal governance – are we entitled to share information under the law?
- Information security – can we mitigate risks to confidentiality and ensure appropriate levels of integrity and availability?
- Data quality – will our information when shared lead to the right outcomes or does it represent a liability?

#### 3.13.7 Common standards are key to information sharing

Organisations typically make investments to mitigate corporate risk to their information. In addition to investments they may also accept curbs on business practices which otherwise would represent business efficiencies.

If these organisations transact business involving the sharing of information with partners who do not make equivalent investments / accept equivalent curbs they suffer two potential disbenefits:-

- The risks they sought to mitigate via the investments / curbs may be realised;
- The business case for the mitigations they put in place may be undermined.

It is unrealistic to expect all organisations to employ the same mitigations to information risk; their business context will make different demands, and from this lead to different choices on mitigation. However the adoption of consistent *standards* allows mitigations and therefore investments to be balanced.

Common data standards are also critical; in the MPS context the CorDM, EAF4PS and SMART are key and capabilities supporting them essential enablers. These enablers also support re-use of information and thus the efficiency agenda.

#### 3.13.8 Business partners are combining into communities of interest and enabling those communities through standards

MPS is a partner or potential partner in a variety of communities which are enabled by information; information which is enabled by technology; and the

design of both technology and information are shaped by standards.

Examples are:-

- The Police and criminal justice organisations clustering around the Criminal Justice Extranet (CJX) and enabling shared services such as PNC and IMPACT;
- The London Public Sector are moving toward a community around the London Public Services Network;
- Care organisations in London will need to combine information to support the needs of implementation of the Children Act 2004.

### 3.13.9 Not all of our partners respect the same standards

MPS does business daily with organisations such as the security services, local government and the voluntary sector. Meeting the policy needs for information in these various environments creates tensions. Not all these partners even employ the same terminology to allow effective dialogue to enable sharing. For example ISO17799 provides a framework for assurance of assets and is relatively ubiquitous in Government; but the protective marking system, which allows information to be valued, does not extend beyond central government and the criminal justice community.

The degree of policy integration between partner agencies needs to be driven by an assessment of our collective ambitions to do business. The greater this ambition, the greater the business case to align our policy controls and to see information as a commodity to be traded widely. If, on the other hand, our needs to do business are specific and defined, a model which “ring fences” our information and only allows it to be traded in controlled environments is appropriate.

These business cases must be explored with each of the partner communities to which we seek to belong. The business cases, informed by standards, will drive the design of our business and technical environments, and through this, our need for investment.

### 3.13.10 Good data quality is a major key control

Information needs to be of adequate quality for the business purposes to which it is to be put. Lack of confidence in the quality of data inhibits use.

### 3.13.11 Controls need to be applied to information regardless of format

Information is often defined by the enabling technology. For example, management of emails is generally approached as one type of problem, solved by technologies aligned to email as a medium. This approach does not allow information to be managed effectively according to business risk and cost.

## Policy Aligns to Business Need, not Enabling Technology



Figure 12 – Policy vs Technology

An additional level of sophistication needs to be achieved to reconcile these views. It must be possible to categorise information according to business context and to apply policy to the categories across a range of media.

### 3.13.12 Exploitation needs to be achieved regardless of format

As with control issues, it is frequently the case that exploitation needs will transgress boundaries of format. Information relevant to a business purpose will exist in a variety of formats and the need is to exploit without this constraint.

### 3.13.13 Digitisation is a key enabler to control and exploitation

Both the application of effective controls and the exploitation of information are better achieved in digital form than in other formats, such as paper. If the MPS information estate is to be standardised, simplified and made efficient, then a general “direction of travel” must be towards a digital environment. If the full range of benefits is to be achieved this must be the aim not only for copies but for original records.

### 3.13.14 Standards and processes are key enablers for digitisation

Digitisation does however require business and technical measures to *assure* the information and outcomes. Authentication and maintenance of adequate evidential weight are essential to making this transition. Key among these standards are:-

- BIP0008 - Code of Practice for Legal Admissibility of Electronic Records;
- BIP0025 (DIRKS Developing and Implementing Record Keeping Systems)
- ISO15489 International Standard for Records Management;
- ISO17799 International Standard for Information Security Management;
- e-GIF, e-GMS;
- CorDM
- TNA 2002

### 3.13.15 Categorisation is a key enabler for control and exploitation of unstructured information

Information can be divided into *structured* information and *unstructured* information. Structured information is information which gains additional meaning through its context – for example, a surname in a box on a form marked “Victim” has a different meaning to a surname in a field in a database marked “Employee”. Typically databases and forms contain this kind of information. Unstructured information does not benefit from its context in this way and has to carry this context within its content – for example, in emails and documents.

Unstructured information needs to be put into context if policy is to be applied to it and if it is to be exploited. This means it needs to be grouped into categories based on meaning; and this in turn means that unstructured information needs to be “tagged” so that it can be grouped. The “tags” are called *metadata* and the groups are called *taxonomies*. If a taxonomy is to be employed to apply policy to information (control it) as well as to group and retrieve it (exploit it), it is called a *file plan*.

These concepts need to be built into our unstructured collections of information if we are to manage them sensibly. Additionally, viewing our *structured* collections this way would allow us to have one view (in business terms) of all of our information assets. This would allow us to assign policy to information to meet business need as proposed above.

### 3.13.16 The paper legacy is significant and must be addressed

Moving our information from a centralised paper-based environment to one which increasingly is invested in electronic content does not automatically address the paper legacy. The *Best Value Review of Records Management* (2002) assessed the options available to MPS through comparison with a range of other organisations and proposed that a policy of scanning / processing of paper documents should only be applied to material frequently used. This suggests that a legacy of paper records will need to be maintained for some time.

The organisational structure, processes and culture necessary for maintenance of essential business records therefore needs to be maintained both to address the paper legacy and to transition the right qualities into the digital environment.

### 3.13.17 Re-use of information promotes efficiency and data quality

It is necessary in the real world to have more than one copy of information for purposes of resilience and optimisation. However there should be no more copies than necessary and certainly information should not be captured more than once without good reason. Multiple copies of information suggest issues of

- Integrity
- Version control
- Quality

The routine capture of information already held by the organisation must cease and re-use must be promoted wherever possible.

3.13.18 Operational staff are not experts in information management

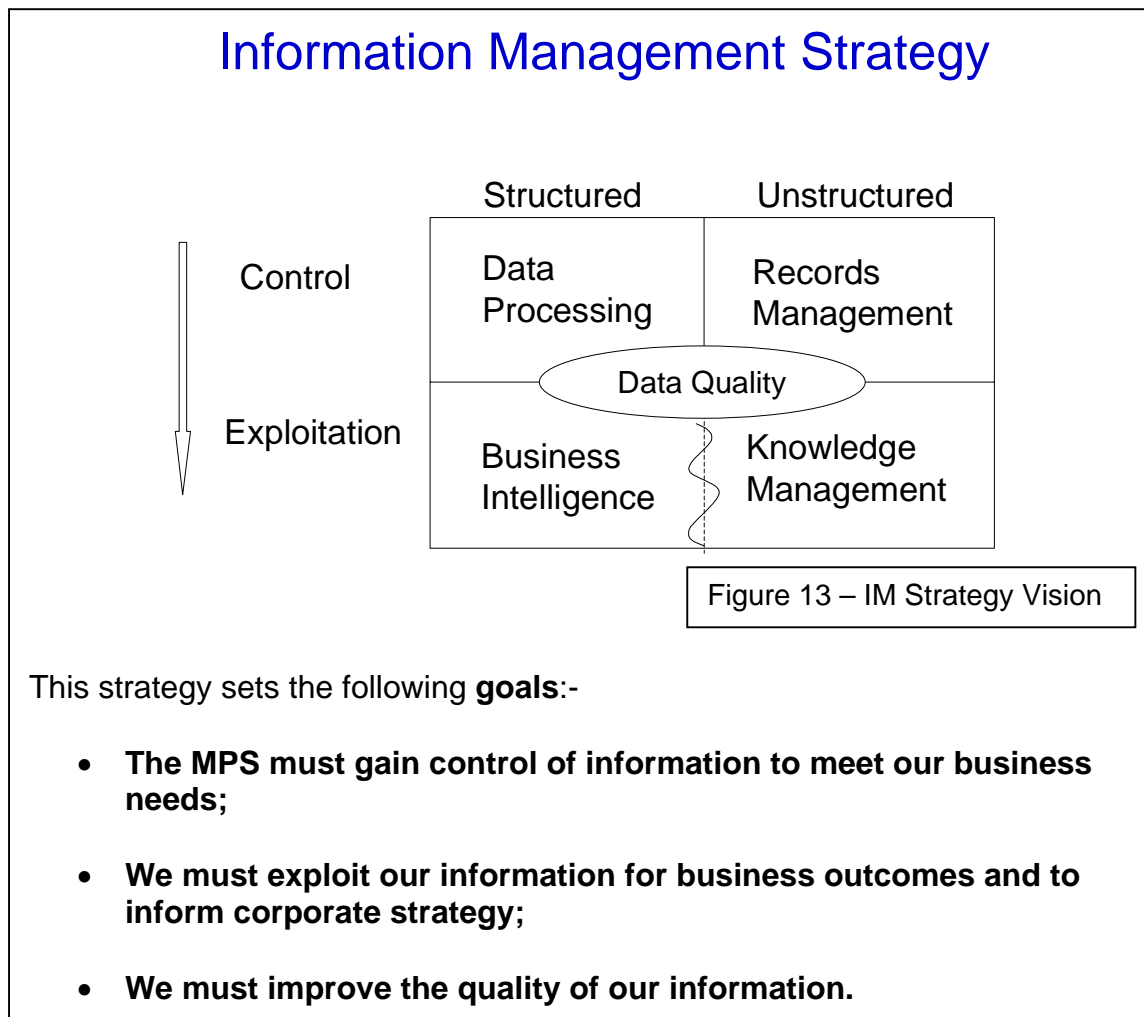
Whilst acquisition of certain organisational capabilities is critical to sustainable improvement in MPS IM, embedding good principles of information lifecycle management into 50,000 individuals is a mountainous task. Achieving this end as far as possible in a way which is transparent to MPS personnel must be explored.

