FIDIS

Future of Identity in the Information Society

Title:	"D4.6: Draft best practice guidelines"
Author:	WP4
Editors:	James Backhouse (LSE) Bernard Dyer (LSE)
Reviewers:	Denis Royer (JWG, Germany) Thierry Nabeth (INSEAD, France) Mireille Hildebrandt (Vrije Universiteit Brussel, Belgium)
Identifier:	D4.6
Type:	[Deliverable]
Version:	2.0
Date:	October 2006
Status:	[Final]
Class:	[Public]
File:	fidis-wp4-del4.6.Draft best_practice_guidelines.doc

Summary

This deliverable is concerned with the recommendations for best practice guidelines and the need for an effective development method and framework, which can be widely used for managing all aspects of identity resulting from the FIDIS research. The emphasis is on the delivery of a practical approach, which incorporates sound tools and techniques, which can be applied in the project and other settings.

The proposed method is a generic one that may be applied to any type of research project, business operation or delivery service to ensure it will fit effectively into a given environment. The method is flexible and customisable and incorporates clearly defined events and procedures throughout the information lifecycle. A holistic and systematic approach is adopted.

The method is first described and then an outline is provided, as to how it may be applied to interoperability, within the e-health sector.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
1.0	14.07.2006	Initial release (James Backhouse and Bernard Dyer) Continuous developments. Contributions to this document: VUB: Mireille Hiderbrandt. Contributions to some of the key concepts. INSEAD: Thierry Nabeth. Contributions to some of the key concepts.
2.0	27.10.2006	Final version

Foreword

This document outlines draft best practice guidelines for managing all aspects of identity resulting from the FIDIS research. They will be developed during the remainder of the project, and will include the work of future deliverables D4.7 to D4.9 in the 3rd Work Plan and the proposed D4.10 in the 4th Work Plan. It is envisaged that the final best practice guidelines will be established after the delivery of D4.10 "Specification of a portal for interoperability of identity management systems". We will be pleased to receive comments on the draft guidelines from researchers of the FIDIS partner institutions, following the dissemination of this document.

Table of Contents

1 EXECUTIVE SUMMARY....7

2 INTRODUCTION.... 8

2.1 WHAT IS BEST PRACTICE? 8
2.2 AIMS OF THE DELIVERABLE 8
2.3 RATIONALE 9

3 AN INFORMATION MANAGEMENT METHOD AND FRAMEWORK FOR FIDIS..... 10

4 BEST PPRACTICE METHOD …… 11

4.1 REQUIREMENTS DOMAIN....12
4.1.1RESEARCH ACTIVITIES…… 12
4.1.2 MANAGEMENT ACTIVITIES....13
4.2 BUSINESS MODELLING DOMAIN.... 14
4.2.1 TYPES OF MODELS....14
4.2.1.1 ENTITY MODELS....15
4.2.1.2 STAKEHOLDER MODELS....16
4.2.1.3 PROCESS AND INFORMATION FLOW MODELS.... 16
4.2.1.4 COMPLIANCE MODELS....16
4.3 INFORMATION MANAGEMENT PRINCIPLES DOMAIN....18
4.3.1 FIVE PRINCIPLES OF INFORMATION MANAGEMENT…… 19
4.3.1.1 INFORMATION....19
4.3.1.2 DUTY OF CARE....20
4.3.1.3 PROCESSES AND PROCEDURES....20
4.3.1.4 ENABLING TECHNOLOGIES....20
4.3.1.5 AUDITING....20
4.4 SYSTEM DOMAIN.... 20
4.5 MAPPING THE INFORMATION....20

5 APPLICATION OF THE METHOD.... 22

5.1 INTEROPERABILITY....22
5.2 E-HEALTH SECTOR....28
5.2.1 MANAGING THE STAKEHOLDER MODEL....28
5.2.2 BEST PRACTICE WITHIN INDIVIDUAL INSTITUTIONS....28
5.2.2.1 REQUIREMENTS DOMAIN....29
5.2.2.2 BUSINESS MODELLING DOMAIN....29
5.2.2.3 INFORMATION MANAGEMENT PRINCIPLES DOMAIN 30
5.2.2.4 SYSTEMS DOMAIN.... 31
5.2.3 MAPPING BEST PRACTICE PROCEDURES....31

6 CONCLUSION AND FUTURE WORK.....…… . 33

6.1 3RD WORK PLAN.....… …33
6.2 4TH WORK PLAN…… ……33

1 Executive Summary

This deliverable concerns the recommendations for best practice guidelines and the need for an effective development method and framework, which can be widely used for managing all aspects of identity resulting from the FIDIS research. The emphasis is on the delivery of a practical approach, which incorporates sound tools and techniques, which can be applied in the project and other settings.

Order and structure are necessary in order to manage the processes and information and to ensure that researchers are able to work effectively with each other within the FIDIS project. Imposing a method, that provides a framework and discipline, should assist with the development, delivery and dissemination of the results.

The proposed best practice guidelines are derived from a generic method that may be applied to any type of research project, business operation or delivery service to ensure it will fit effectively into a given environment. The method is flexible and customisable and incorporates clearly defined events and procedures throughout the information lifecycle. A holistic and systematic approach is adopted.

The rationale for developing the method and framework to assist with the creation of the best practice guidelines is outlined in Chapter 2. Chapter 3 emphasises the importance of applying information management techniques within FIDIS. The best practice method is described in Chapter 4. Chapter 5 discusses interoperability and then outlines how the method may be applied to interoperability within the e-health sector. Chapter 6 discusses how the work will be progressed in the FIDIS 3rd and 4th Work Plans and outlines the envisaged method for disseminating and exploiting the FIDIS results.

2 Introduction

FIDIS examines the characteristics of identity management systems from the technical, policy, legal and socio-cultural perspectives, and Work Package 4 addresses the interoperability issues therein. It looks at the limits on identity systems designed for one purpose being used for other purposes (inter-purpose interoperability: e-government, e-health, e-commerce systems), and sees the role of the market in generating interoperability (interplay of governmental regulation, self-regulation and no regulation: cross-border and cross-sector comparisons). The project involves research in many disciplines, performed in several work packages by 24 institutions. The aim of the project is to develop integrated approaches for security, virtual identity management, and privacy enhancing technologies at application level, system level and infrastructure level. The proposed best practice guidelines endeavour to provide managers and developers with tools to aid navigation through these many and often tricky issues that identity management technology and systems engender. They bring together a wide range of materials and techniques that are required to reach good decisions on interoperable identity.

2.1 What is best practice?

Best practice is a technique or method that, through experience and research:

- Proves reliable to lead to a desired result
- Produces superior performance in an institution
- Improves effectiveness, efficiency and innovation
- Is the best possible way of doing something

Information management is fundamental to all aspects of best practice. Information management refers to management of the systems, activities, and data that allow information in a project to be effectively acquired, stored, processed, accessed, communicated, and archived. There should be a valid audit trail of this communication process. Projects generate and absorb vast quantities of data that need to be managed effectively.