3.13.19 Architecture is a key enabler for control and exploitation

Our information needs to be better organised so that we can find it and apply policy to it. An architecture will allow us to address many of the issues in this section.

## 4. Where we need to be – Key Messages

### 4.1 IM Vision: Information Management – from Control to Exploitation



Certain **key ideas** must be adopted to achieve these goals. These are:-

- Obtaining “one whole view” of information through:-
  - Joining up our policies to reflect real-world issues;
  - Joining up formats and sources of information.
- Using principles to describe how our information, organisation and behaviours need to change and which give us a vision of the goals.

The **enablers** for the strategy are:-

- Marketing the MPS Information Management vision, internally and externally;
- Consolidating and developing new corporate capabilities supporting that vision;
- Business change to deliver the strategy goals.

## 4.2 Controlling Information to Meet Business Needs

Statutory, strategic, and policy drivers along with productivity issues demand that we exploit *new markets* for our information from which substantial benefits may be derived. The key enabler for these new markets is the effective *sharing* of our information assets.

But unless we apply appropriate **controls** to achieve confidence in sharing, involving effective *security* and *quality* improvements we will expose ourselves to unacceptable *cost* and *risk*.

*Information and organisation growth* exacerbate *quality* issues and introduce *liabilities*.

## Sound Controls Enable Effective Exploitation of Information

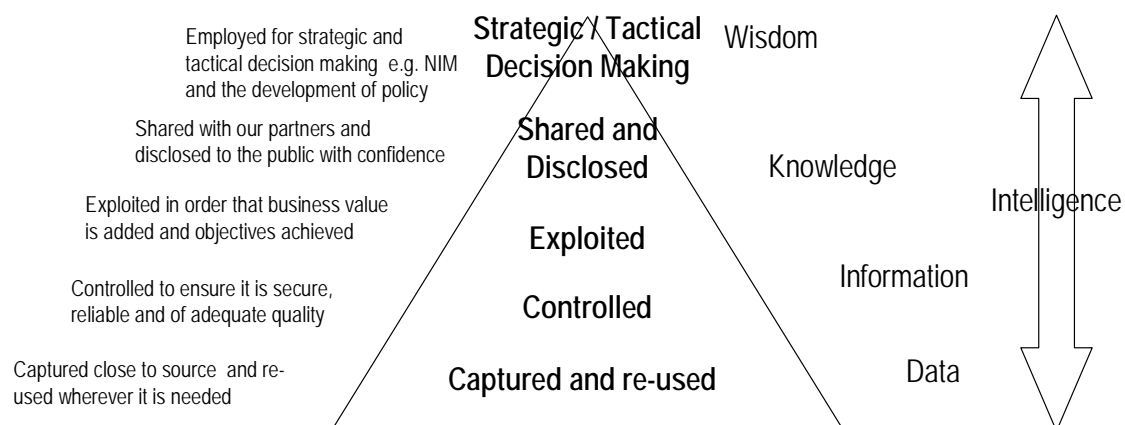


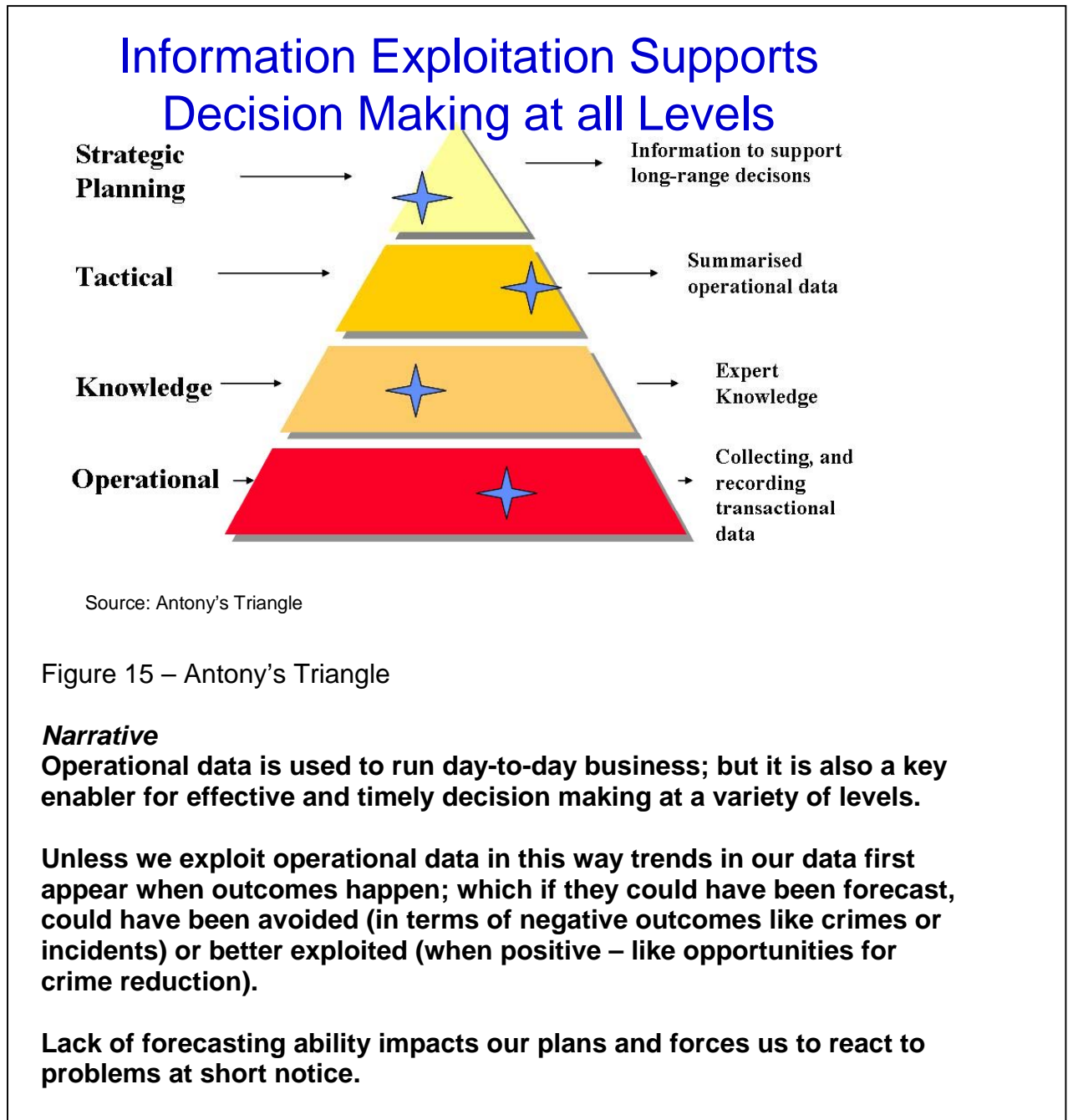
Figure 14 – DIKW / intelligence / information principles

### **Narrative**

**Information captured is subjected to controls to allow exploitation; significant exploitation issues for the MPS are sharing / disclosure and strategic and tactical decision making. Re-use of information promotes efficiency and integrity.**

### 4.3 Exploiting Information for Business Outcomes

We must build *new capabilities* to **exploit** the information resources we already have through the re-use of *experience* and better *analysis* of recorded information.