Although most projects and systems involve many disciplines, it is possible to study their effectiveness by breaking them down into discrete parts.

2.2 Aims of the deliverable

The aims of the deliverable are:

- Presentation and explanation of a generic method, and models for information and knowledge management that may be applied within the FIDIS project
- Application of the method and models to the exchange and integration of knowledge and information with the FIDIS network, and to the dissemination of the knowledge FIDIS has generated to the outside world

- Illustrate application of the method and models to identity management in different types of institutions
- Demonstrate application of the method and models to support interoperability
- Outline of how the method and models may be applied to the domain of e-health

2.3 Rationale

Whether an institution is performing research, developing a business operation, creating a product or delivering a service, significant attention must be paid to managing the necessary information. The research teams, analysts, operators and other personnel involved with the work must be able readily to apply and manage the information which is available to them. The relationships between academic institutions, business partners, suppliers and customers, and the information which is exchanged or shared between them must be managed effectively.

To manage information successfully institutions must specify the information requirements for all stages of the information lifecycle from creation, to installation, operation, maintenance and termination. Each situation and activity, which uses the information must be defined, understood, analysed and developed in an appropriate way. Comprehensive specifications need to be produced which define the requirements, functions, processes and information for the activities being addressed and the way that they will contribute to performance of the institution.

In the FIDIS project, to meet the challenge of bringing together the many different disciplines of identity management, which are illustrated as an entity diagram in Figure 1, there is a need for recommending best practice guidelines which incorporate effective governance and information management.

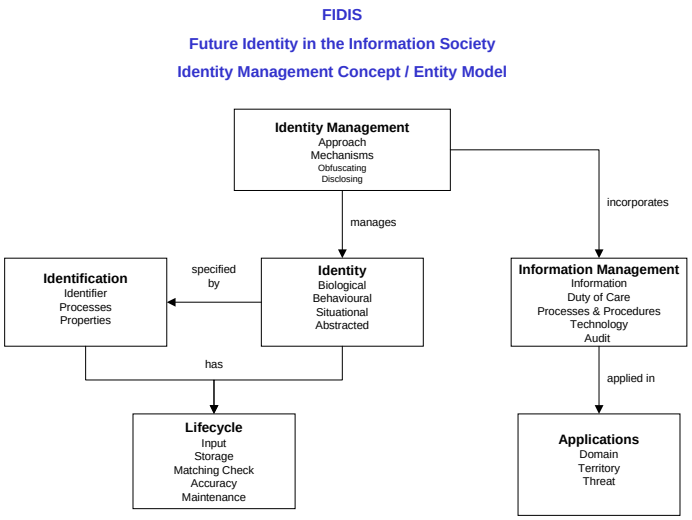

Figure 1

This report makes recommendations for best practice guidelines that may be widely used by FIDIS partner institutions, and external stakeholders, involved with multi-disciplinary activities of identity management. The emphasis of the report is on the delivery and application of a generic method, the Best Practice Method (BPM), that incorporates sound tools and techniques, which may be applied to perform a wide variety of activities, including interoperability.

3 An Information Management Method and Framework for FIDIS

The BPM concerns the analysis of identity management processes and, in particular, the analysis of information flows within and between the institutions, departments and personnel involved with identity management. A holistic and systemic approach is proposed that overcomes the issue of fragmentation and enables institutions to develop effective information management strategies relating to identity management.

The approach can be summarised as follows:

- An holistic approach covering financial, technical, commercial and social requirements
- A modular approach is adopted
- Analysis and application can be either “top-down” or bottom-up”
- It is generic and applicable to all business areas
- It provides a framework for gap analysis, knowledge transfer and dissemination
- It provides a set of models covering many business activities in the information lifecycle
- It offers consistency for disciplines and for enhancements

The method/framework can be applied to managing information for any type of project, business operation or service to ensure it will fit effectively into a given environment. The method is flexible and customisable and incorporates clearly defined events and procedures throughout the information lifecycle.

A method such as this must not just be used to manage information in isolation but must enable it to be integrated with existing information resources and business practices. This needs to be accomplished under the umbrella of comprehensive information management.

The approach requires continuous analysis in which there is close interaction with the personnel involved, to develop specifications, roles and responsibilities, possible risks, models of information flows, and compliance within and between stakeholders. The models should show where and how the use of information technology supports operations. The challenge is to identify ways of optimising and improving interoperability processes based on existing resources and on identifying how and where further improvements may be justified.

4 Best Practice Method

The LSE's researchers have developed and applied the Best Practice Method to assist institutions to build a framework of their operations and to design appropriate best practice procedures for improving performance[1],[2],[3]. It aims to bring clarity to areas that are complex and inter-linked. It has adapted the method to incorporate issues such as:

- Statutes and regulations
- Risk assessments
- Multiple disciplines within and between institutions
- Compliance monitoring
- Managing the sharing and exchanging of information
- Roles and responsibilities of personnel
- Integration of the activities of the institutions involved
- Developing best practice procedures

The method is separated into four domains, as shown in Figure 2, namely the requirements domain; the business modelling domain; the information management principles domain; and the system specification domain. In FIDIS these domains cover all aspects of identity management.

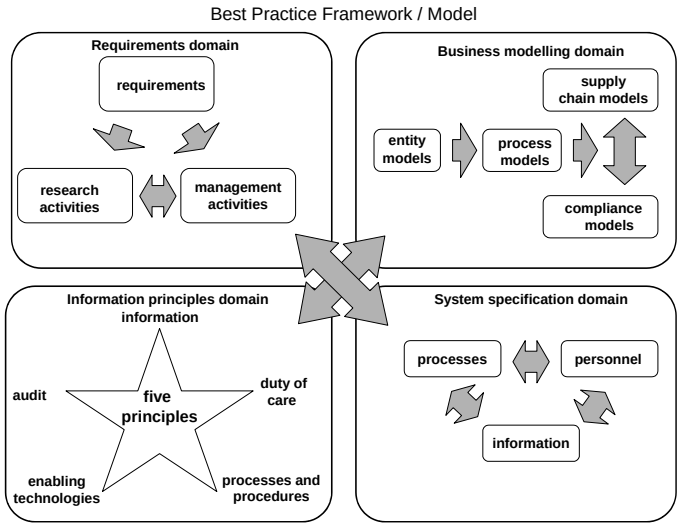

Figure 2

[1] BSI Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically
[2] England and Wales Flood Risk Assessment Guidance for New Developments
[3] Spotlight - New approaches to fighting money laundering

4.1 Requirements domain

A typical entity model of the requirements domain, for the FIDIS project, is shown in Figure 3. It should be a representation of identity management that will satisfy the requirements criteria for all aspects of the project, of which the information resource is a part. It will include a contextual description of the purpose of identity management within an institution. The requirements should specify what information is needed throughout the lifecycle of research and its application to the development, delivery and dissemination of FIDIS results. The requirements should specify where, when and how the information is to be delivered to all stakeholders.

The requirements are divided into two main areas, those specifying the research activities and those specifying the management activities.