## 4.4 Improving Data Quality

### Data Quality is a Necessary Enabler for Effective Exploitation of Information

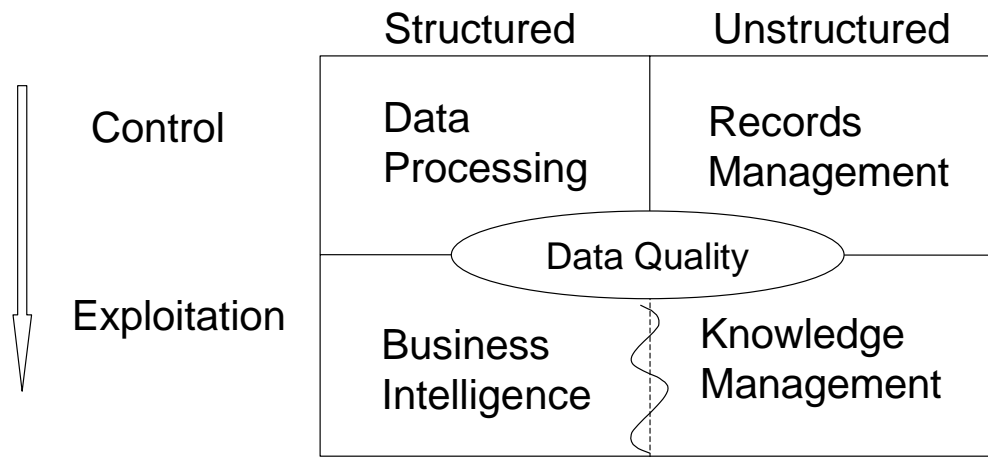


Figure 16 – Data Quality supports control to exploitation

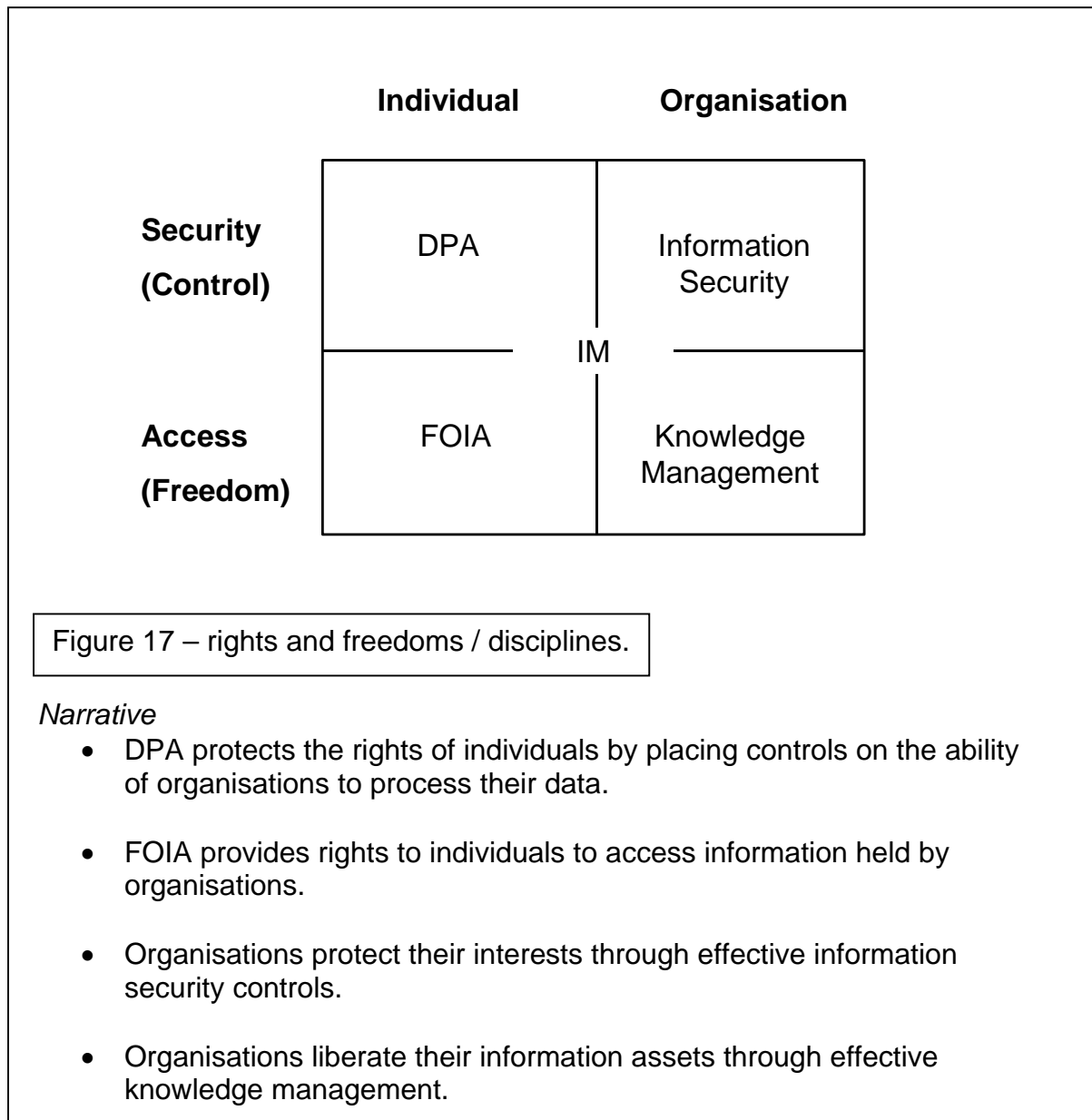
***Narrative:***

**In order to exploit information effectively it is critical that the issue of data quality is addressed. Seeking improved exploitation without addressing data quality is likely to result in poorly informed decision making. Data quality is therefore a key enabler to allow effective exploitation of information.**

## 4.5 One Whole View – Standardising and Simplifying Information

### 4.5.1 Our policy must balance security of operations and rights and freedoms

Information must be **trusted, accessible** and **usable (see vision)**. *Whose interests are protected, who may be granted access, and how information may be used* are issues which provide UK public sector organisations with some challenges.



**There is a balance to be struck between the rights and freedoms of individuals and the effectiveness of organisations in delivering effective IM. IM organisations in the UK public sector need to reconcile these interests. The relationships between the issues / disciplines shown need to be understood. Only by bringing our policy development and supporting disciplines together can we achieve joined up thinking – a “whole view”.**

#### 4.5.2 Joining up policy to control information

When applying controls, the real world is not conveniently divided into separate problems of data protection, information security, freedom of information or records management.

These issues are generally interlinked in any real situation. So must be our thinking.

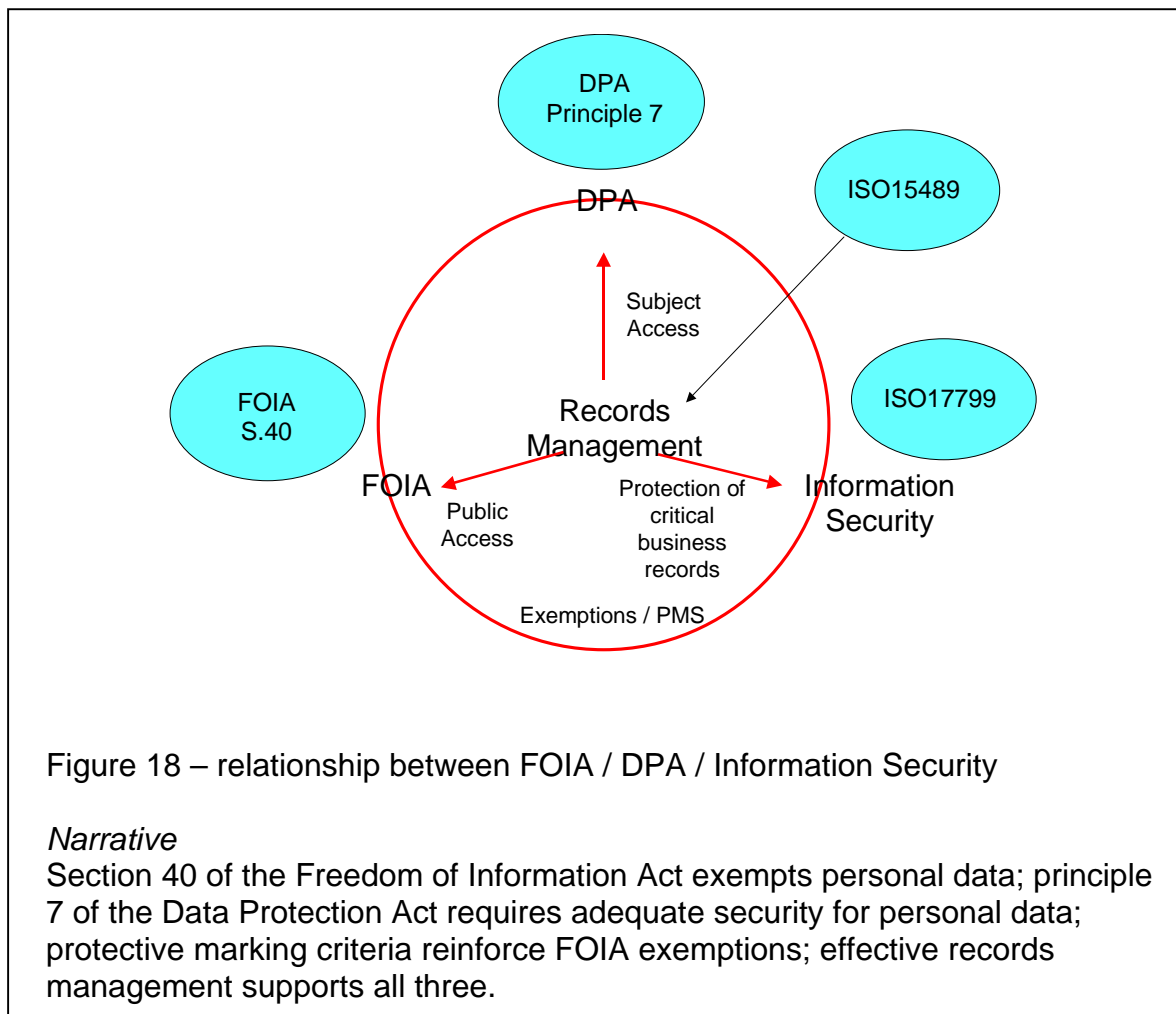


Figure 18 – relationship between FOIA / DPA / Information Security

#### *Narrative*

Section 40 of the Freedom of Information Act exempts personal data; principle 7 of the Data Protection Act requires adequate security for personal data; protective marking criteria reinforce FOIA exemptions; effective records management supports all three.

**All of these issues are interdependent and will need to be brought to bear on real world issues together. We must obtain a “whole view” - understand these relationships and find whole answers to real world problems.**

The relationship between these Acts and standards can be complicated. We need to introduce tools and processes which make them easier to apply, and to manage circumstances where their demands conflict.

#### Notes –

DPA = Data Protection Act 1998

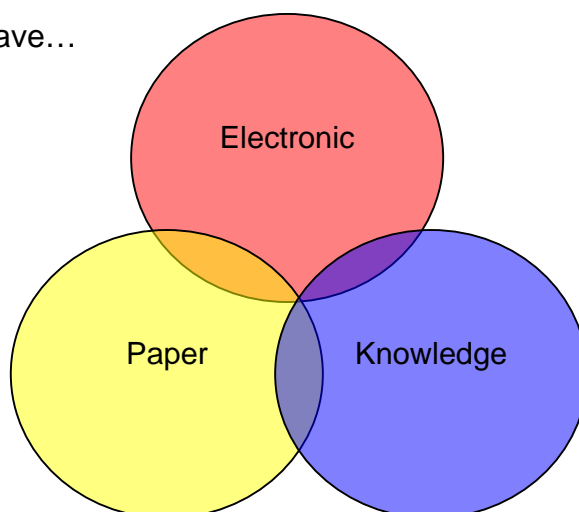
FOIA = Freedom of Information Act 2000

ISO 15489 = International Standard for Records Management

ISO 17799 = Code of Practice for Information Security Management

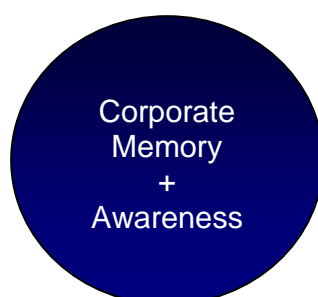
### 4.5.3 Joining up formats and sources of information

At present we have...



...three separate views of information depending on format. In control terms we also need to apply policies consistently across these formats.

**We need to overlay these views as far as possible, achieving one view...**



We need clear “whole view” policies to apply to this “one view” environment; the ability to apply those policies consistently; and to be able to access the information we need regardless of format.

*Narrative*

**To build “one whole view” we must introduce a new *architecture* for MPS information, supporting the corporate memory and awareness; we need the organisational *capability* to build it; and will need to exercise *authority* to maintain it.**

Figure 19 – Converging Formats

## **4.6 IM Vision – Information Principles, Organisational Qualities, Behaviours**

This section describes a vision of an MPS better able to cope with the demands of its environment. The vision is described through principles which set out how our information, organisation and behaviours should change.

### 4.6.1 Information Principles

Our *Information* needs to be –

- Trusted
- Accessible
- Usable

#### **Trusted**

##### ***One version, captured once and re-used***

Multiple copies:-

- of information of different versions which purport to be the same are a liability; it is likely that the wrong version will be acted upon;
- may imply the need to capture information more than once, suggesting wasted effort;
- imply a potential integrity problem in terms of keeping versions up to date;
- may become liabilities if they persist when the “official” version has been deleted according to policy.

##### ***Appropriate quality information for action***

Acting on poor quality information may have serious implications in a policing context including compromise to:-

- Public safety;
- Officer safety;
- Police operations;
- Litigation;
- Corporate reputation.

##### ***Compliant with policy and the law***

The use of information in the MPS is governed by a range of policies, both MPS policies and the policies of our partners and the communities (such as the criminal justice sector) to which the MPS belongs. Often these policies support legal requirements but can also reflect business needs such as corporacy and consistency.

##### ***Protected from loss or misuse***

This is basic security practice in protecting information from compromises to confidentiality, integrity and availability. When this principle is combined with *managed according to its value* this describes the need to employ cost-effective measures to protect information based on its business value and an assessment of risk.

## **Accessible**

### ***Managed according to its cost and its worth***

Not all information has the same worth in business and policing terms. The implications of retaining / storing / protecting / retrieving information out of the context of its business worth involves both financial and risk impacts.

### ***Captured close to source, available when and where it is needed***

Policing is a 24 x 7 activity which may take place anywhere. Information is core to decision making and needs to be available anywhere a decision can be taken, when it needs to be taken. Outcomes often need to be recorded when the event is at least fresh in the mind; and as far as possible, whilst it is happening.

### ***Shared with our partners and disclosed to the public with confidence, in an open and accountable manner***

Sharing information beyond the boundaries of the organisation involves consideration of both legality and risk. Disclosure involves an accountable business decision to release information without seeking the application of controls.

## **Usable**

### ***Easy to find and deploy***

Information which is difficult to find wastes resources and ultimately may result in the information not being found at all. Good deployment enhances the effectiveness of the information once it is retrieved.

### ***Presented in context, in the best way possible***

Policing involves the need to make decisions quickly, to make them about complex issues and to make them intuitively. Presentation of information in the right context can reveal meaning which may be hard to detect in "raw" form.

### ***Used and understood by a skilled workforce***

Our information needs to be understood and used by people with the right skills and capabilities to be used to its best effect.

#### 4.6.2 Organisational Qualities

This section defines the qualities desired in the MPS *organisation* to fulfil the goals of the IM Strategy.

The future will require an MPS in which we

- Know what we know and how to find it;
- Promote openness and accountability;
- Protect our information proportionately, according to its worth;
- Exploit our information effectively and efficiently;
- Manage the information we need in accordance with business need, policy and the law;
- Share our information with others.

These themes are explored further below.

##### ***Know what we know and how to find it;***

We must understand what information we hold. Subject to appropriate security controls and business context, we must be able to retrieve it, both to meet statutory needs and to support the basic requirements of our business. In order to do this we must move from a view of information as a resource supporting local needs to a corporate resource.

##### ***Promote openness and accountability;***

Our first consideration must be to share information as widely as we can, both within the business and without. This supports our core value of openness and provides the opportunity to realise the maximum business potential from the information we hold.

Accountable decisions are generally good decisions. Promoting and supporting accountability for our decision making speaks to the core of our ability as an organisation to deliver. Committing our decisions to the corporate memory achieves this; and also our ability to learn as an organisation. Good record keeping is therefore fundamental to maintaining an open, accountable, learning and performing organisation.

##### ***Protect our information proportionately, according to its worth;***

Our ambitions toward openness must recognise that there will never be a day when all of our information assets will be in the public domain, because of the business we are in. We hold information about and belonging to others, and we must respect their rights in achieving our aims. We must take proportionate, cost-justified steps to ensure that information to which access must be controlled is protected against loss or compromise. We must employ

standards to ensure that the measures we take are effective, equivalent to those of our partners and are consistent across our business.