4.1.1 Research activities

The model should be constructed after various analyses have been performed, by the Work Package leaders and decisions made on such topics as: the needs of stakeholders, institutional structures, existing processes, information needs, personnel resources, and possible standards to be adopted. The decisions should be based on envisaged service levels and performance criteria.

The specifications should include descriptions of the information resources, their origin and application. They should describe the validation and verification procedures employed to ensure the integrity, accuracy and timeliness of the information. There should be coverage of the legal issues to be addressed, the roles and responsibilities of personnel, the processes and procedures to be adopted, the technologies to be applied and the audit and control methods required. It is important that the requirements, having been defined, are formally agreed.

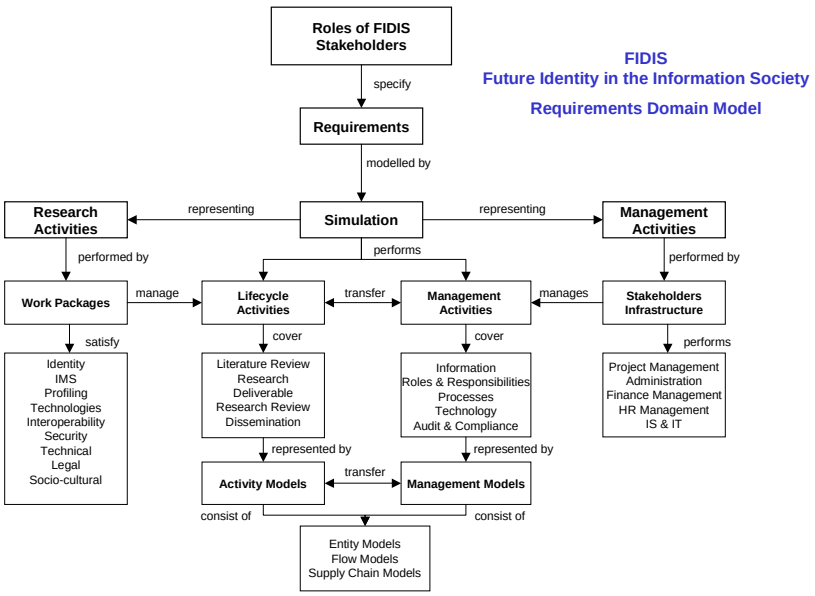

Figure 3

4.1.2 Management activities

The requirements for management activities should specify the management tools, techniques and procedures, which have to be employed to ensure that all the information, roles and responsibilities, processes and technologies are in place to manage identity activities.

Typical activities and the required actions to be performed are illustrated in Table 1.

Activities	Actions
Processes	What needs to be done
Procedures	How the procedures are performed and how the institution can establish they have been performed in accordance with requirements
Roles and Responsibilities	Who is carrying out the tasks
Techniques and tools	The means of assisting people perform their work

Table 1

4.2 Business Modelling Domain

Business modelling of the operations is an essential prerequisite before information management can be implemented. Institutions should be able to analyse and anticipate the effects of processes, information flows, document management and enabling technologies, such as e-business, upon their operations.

There are various modelling techniques, which may be applied, some of which are described below, to provide different and comprehensive views of the business activities.

Models should be developed to represent such items as:

- Activities and processes of the business application within and between, stakeholders
- Information resources and flows
- Application of technologies

Processes should be documented for such items as:

- Work procedures and tasks
- Roles and responsibilities of personnel
- Audit and monitoring procedures

4.2.1 Types of models

Business modelling takes many different forms and there are many techniques available. What is important is that fundamental processes should be modelled, and the way that this is done should maximise the generation of value for the institution. For example, analysis of information needs and resources should lead to the development of a corporate information model. In the FIDIS context the generation of value within research activity is important. To this end in later development of the guidelines we would expect to define the objectives, and how we measure them. For instance, the guidelines would have to support: the circulation of information within the Network, the identification and selection of relevant information for ongoing research purposes, the clarification of identity concepts, and certainly innovation itself.

4.2.1.1 Entity models

Entity models specify the relationships between such entities as people, objects, processes, and information within and between institutions. They are used to brainstorm, or when working from a fresh start, to specify and resolve business issues and to define the related corporate information. An entity model for information management within FIDIS is shown in Figure 4. It is a generic model, which may be applied by each Work Package.

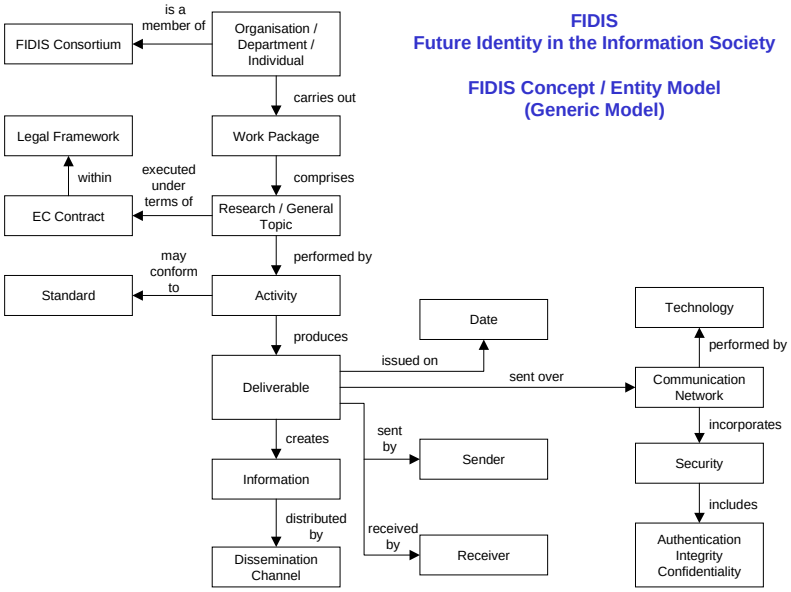

Figure 4

4.2.1.2 Stakeholder models

Stakeholder models highlight the different stakeholders who are involved in the various activities of identity management throughout the supply chain. Stakeholder models may be created for particular business sectors, such as e-health, and they may be used as a basis for information flows within and between stakeholders. In Figure 5, some of the stakeholders involved with identity management are shown at differing levels of governance:

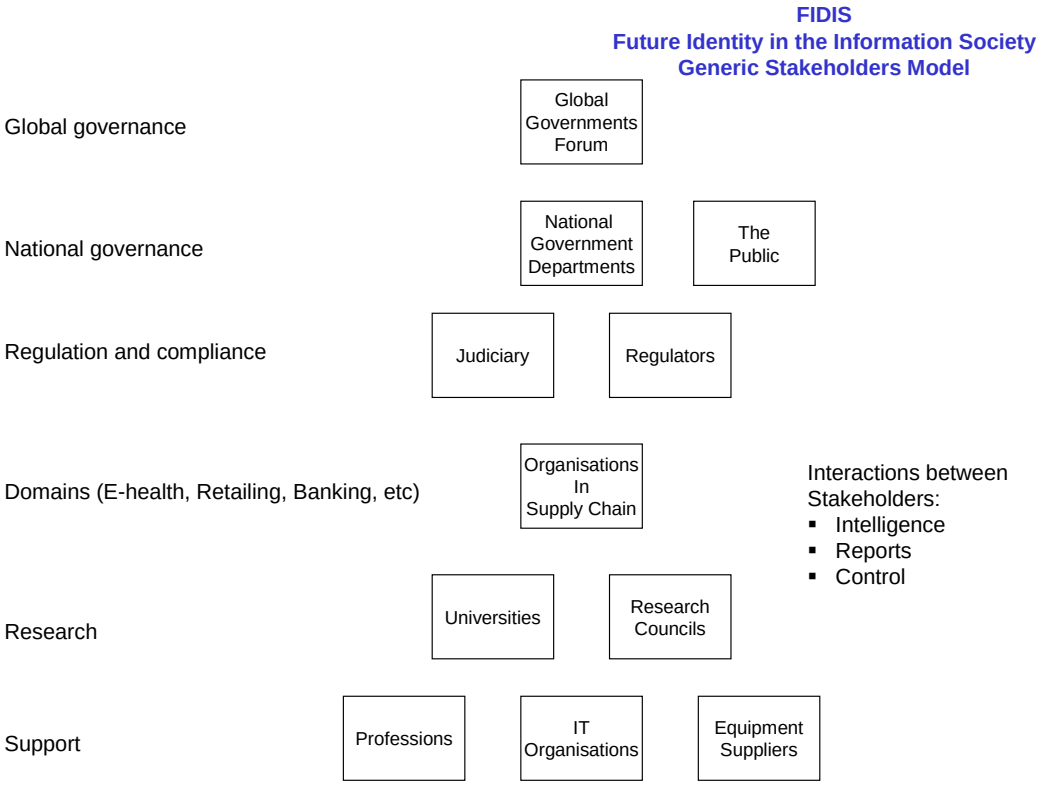

Figure 5

4.2.1.3 Process and information flow models

Information flow models show the business processes, how they interact with each other and how information flows between them. They provide a functional overview of the operations and allow personnel to see the functions and processes of a business quite independently of the organizational chart. They may show the essential and supportive processes and provide judgment about the value contributed by these processes to business operations. We can superimpose upon the models such flows as information, intelligence, documents, people and finance to indicate how we, as identity management systems developers or research network actors, drive and control the processes.

4.2.1.4 Compliance models

A generic compliance model has been developed in order to assess the degree to which institutions are fulfilling their obligations and their effectiveness in applying identity management. The model is shown in Figure 6 and the following statements briefly describe the areas of interest within the model.

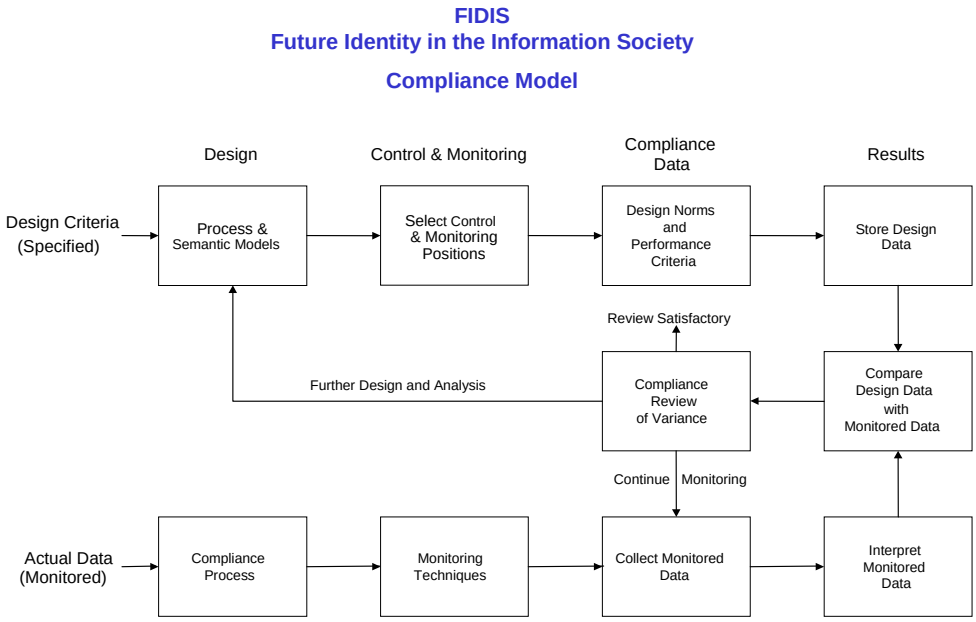

Figure 6

The model is divided into three parts:

The ***top line*** shows the processes for specifying the **Design Criteria** for ensuring compliance with the required regulations:

- **Process and Semantic Models**

The process and semantic models that satisfy legal and other requirements.

- **Select Control & Monitoring Positions**

The monitoring positions where relevant information needs to be collected for compliance purposes.

- **Design Norms & Performance Criteria**

The required norms and performance criteria, which need to be addressed for compliance with regulations.

- **Store Design Data**

The store containing all of the information that represents the design criteria.

The ***bottom line*** illustrates the processes for the **Actual Monitored Data.** This data needs to be collected and measured to enable compliance to be achieved:

- **Compliance Process**

The specification of the compliance process to be applied to activities.

- **Monitoring Techniques**

A description of the monitoring techniques being applied at the various audit points.

- **Collect Monitored Data**

A store containing all of the monitored data that is collected during the compliance process.

- **Interpret Monitored Data**

The analysis and interpretation of the monitored data.

The ***middle line*** represents the processes that compare and analyse the **Actual Monitored Data** with those of the **Design Criteria**:

- **Compare Designed Data with Monitored Data**

The process that compares the actual monitored data with the designed data

- **Compliance Review of Variance**

A compliance review to determine the variance between actual and design data. This gap analysis determines one of three outcomes: satisfactory review, monitoring to be continued or further design and analysis is required.

The audit points should be where particular activities of interest are taking place or where a transfer takes place of information from one person, department or institution to another. Information which needs to be gathered and checked against specified criteria, may include:

- Process being audited
- Information being processed
- Person responsible for performing the work
- The rules and norms which need to be satisfied
- Transmission and receipt logs

4.3 Information management principles domain

The five principles[4] discussed below underpin the work behind the modelling and are intended to serve as guidelines for those involved with the design and operation of information systems, irrespective of the technology being deployed.

[4] Mayon-White and Dyer (1997): Principles of Good Practice for Information Management, *British Standards Institution BSI PD0010*

The principles bring together the high-level internal policy issues and the detailed operational levels of any business. They are intended to provide a framework within which managers and others can develop detailed operational procedures. Alternatively they may be used as a template to check for the completeness or adequacy of an existing set of procedures and job descriptions.

The five principles take the form of a set of statements of objectives for information management. These are intended to act as guidelines for a set of procedures that any institution should be capable of devising and operating as an extension of their current standard operating procedures, or of their quality management processes. In other cases some of the recommended controls may already exist as part of a set of industry regulations.