***Exploit our information effectively and efficiently;***

Aside from the physical act of apprehending offenders, almost everything we do involves the management of information. It is therefore fundamental to our ability to perform as an organisation that we exploit the information we hold effectively; and that we are as efficient as possible in doing this. To achieve these ends we will seek to dissolve artificial boundaries which keeps our information parochial; minimising the versions that we keep and realising connections between facts that we hold for different purposes. We must also dissolve the boundaries between data, information and knowledge, allowing us to see recorded, explicit information in both paper and electronic formats, and experiential, tacit information as the same resource.

***Manage the information we need in accordance with business need, policy and the law;***

There is a growing corpus of statutory controls concerning the management of information. We must understand these controls and ensure that they are applied across our business and across all appropriate formats.

In a connected world, we must understand and comply with the policies of our business partners and the communities we join.

The policies, processes, structures and tools we use to manage the information which supports our business must be clear, comprehensible and made known effectively to those who must use them.

***Share our information with others;***

The modern world increasingly involves the delivery of public services without reference to the conventional boundaries of public service departments. This will give rise to new challenges in respect of consistency in the meaning of our information, how it is transmitted and how it is governed. To effect this we must apply a variety of standards which will make these values consistent with our business partners.

It is also increasingly difficult to define the boundaries which define the organisations involved in delivering “policing” to the capital; and thereafter where “policing” meets the wider needs of society. In achieving our organisational goals and those of our business sectors we are in danger of losing an applicable definition of who we are and our ability thereafter to apply the right policies and controls to our information.

We must develop more sophistication in our ability to understand and apply valid legal powers to share information and to manage the mitigation of risk which may arise from the act of sharing it.

### 4.6.3 Personal Behaviours

This section defines the qualities desired in MPS *personnel* to fulfil the IM Strategy. They comprise a set of behaviours which should be marketed to all MPS personnel.

#### **Basic IM Principles**

Together the principles spell the mnemonic

**S**ecure and protect valuable information

**O**ne version of the truth

**R**eview information over time

**T**hink of finding when storing

**E**xpect to share information

**D**ispose of redundant information

#### ***Secure and protect valuable information***

*All information is not the same.*

- Not all of our information has the same value to our business.
- Some of our information is critical to running our organisation. We need to rely on getting access to it when we need it.
- Some of our information would hurt our business or others if the wrong people got access to it.
- We need to understand which information may be critical / damaging.
- We need to protect this information in proportion to what might happen if it is lost or misused.

*We can value our information to understand what is important.*

*We can understand the risks to our information.*

*We can use our knowledge of value and risks to understand the measures necessary to protect it.*

#### ***One version of the truth***

*Acting on the wrong version of information / incorrect information can harm us or others.*

- We can waste time.
- We can make mistakes. They can be bad ones.

*We can label our information to show its version.*

*We can keep records of the versions so we know which is relevant and track the changes.*

#### ***Review information over time***

*The value of information can (will) change.*

- Our business needs and our environment change over time.
- The information necessary to meet those needs changes too.

*We can review the information we hold.*

*We can change its protective mark if this is appropriate.*

*We can mark it for disposal.*

### ***Think of finding when storing***

*If information is worth storing, it must be worth being able to find it again.*

- Failure to retrieve valuable information negates its value.
- We may have to repeat work already done.
- We may act on incomplete or wrong information.
- We may be unable to evidence or defend our decisions or actions.

*We can use standard terms to store information.*

*We can store our information in a logical structure.*

### ***Expect to share information***

*Sharing knowledge is power. Openness evidences confidence and honesty.*

- Information must be a corporate resource if we are to realise its full value.
- The public have a right to know that we are working effectively in their interest.

*We can publish as much of our workings as we are able, to the public and to each other.*

### ***Dispose of redundant information***

*Information can be a liability as well as an asset.*

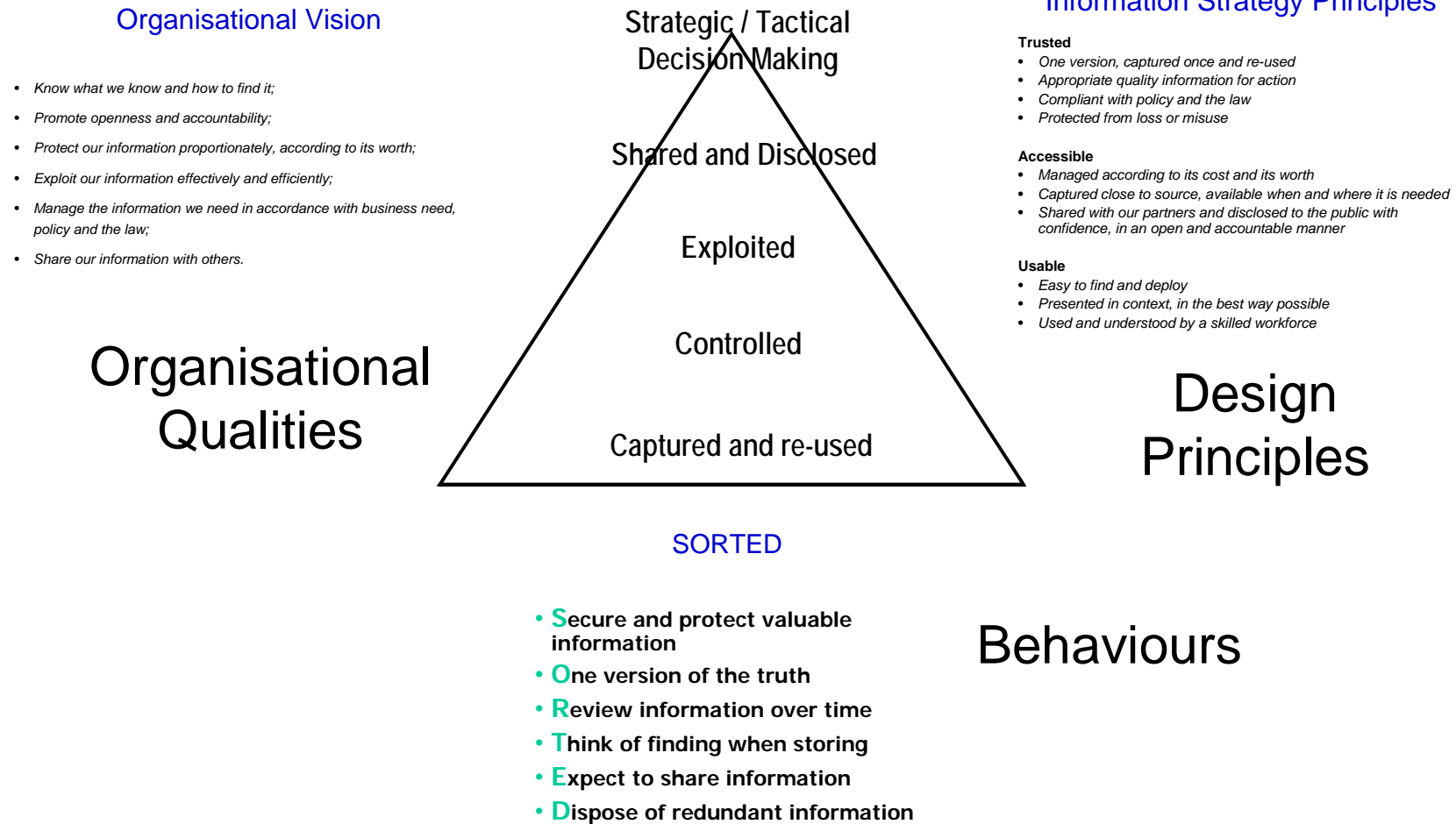
- Information kept past the needs of the business costs us money; we will have to maintain it for no purpose; it may breach the law; it may damage our reputation; it is more difficult to find if we are keeping too much.

*We can dispose of information if we no longer need it.*

*We can keep records of what we have disposed of or plan to dispose of so that we can justify ourselves if challenged.*

Together, our principles describe the information, organisation and behaviours we need for a better MPS

# IM Vision - Principles



## **5. How we get there – Enabling Information Quality**

This section discusses the steps necessary to take “where we need to be” and to put it into effect.

### **5.1 IM Organisational Capabilities**

Certain capabilities are needed to deliver the IM vision set out in “where we need to be”. The following paragraphs explore those capabilities and indicate progress or the need for it.

#### 5.1.1 IM Group

As discussed in “where we are”, a capability has been established in the Directorate of Information with the remit to focus on the business issues in information. The Information Management Strategy (2005) proposed a review of the functions purposed to this end and this was undertaken during the following year.