Thus, instead of attempting to specify in detail what these procedures should be, it is understood that different industry sectors will have different requirements and may only need to use the principles as a checklist to test the completeness of their current regulations.

4.3.1 Five Principles of Information Management

The Five Principles are:

1 Recognise and understand all types of information

2 Understand the legal issues and execute "duty of care" responsibilities

3 Identify and specify business processes and procedures

4 Identify enabling technologies to support business processes and procedures

5 Monitor and audit business processes and procedures

The ordering of the principles also reflects a cascade from the high level classification of information streams to responsibilities, and then on to technology and operational considerations.

4.3.1.1 Information

To ensure that the institution:

- Recognises, understands and controls data and information through its classification, structure and the way it is represented
- Chooses appropriate methods to capture, store and transmit data within the institution and across its boundaries to, and from, its business partners
- Evaluates the information that it holds and takes appropriate measures to protect its information resources.
- Implements appropriate levels of security for managing its information.

4.3.1.2 Duty of Care

To ensure that the institution:

- Informs appropriate staff of pertinent legislation and regulations which apply to the way information and data is handled within their industry and business activities
- Executes its responsibilities under the duty of care principle.

4.3.1.3 Processes and procedures

To ensure that the institution:

- Identifies, documents and describes its processes and procedures.
- Monitors and controls changes to standard procedures using the documented descriptions of its operations.

4.3.1.4 Enabling technologies

To ensure that the institution:

- Identifies, assesses and applies appropriate technologies to support and enable its business processes and procedures
- Establishes procedures to monitor and control potential exposure to risks arising from the misuse or failure of its computer systems

4.3.1.5 Auditing

To ensure that the institution:

- Employs appropriate measures to monitor and document its operations and any deviations from its designated standards and methods of operation as established by its industry's regulatory bodies.

4.4 System Domain

Applying all of the above domains and their components helps to create the specification and requirements of an application system, either manual or electronic, in terms of **processes, information** and **personnel.**

4.5 Mapping the information

The information may be mapped onto the models as well as onto a matrix. Table 2 shows a typical matrix for developing an identity management system: one axis being the five principles of information management and the other axis being the stages of development of the identity information system. In the present document, development refers concretely to the development of the information system for supporting our research reflecting on the concept of Identity, and arguably to identity management systems

developers in general. The approach, given its status as a method for systems development, addresses the tasks of developers rather than those of end users.

	Information	**Duty of Care**	**Processes and Procedures**	**Enabling Technologies**	**Monitor And Control**
Requirements	Data Input & output Interoperability activities	Directors & Operators Legal Audit IT	Internal External	System Spec Networks Communications	Internal External
Analysis and Design	System model Simulation Tests Benchmarks	Designers Analysts Focus Groups	Input processes Operational processes Output processes	Alternative solutions	Audit Points Audit Specs
System Build	System Specs Input Output	Project management team	Relationships with stakeholders	Installation Testing Acceptance	Audit Points Audit Specs
Operations	Performance Capacity	Operators Managers Users	Day to Day Operations Availability Performance Maintenance	Hardware Operating System Software Communications	Frequency and nature of audits
Maintenance	Decision analysis Continue Enhance Replace	Directors Senior management Operators Users	Maintenance processes	System Transfers Backups Contingencies	Maintenance audit

Table 2

5 Application of the method

This section outlines how the Best Practice Method may be applied to interoperability within the e-health sector. Deliverable D4.9 "An application of the management method to an interoperability case study" will apply the method in detail to determine recommendations for best practice, relating to identity management, within the e-health sector.

5.1 Interoperability

Institutions function by means of human and automated systems communicating with each other, but always by means of sharing or exchanging information. Internal communication takes place between information systems and people within the same institution. External communication takes place between institutions and their business partners. Increasingly, external communications will be critical in assuring the future success of FIDIS. The right technologies, including the communication network, need to be put in place and the strategic advantages need to be specified, of sharing or exchanging information across whole supply chains, in order to reduce inventory and to accelerate the movement and availability of demand information relating to identity.

Interoperability in e-business may be defined as the communication, using standards, between several information technology systems held by various institutions or institutions.

The important benefits of interoperability include: increased cost-efficiency for the data exchanges, reduction of costs and more efficient retrieval of the needed data. An entity model for interoperability of systems between stakeholders, is illustrated in Figure 7.

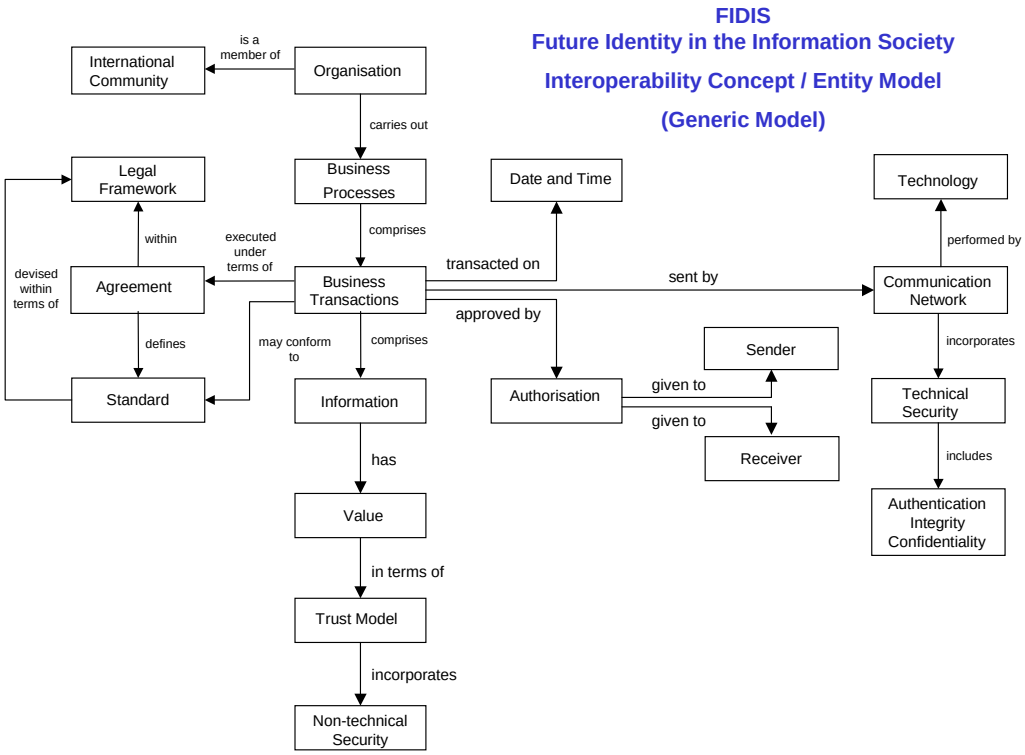

Figure 7

The model shows the particular areas of interest concerning interoperability and their relationships with one another. The reader should bear in mind that the model is not a flow diagram; it is in the form of an entity-relation diagram or concept model and represents the structure of interoperability activities.

The model breaks down the overall scope of interoperability into its essential components and associates each with related components. Experience in using similar concept models has shown that it is a good basis for organising and controlling operations. It also provides a means for an institution to monitor and control changes in its operations. It thus provides a focus for specifying technical and business activities with regard to standards, sources of network services and contractual requirements.

The following sections briefly describe the areas of interest within the model. The first paragraph explains the meaning of the terms used; the remaining paragraphs make comments about the elements of the model.

- **International Community**

The sector of government, business or industry, such as e-health, which is being addressed for the subject of interoperability.

Several industries have set up user groups so that experience and development of interoperability and related technologies can be shared between the members of the groups. This avoids duplication of effort and divergence of interests.

- **Institution**

The institution that is concerned with interoperability.

Currently many institutions are only involved with interoperability for a small part of their activities. The full potential of e-commerce and the benefits of interoperability will only be realised when the institution is using these techniques throughout the institution as a whole and with its trading partners. The institution's strategies for its business applications, electronic commerce, information technologies and information systems should include interoperability.

- **Legal Framework and Agreement**

The relevant laws and regulations governing operations.

These may include laws covering legal practices, contract agreements, taxes, financial exchanges, customs and excise conditions within and between countries, and the obligations of personnel dealing with the transfer of information. Personnel need to be aware of the legal implications and should ensure that appropriate procedures are followed.

- **Standard**

The defined standard being used for performing interoperability activities.

The importance of standards is being highlighted more and more by the application of Internet, Intranet and Extranet technologies. The subsequent effect of these technologies has meant that information, that has been originated, for example, in Microsoft Office may be published internally on a corporate intranet, viewed externally by business partners on an extranet, or published on an external web server to be viewed by the general public.

The role of the standardisation authorities in their unification is extremely important and should be closely monitored. Interoperability may be achieved by using more than one data standard since the adoption of a single standard may not be always possible.

- **Business Processes**

A business process furthers the work of an institution. In this model, it is the highest level view of what is done within a business. A business process may or may not be supported by interoperability.

Potentially all business processes performed by the institution should be reviewed and studied to determine if benefits are to be gained by applying interoperability techniques. The concept of "business process" is fundamentally important to the proper analysis of interoperability in business. Increasingly, identity management systems are becoming critical to the proper functioning of many business processes.

- **Business Transactions**

One or more activities make up the detail of business processes within institutions and between institutions.

Where institutions are working with each other an agreement should be reached between the parties concerned on the activities being carried out by interoperability, before transactions are performed.

The business transaction will involve either transmitting or receiving documents, images or other forms of communication such as voice mail or video conferencing sessions. These various kinds of messages may include text, numeric, graphic, voice or video files or any combination of them. Therefore an institution needs to be able to handle (i.e. receive and transmit) a range of message types, and to have procedures and relevant standards agreed with its trading or interacting partners, which apply for each of these.

- **Value**

The value of the data or information being processed or transacted.

Value is a key issue for developing the risk management and security aspects of interoperability.

- **Trust Model**

The mutual trust between two or more institutions

In today's world, institutions must be nimble and fast. The electronic foundation must permit people and computers to transparently, and quickly search, locate, and access

information to make effective business decisions quickly. This, therefore, requires a high level of trust and reliability.

Institutions should not only have trust in their own systems. Electronic messaging is an important tool for inter-institution communication, and allows institutions increased accessibility to each other's information. For business partners, there must be trust in each other's messaging systems too. For trust to develop in an institution's electronic messaging system, security is a minimal requirement. This mutual trust can be achieved through a guarantee that the institution's systems meet a recognised security standard that addresses their security threats.

It is important to distinguish between:

Trust – the relationship between social actors and entities or systems
Trustworthiness – an attribute of an entity or system

- **Sender / Publisher**

The sender/publisher of the information, document, image or other form of communication.

The sender/publisher may be an institution, a part of an institution such as a business unit, a department, or an individual. The notion of "sender/publisher" introduces the question of authority to send messages and the legality of doing so.

- **Receiver/Accessor**

The receiver/accessor of the information document, image or other form of communication.

It is important that the receipt of the information, document, image or other form of communication is recorded by the recipient. It may be preferable to send an acknowledgement message back to the sender/publisher. Once the message is received it should be understood and the necessary action taken.

- **Authorisation**

The authorisation of the transaction

Institutions need to establish a chain of accountability and assign responsibility for activities involving interoperability at all levels. This will establish a pattern of supervision and control.

- **Date**

The date and time when a transaction is carried out.

Procedures for demonstrating the integrity and authenticity of a time stamp and its binding to a particular piece of information should be documented.

- **Technology**

The enabling technology which performed the transaction.

- **Communication Network**

The network is the communication's medium used for transmitting and receiving messages.

A network may be an internal one, set up and managed by an institution for its own use, or it may be one operated by an institution whose business is to provide a communication facility specifically for the transmission of information, documents, images and standardised electronic messages.

- **Security**

The technical and non-technical security of the system

In this world of increasing interconnectivity and reliance, security is critical to ensure institutions can trust their own systems, and that of their business partners, to deal with security threats and ensure the continuation of business. Through a programme of trustworthiness development, evaluation and certification to a recognised standard, an institution can guarantee their electronic message handling systems to a demonstrable level of security.

A secure technical infrastructure is only one of the elements required for securing electronic commerce. Institutions must also consider the non-technical security of their systems, defined by policies, which may include cultural aspects, perceptions, and the roles, responsibilities and behaviour of personnel. Institutions are however always driven to balance security risks against commercial costs.

- **Authentication, Integrity and Confidentiality**

Authentication – the assurance to one entity that another entity is who he/she/it claims to be.
Integrity – the assurance to an entity that data has not been altered between transmission.
Confidentiality – the assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended.

5.2 E-health sector

When applying the method within the e-health sector it is recommended that best practice processes be developed for two areas of interest:

5.2.1 Managing the stakeholder model

A recommendation is that the stakeholder model is managed and maintained by a government department or a dedicated body, representing the sector being managed. It is acknowledged that this is an enormous and difficult task, which may take a very long time to achieve. However, making identity management "completely effective" may require this approach. There are many issues to take into account, such as security, privacy, data protection, inter-relationships and interoperability between the many institutions that need to be involved. It is envisaged that the FIDIS Best Practice Method will assist in this task.

5.2.2 Best practice within individual institutions

Within different institutions best practice processes will be similar. Such institutions include hospitals, medical councils and health authorities. These are broadly shown within the stakeholder model in Figure 8.