As a result of the review:-

- Records Management Branch, the Publication Scheme, Public Access Office, Intranet / Internet Team and Forms Unit have been incorporated inside IM Group;
- New capabilities have been built addressing Data Quality and Data Modelling;
- An initiative has begun to introduce a Knowledge Management capability, initially within the Directorate of Information;
- The results have been consolidated into a DoI “Group” called IM Group.

There is however more to do;

- A major business change activity is needed to meet the Bichard CoP / MoPI;
- The relationship between the data modelling capability (Managed Information Team or MIT) and the Corporate Data Warehouse (CDW) needs to be established;
- The Information Sharing Support Unit needs to be marketed to the MPS and made sustainable;
- The shape of the Group as a whole needs to be reviewed anew.

These activities need to be scoped and resourced.

### 5.1.2 IM Professional Specialism

Dialogue has been underway with the professional standards bodies which own the “information space” – principally the British Computer Society (BCS) and Chartered Institute of Librarians and Information Professionals (CILIP). A forum (the IM Professional Forum) has been established, including BCS / CILIP, Gartner, Henley Management College and other “delivery” organisations. The need for definition of the professional home for information disciplines has been recognised and is being taken forward under the banner of the BCS IT Professional Forum.

This needs to be pursued to a conclusion, hopefully by the inclusion of a recognised professional discipline for IM within the SFIA (Skills Framework for the Information Age) framework.

Once this is achieved, options will be to introduce these concepts to the UK Police Service and to the MPS. The order of these steps needs to be decided.

### 5.1.3 Information Managers

Around 80 – 100 “Information Managers” were seeded throughout the MPS during 2004/05 to improve MPS information management practices. One of the main drivers for this action was the Freedom of Information Act 2000.

The role and effectiveness of the MPS Information Managers is to be reviewed in the light of changes to MPS circumstances such as the advent of the right of public access under FOIA (01/01/2005) and the coming of the Bichard CoP / MoPI.

### 5.1.4 Information Authority and supporting Processes

An “Information Authority” (IAu) has been constructed to champion the information principles in this strategy. It has the following responsibility:

*“To ensure the MPS establishes, develops, implements and maintains appropriate information architectures, standards, methodologies, policies, strategies and plans for the collection and use of MPS information, to support and enable the business in the effective delivery of current and future operational and support services.”*

All information management policy decisions must be agreed with and ratified by the IAu before any activity commences, or resources are committed; including policy issues implicit in design of new business solutions.

The IAu needs certain supporting processes to allow it to function. These have been defined and work undertaken to address the queue of business solutions in development for MPS requirements.

At a later stage the IAu should be extended to embrace management of all MPS information collections, corporate or local, ICT-enabled or manual.

### 5.1.5 Information Architecture

Holding information outside an architecture is not sustainable in a large modern organisation. An architecture is needed to:-

- Achieve efficiency in investment and procurement
- Share information effectively
- Maintain an effective corporate memory
- Promote good quality information
- Enable accountable decision making
- Manage information risk and cost

A properly implemented information architecture enables staff to control and exploit information without needing to be experts in information management.

Introducing an information architecture involves:-

- Introducing a framework of governance, policies and standards;
- Building certain organisational capabilities which develop and maintain the architecture;
- Achieving investment in business tools (including technology) which enable the introduction of the architecture to the organisation;
- Integration with technology architecture.

An information architecture allows an organisation to understand the information it holds and the business issues which apply to it. It enables policy *controls* to be applied to information so that it can be managed in the context of its business value – for example how long it should be kept, and who may have access to it. A clear understanding of these controls enables information to be *exploited* to achieve business benefits – for example how it may be shared, or combined meaningfully for analysis purposes. Knowing what information you have also helps to prevent information being collected which is already held somewhere else.

An information architecture does not concern itself with issues of technology; but it does inform the requirements for technology investments.

An information architecture understands the structure and business rules which apply to organisational information.

An information architecture would provide the following benefits:-

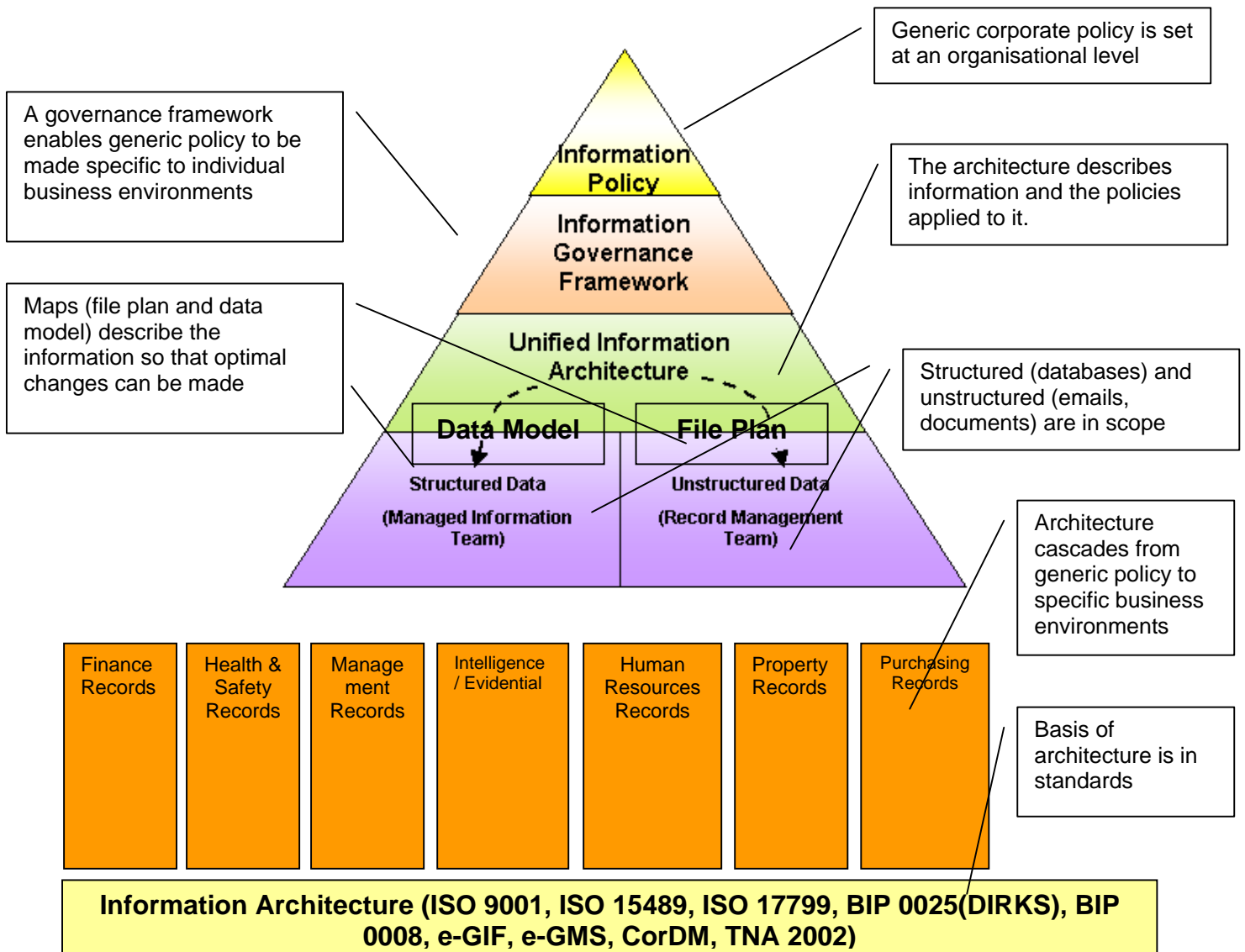
- The ability to connect information together from different sources to create added value from the results (*Bichard, warehousing for performance, intelligence*);
- The ability to apply policy to information based on its business value rather than based on the format or technology which holds it (*Bichard, MPS Storage Strategy, information sharing*);

- The ability to store information in a common logical filing structure and enable its retrieval (*Bichard, information sharing, accountable decision making supporting the corporate memory*);
- The means to minimise the copies of information held and the number of times it needs to be captured (*efficiency and data quality*)

### 5.1.6 Master Reference Data

Certain collections of information within the architecture are of key importance as they are widely re-used and / or high reliance needs to be placed on them. These include data concerning identity, and spatially referenced data. Because of their ubiquity it is often difficult to find MPS owners for these collections and it is proposed that IM Group lead on managing these for the Service.

**Figure 21 -Information Architecture in Graphic Form**



#### 5.1.7 Information Policy Framework

MPS has established an “Information Policy Framework” (IPF). The IPF identifies policy needs which must be addressed by all MPS business solutions. The IPF has been developed and is in change control. However it needs to be better integrated with the development cycle for MPS solutions (the project lifecycle). The IPF informs the top tier of an Information Architecture.

At a later stage this framework should be extended to embrace management of all MPS information collections, corporate or local, ICT-enabled or manual.