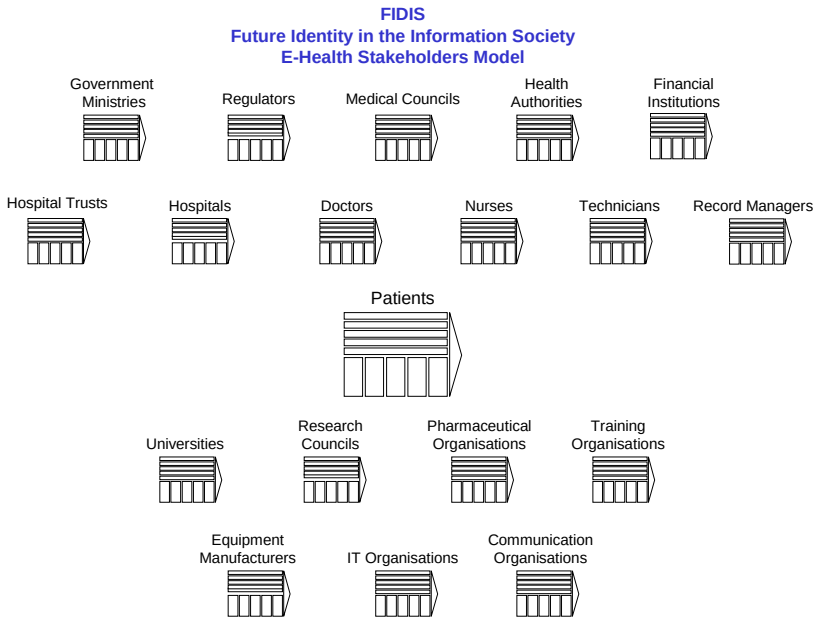

Figure 8

The actions which need to be addressed, when managing the stakeholder model, and by the individual institutions are listed below.

5.2.2.1 Requirements Domain

Identity management activities:

- Develop a stakeholder model
- Specify interoperability activities, which should include:
  - *What* information is required
  - *Where* the information is to be delivered
  - *When* is the information to be delivered
  - Information resources, their origin and interoperability uses
  - Legal issues to be addressed
  - Roles and responsibilities of personnel
  - Incentives
  - Processes and procedures to be adopted
  - Technologies to be applied
  - Audit and control methods required
  - Quality levels to be adopted
  - Standards to be applied
  - Change management

Management activities:

- Develop a strategy for managing and maintaining interoperability activities
- Specify risk assessments to be performed
- Decisions to be made on such topics as:
  - Security
  - Processes for performing analyses
  - Processes for delivering information
  - Management tools, techniques and procedures to be employed
- Specify information, roles and responsibilities, processes and technologies to manage the resources

5.2.2.2 Business modelling domain

- Develop models, similar to that shown in Figure 9, to represent the interoperability processes:
  - Activities within and between institutions
  - Application of technologies
  - Information resources and flows
  - Trigger events and their impact on interoperability
- Document interoperability processes including:
  - Work procedures and tasks

- Roles and responsibilities of personnel
- Audit and control points

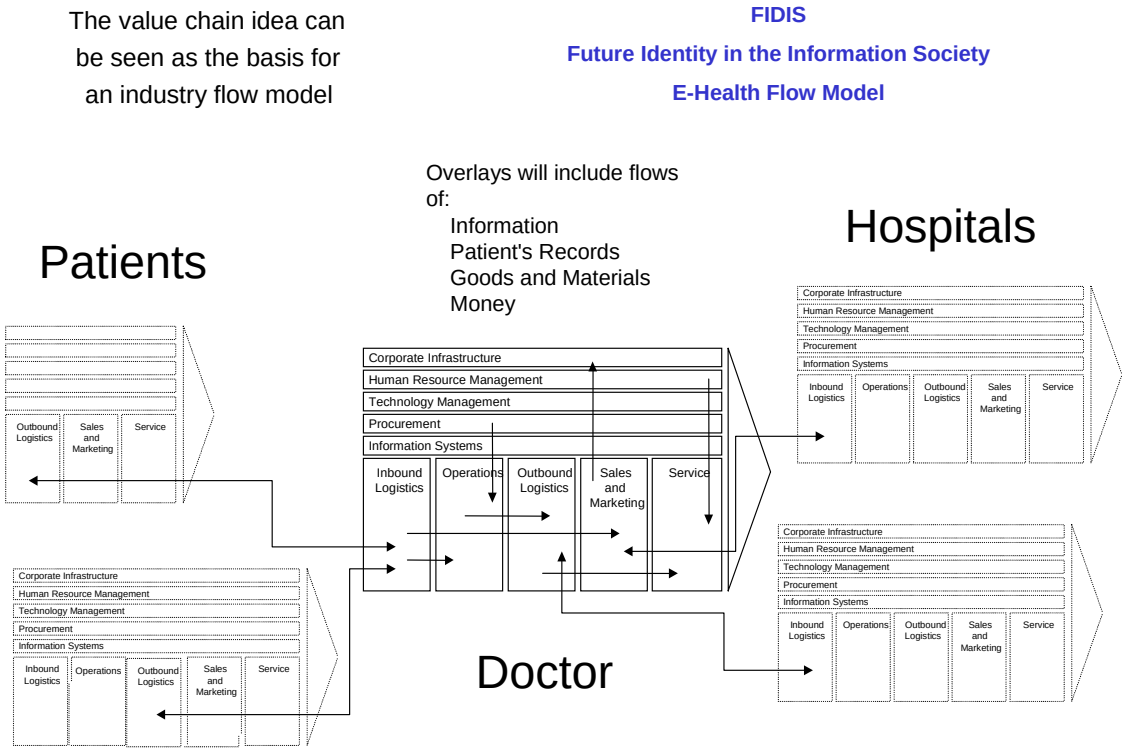

Figure 9

5.2.2.3 Information management principles domain

Information:

- Information to be collected, analysed, distributed, stored and maintained includes:
  - Identity parameters
  - Personal details
  - Laws
  - Regulations
  - Intelligence reports
  - Behaviour profiles

Duty of Care:

- All personnel should be aware of their legal obligations
- Procedures should be documented to assist staff in their work
- Perform training for staff
- Understand laws and regulations

- Specify liaison between stakeholders
- Specify the roles and responsibilities of staff

Processes and procedures:

- Specify and document all interoperability processes and procedures including:
  - Introducing the changes (evangelisation, training, overcoming the resistances, etc.)
  - Creating and monitoring rules and regulations
  - Identity procedures
  - Investigation procedures
  - Recovery and correction procedures

Enabling technologies:

- Identify, assess and apply appropriate technologies to support and enable interoperability processes and procedures
- Establishes procedures to monitor and control potential exposure to risks arising from the misuse or failure of its computer systems
- Develop electronic versions of policies, processes, procedures and reference material on the institution's computer network to allow access by relevant staff, at the appropriate level of security.

Audit:

- The positioning of audit points should be specified and agreed
- The audit methods at each audit point should be documented
- The nature and frequency of audit to ensure compliance should be documented

5.2.2.4 System Domain

All of the above domains and their components should assist with creating the specification and requirements for any specified computer or manual identity management system in terms of **processes, information** and **personnel** requirements.

5.2.3 Mapping best practice procedures

The information may be mapped onto the models as well as onto a matrix. Table 3 shows a typical matrix for developing best practice within the e-health sector as discussed above; one axis being the five principles of information management and the other axis being the stakeholders.

Stakeholder	Principles of Information Management				
	Information	**Roles & Responsibilities**	**Processes & Procedures**	**Enabling Technologies**	**Audit**
Government Ministries	Laws and statutes	Creating & upholding laws	Legislation	Identity Management Security Websites Information systems Databases Interoperability End-to-end processing etc	Monitoring laws
Regulators	Regulations	Enforcing regulations	Creating & monitoring regulations		Ensuring stakeholders comply with regulations
Medical Councils	Lists of medical professionals	Managing professional institutions	Ensuring professional conduct and practice		Ensuring professional conduct & practice
Health Authorities	All aspects of e-health	Ensuring health care	Ensuring finance and health care		Monitoring & ensuring health care
Financial Institutions	Funding	Supplying & monitoring funds	Provision of funds		Monitoring of funds & ensuring budgets are kept
Hospital Trusts	Institutional structures	Supplying & monitoring health care	Ensuring finance and health care		Monitoring of funds & ensuring budgets are kept
Hospitals	All aspects of care	Providing health care	Ensuring finance and health care		Monitoring & ensuring care is kept to standards
Doctors	Qualifications and identity	Ensuring identity of patients is secure	Ensuring health care is given to right patient		Patients' care
Nurses	Qualifications and identity	Ensuring identity of patients is secure	Ensuring health care is given to right patient		Patients' care
Technicians	Medical equipment	Installation and maintenance	Operators' guides and manuals		Equipment is performing well
Record Managers	Patient records	Secure identity & keeping records up to date	Records management		Secure identity & keeping records up to date
Patients	Identity & medical history	Protecting identity & keeping laws	Keeping health records up to date		Patients behave within law

Table 3

6 Conclusion and future work

This deliverable should only be considered as the start of a continuous process for developing best practice guidelines. It concerns the recommendations for best practice guidelines and the need for an effective development method and framework, which can be widely used for managing all aspects of identity resulting from the FIDIS research. The emphasis is on the delivery of a practical approach, which incorporates sound tools and techniques, which can be applied in the project and other settings. It is hoped that the deliverable will stimulate participation of the FIDIS partner institutions in developing the guidelines and the adoption of the proposed method and framework. Emphasis will be on the ease of use, robustness of the method and the ability of partners to apply the method, in developing their research.

The method will be enhanced to create integration and interoperation, as far as possible, all the FIDIS research findings, such as those in taxonomy, anonymity and pseudonymity, technologies, ID-theft, privacy and security; forensics, profiling, and to support the collaboration between stakeholders in identity management. The activities will include modelling the interoperability between stakeholders and identifying the information, business processes, roles and responsibilities, technologies and audit/compliance issues.

6.1 3rd Work Plan

The next deliverable, D4.7: "Review and classification for a FIDIS management model", will focus on developing a classification system, which can be applied by the best practice method and framework. It will be based on the information specified in delivery "D2.1: Inventory of topics and clusters","D2.3: Models" and other related documents.

To ensure that the method is generic it will be studied for its application in e-government, e-health, e-commerce, or similar context, demonstrating how interoperability may be applied in that context. The findings will be documented in D4.8: "Creating the method to incorporate FIDIS research for generic application".

Deliverable D4.9: "An application of the management method to an interoperability case study" will apply the method in detail to determine recommendations for best practice, relating to identity management, within the e-health sector.

6.2 4th Work Plan

If the FIDIS deliverables are to be exploited successfully then potential users must strive to understand how the natural balance of interest best lies between all those involved. The aim must be to discuss and understand the issues related to awareness, evaluation, implementation and application, as well as, the different perceptions of cost and benefit.

This understanding applies to the institution and amongst the stakeholders so that any differences are both recognised and managed. Successful relationships between stakeholders need to be established so that they all benefit from the service. Collaboration agreements, covering such topics as obligations, IPR, liability, quality, delivery times, access and finance need be established in order to reach successful business relationships. The dissemination and exploitation should be continually monitored and the performance of them measured against defined criteria to ensure that the expected benefits have been achieved.

To enable the practical adoption of the management method, we are proposing for development in a further deliverable, a FIDIS portal, rooted in the constructs illustrated in Figure 10, established to assist with the dissemination and exploitation of the FIDIS results. It is envisaged that the final best practice guidelines will be established after the delivery of D4.10 "Specification of a portal for interoperability of identity management systems".

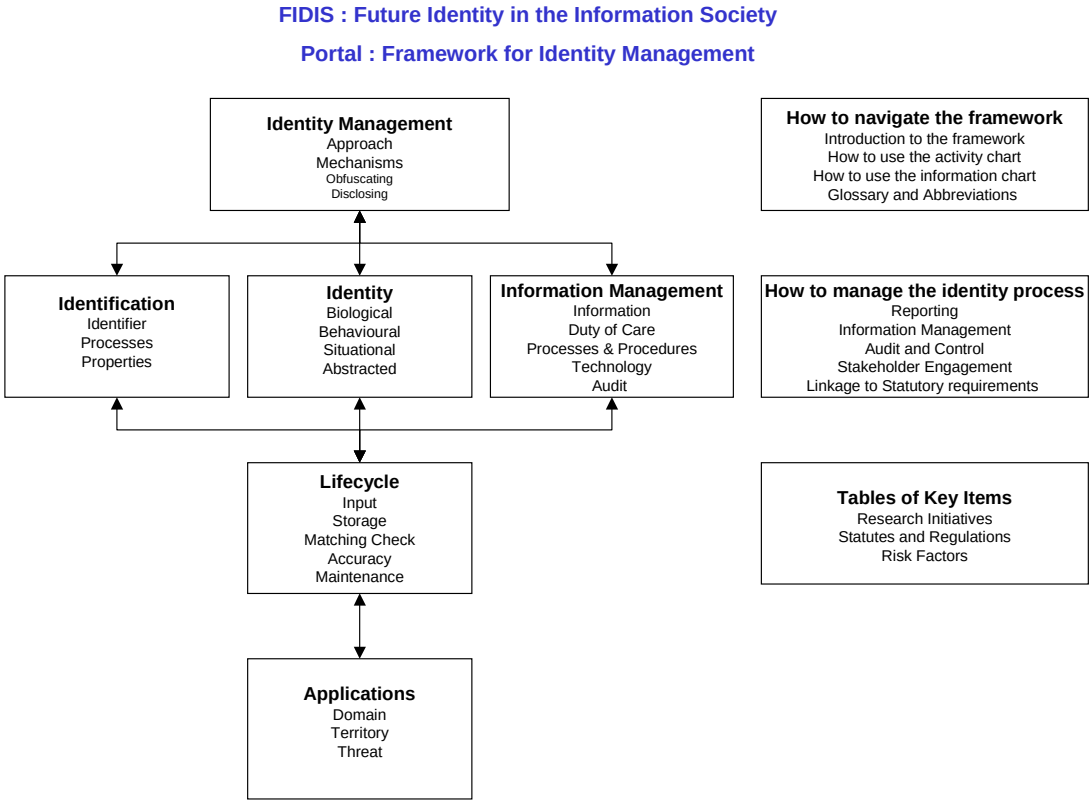

Figure 10