#### 5.1.8 Information Governance Framework

The Information Governance Framework (IGF) provides a governance model to enable corporate policy to be made applicable to individual collections of information. It will sit toward the top of the architecture and for each collection we hold it will:-

- Define the business interest (the “owner or governor”) for each collection;
- Define the rules which need to be set for MPS information.

By this means we will assign rules to govern all our information, and accountability for setting them. The IGF enables the second tier of an information architecture.

#### 5.1.9 Data Modelling – Managed Information Team

A team has been established to model MPS structured data and processes. The MIT supports the IAU in promoting efficient re-use of information in new or changed business requirements.

This capability needs to be made sustainable and to extend its remit from enterprise data modelling (EDM) into enterprise architecture frameworks (EAF). Dialogue is underway with PITO to explore a common national toolset to support this function. Toolset options exist to extend these controls from the structured environment to cover unstructured information. If such tools are employed IM Group should review how the modelling of structured and unstructured information assets are managed organisationally within the Group.

#### 5.1.10 Business Intelligence Capability

MPS is about to commission the tools to establish a corporate data warehouse (CDW). Whilst the procurement of disk capacity and software tools to extract, transform and load (ETL) data into the warehouse will be critical enablers to achieving added value from our transactional information, this falls significantly short of the capabilities needed to derive business intelligence necessary to inform our tactical and strategic decision making.

An assessment of the capabilities necessary, and engagement with MPS stakeholders in outcomes of BI, leading to a BI strategy, must be undertaken.

#### 5.1.11 Information Assurance

MPS has established functions to provide assurance of information in respect of legal governance and information security. The boundary of this assurance capability needs to be reviewed to ensure that the “one whole view” of information issues can be applied to ensure compliance with the IM Vision.

#### 5.1.12 Knowledge Management Capability

Following publication of the MPS Information Management Strategy in December 2004, a Knowledge Management capability has been constructed in IM Group. This capability has been deployed to improve re-use of information in the Directorate of Information, as a proving ground for methods / approaches. On completion of this objective in DoI this capability needs to be reviewed, and the business case for an MPS KM capability established.

#### 5.1.13 GIS Capability

The MPS GIS Strategy needs to be reviewed and revisited to ensure it fits with the wider Information Strategy. A programme of activity will need to be embarked upon to rationalise the legacy GI applications currently deployed in order to exploit the development of corporate solutions and centrally managed data repositories holding up to date spatial data sets.

#### 5.1.14 Identity Management Capability

A strategy for the management of identities (people, and other entities which need to be uniquely identified) must be developed and supporting capabilities identified.

#### 5.1.15 ACPO / ACPOS Community Security Policy Compliance

MPS CSP compliance has been achieved; this needs to be sustained, through:-

- Maintenance of security policy
- Maintenance of security governance (incident reporting, METSEC Programme Board)

#### 5.1.16 Information Sharing Capability

A deliverable of the Corporate Information Sharing Project (CISP) has been the Information Sharing Support Unit (ISSU) and a toolkit to assist in the introduction of an improved, standardised model for sharing of information supporting MPS partnerships. This capability needs to be marketed and made sustainable. A knowledge base of Information Sharing Agreements (ISAs) is being constructed and this needs to be built on as a component of MPS compliance with the Bichard Manual of Police Information (MoPI).

## **5.2 Business Change**

This strategy proposes changes to MPS business operations and processes. This section explores those proposals and identifies necessary action.

### 5.2.1 Compliance with the Bichard Code on Management of Police Information

As the implications of the Code and Guidance suggest major business change for Forces it is recognised that compliance cannot be achieved straight away. A

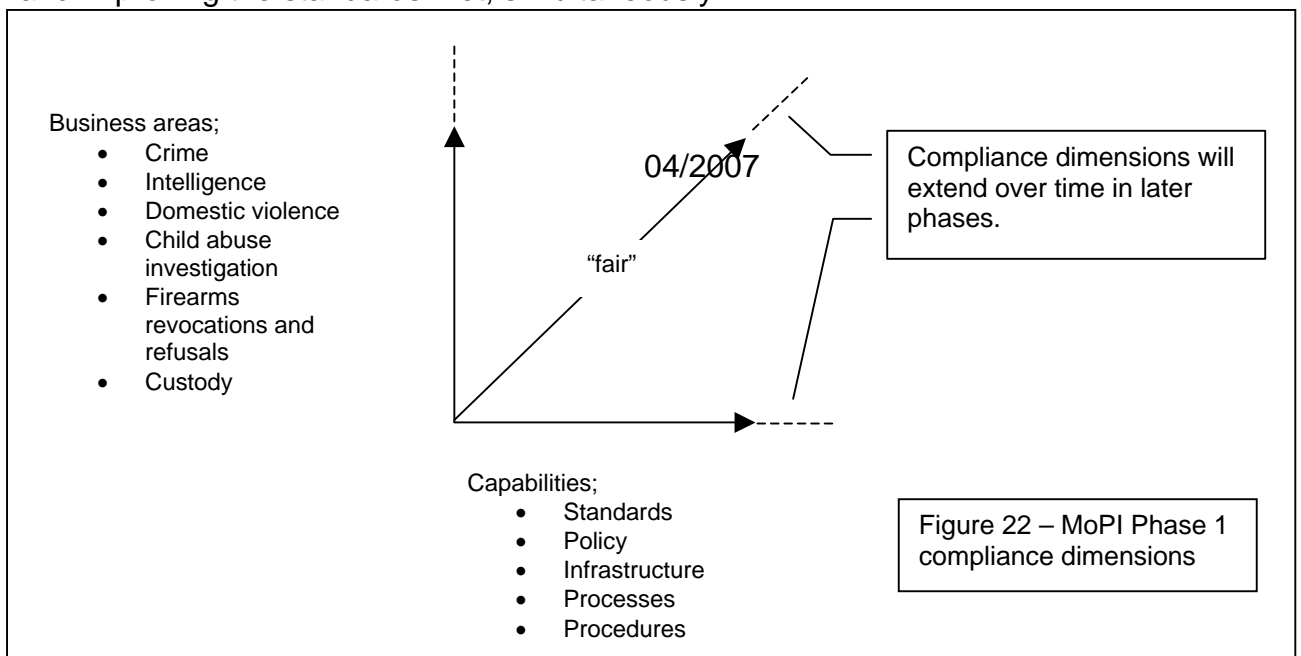
compliance regime and supporting toolset are in the process of construction based on the CoP and MoPI which attempts to introduce necessary changes in phases. Only the first phase is defined at present; compliance will be measured by HMIC (Phase 1 by 31<sup>st</sup> March 2007). This is likely to take the form of self-assessment at least in the short to medium term. There is no end date set for full compliance.

From the Guidance is drawn a set of minimum standards for Phase 1 (now called Threshold Standards) which indicate the business controls which should be present in compliant organisations. HMIC will use the Threshold Standards to measure compliance. Phase 1 of MoPI seeks to address the following business areas

- Crime
- Intelligence
- Domestic violence
- Child abuse investigation
- Firearms revocations and refusals
- Custody

Phase 1 also emphasises standards, policy, infrastructure, processes and procedures, leaving other issues for later phases. It is the intention to “raise the bar” on compliance by requiring Forces to meet standards for “fair” initially and to raise these standards later to meet “good” and / or “excellent” criteria later. A set of “Threshold Standards” has been defined setting out these criteria.

This suggests a regime which will seek progressive improvements in terms of widening the business areas addressed, extending the range of capabilities and improving the standards met, simultaneously.



Following the NIM-aligned methodology for implementation a “Capability Assessment” and a “Force Action Plan” will assess force readiness and define change activities for each phase. Resources to undertake these assessments

and deliver change must be found; and the necessary business change effected.

#### 5.2.2. Bichard IM Strategy and an Information Governance Framework

Phase 1 Bichard MoPI compliance will drive the introduction of a governance model for information, described as an IM Strategy. This will define roles and responsibilities for the management of information assets. It will provide a strong business driver for the introduction of an IGF, described above.

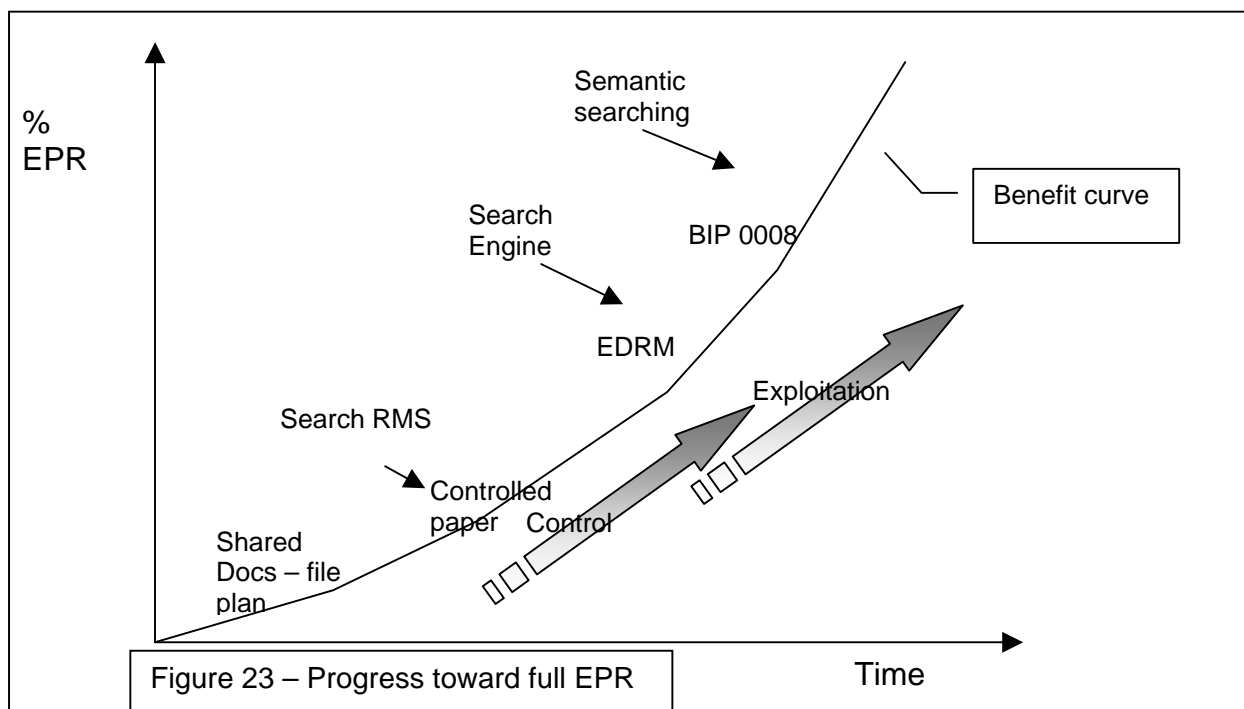
This provides an opportunity for MPS to introduce sound and nationally-consistent governance for information.

#### 5.2.3 MPS Records Management Improvement, the move to Electronic Content Management and an Electronic Primary Record

Our current means for managing essential business records rely largely on a central repository which employs manually-intensive processes to maintain paper-based records. We have a widely distributed, technology-enabled organisation. In order to move from one paradigm to the other we need to introduce the level of authentication and accountability to the electronic processes as can be found in our paper processes. To get there we need certain enablers:-

- We need to categorise our information in such a way that we can file and retrieve it and apply policy to it consistently across the MPS. For this we need an MPS-wide application of the *MPS file plan*.
- We need to explore technology enablers which can enable the MPS file plan, removing reliance on written procedures. In the unstructured environment these tools are commonly described as *electronic documents and records management (EDRM)*.
- These tools must be implemented in a way that respects necessary standards for maintenance of *evidential weight, information security and good records management*.
- For a subset of information the tools need to extend from record keeping into the domain of publishing and communications. At this point we will have achieved *electronic content management*.
- By this means we will have moved progressively to an *electronic primary record*.
- We must mirror these controls as necessary in both structured and unstructured environments.

This will provide us with the bottom two tiers of an MPS information architecture. This goal will not be achieved overnight. It is possible, however, to move progressively to the goal realising benefits on the way.



Significant additional benefits in terms of time-to market of business solutions can be achieved by automating processes using EDRM and associated tools such as document image processing and workflow.

In this model processes can be the subject of local manipulation, with necessary standards, but the data stores they feed must be corporate and corporately managed.

Performance information in this model is also derived from the automated processes instead of being an additional process overhead.

#### 5.2.4 Better Administration of the Paper Legacy

In moving MPS to an electronic primary record, the investment in paper records cannot be overlooked. Most of our business critical records are based on paper and this will remain the case, albeit decreasing in proportion, for as much as 30 years. We must reintroduce sound working practices for paper file management and carry this practice through into the electronic replacement.

#### 5.2.5 Data Quality Improvement Programme

A Data Quality Team has been set up within the Information Management Group to give an organisational lead on data quality issues and to support the business in improving its information assets. It is a repository of expertise and knowledge that can be drawn on to advise the DoI and the MPS on data quality issues.

It is a multi-skilled team comprising individuals with expertise in:

- Information Resource Management
- Data Analysis

- Business Process Analysis
- Project Management

A technical environment has been developed and maintained with tools to analyse and, where possible improve data quality in selected environments.

When leading data improvement projects the team follows a broad methodology based on industry standard good practice through

- Engagement
- Data Analysis and Profiling
- Improvement
- Sustainability

Now that the capability has been built and deployed against a number of MPS issues, governance needs to be established to decide on priorities for further deployment of the Data Quality Team, and this should inform the construction of a programme of agreed improvement interventions to raise the quality of MPS information.

#### 5.2.6 ACPO / ACPOS CSP Compliance – Change Activities

In addition to maintenance of capabilities, business change activities will be needed to ensure sustainable compliance with the CSP. These will include security awareness measures and infrastructure improvements through the CUBIT Service Improvement Programme.

## 6. Glossary

ACPO	Association of Chief Police Officers
ACPOS	Association of Chief Police Officers (Scotland)
ALG	Association of London Government
BCS	British Computer Society
BI	Business Intelligence
BIP0008	Code of Practice for Legal Admissibility of Electronic Records
BIP0025	(DIRKS – Developing and Implementing Record Keeping Systems)
CDW	Corporate Data Warehouse
CISP	Corporate Information Sharing Project
CILIP	Chartered Institute of Librarians and Information Professionals
CJO	Criminal Justice Organisation
CJX	Criminal Justice Extranet
CoP	Code of Practice (Bichard)
CorDM	Corporate Data Model
CRIS	Crime Report Information System
CSP	ACPO / ACPOS Community Security Policy
CUBIT	CGS, Unisys, BT (MPS technology partner)
DIKW	Data, Information, Knowledge, Wisdom
DoI	Directorate of Information
DPA	Data Protection Act 1998
EAF	Enterprise Architecture Frameworks
EAF4PS	Enterprise Architecture Framework for the Police Service
EDM	Enterprise Data Modelling
EDRM	Electronic Documents and Records Management
e-GIF	e-Government Interoperability Framework
e-GMF	e-Government Metadata Framework
e-GMS	e-Government Metadata Standard
EPR	Electronic Primary Record
ETL	extract, transform and load
FOIA	Freedom of Information Act 2000
FSS	Forensic Science Service
GLA	Greater London Authority
HMIC	Her Majesty's Inspectorate of Constabulary
HOPSATS	Home Office Police Science and Technology Strategy
HRA	Human Rights Act 1998
IAu	Information Authority
ICT	Information, Communications, Technology
IM	Information Management
IMBA	IM Business Area (ACPO)
IS	Information System(s)
ISAs	information sharing agreements
ISO 15489	International Standard for Records Management
ISO 17799	Code of Practice for Information Security Management

ISO15489	International Standard for Records Management
ISO17799	Code of Practice for Information Security Management
ISS4PS	Information Systems Strategy for the Police Service
ISSU	Information Sharing Support Unit
KM	Knowledge Management
METSEC	MPS Security Policy / programme
MIT	Managed Information Team
MMP	Met Modernisation Programme
MoPI	Manual of Police Information (Bichard)
MPA	Metropolitan Police Authority
MPS	Metropolitan Police Service
MSA	Mapping Services Agreement
NCPE	National Centre for Policing Excellence
NCRS	National Crime Recording Standard
NICF	National Integrated Competency Framework
NIM	National Intelligence Model
NIO	Northern Ireland Office
NIRS	National Incident Recording Standard
NPIA	National Police Improvement Agency
NPP	National Policing Plan
OTIS	Operational Technology Information System
PESTLE	political, economic, social, technological, legal and environmental
PITO	Police IT Organisation
PNC	Police National Computer
PPAF	Policing Performance Assessment Framework
PRA	Public Records Acts 1957 – 1959
PSA	Public Service Agreement
PSDB	Police Scientific Development Branch
RIPA	Regulation of Investigatory Powers Act 2000
RMB	Records Management Branch
RMBVR	Records Management Best Value Review
RMS	Records Management System
SFIA	Skills Framework for the Information Age
SIC	Statement on Internal Control
SMART	Strategies for Metadata and Related Taxonomies
SWOT	Strengths, weaknesses, opportunities, threats
TNA	The National Archive
TP	Territorial Policing
UK	United Kingdom