GOVERNANCE MODELS FOR SHARING AND RE-USE

For Common IT Solutions

This report / paper was prepared for the ISA programme by:

TRASYS SA[1]
in the scope of the specific contract 007743 of framework contract DI/6772 in between STRATIQO and DIGIT
Author: Clémentine VALAYER.

Disclaimer
The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.
The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof. Reference herein to any specific products, specifications, processes, or services by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute nor imply its endorsement, recommendation, or favouring by the European Commission.

---

[1] TRASYS is a member of the STRATIQO consortium

Contents

1. INTRODUCTION

1.1. Context and approach

1.1.1. Context

This deliverable "Governance models for Sharing and Re-use" is produced in the scope of ISA Action 4.2.5. "Sharing and re-use Strategy".

The aim of this ISA action - Sharing and Re-use Strategy - is to develop a holistic approach to sharing and re-use across border and sectors. It aims to help public administrations all over Europe to share and re-use solutions related to public services delivery in an efficient and effective way. A common strategy is to be defined together with the governance, the processes and the instruments. This will optimise the potential of sharing and re-use activities and it will increase the savings that they can bring to public administrations. Task 2.3 of the ISA action aims at identifying agreements and governing model guidelines. This deliverable D2.4 addresses the governing models, whereas a separate document, deliverable D2.3, addresses Sharing and re-use templates and guidelines for agreements.

1.1.2. Approach

The study is based on desk search and on feedback collected from stakeholders of this ISA action.

The desk search gathers some feedback from experience from the field, thanks to:
- identification of sharing and re-use initiatives on various websites, such as news and case studies Joinup[2], the ePractice[3] website, eGovernment strategy websites of Member States and other news websites ,
- exchange of experience at conferences in Member States and at the European Commission,
- interviews of project leaders.

The stakeholders are:
- At Member State level: ISA Expert group
- At European Commission level: the Technical IT Committee, which includes the Information Resource Managers of the different Directorate Generals.

1.2. Aim and content of the document

Public services can be implemented faster and more efficiently by using already available solutions and common services and by learning from the experiences of other Member States. Using the same solutions and adapting others' best practices indirectly results in services that are more interoperable and more open. The sharing of assets can either refer to making assets available to others, or developing them as a common solution.

---

[2] http://joinup.ec.europa.eu/
[3] ePractice.eu

This document presents *real life cases* of sharing and re-use among public administrations, with their benefits and drawbacks. The cases' description focuses on the governing models for the common IT solutions.

For some cases, governance models are less developed, and the description focuses on the mechanisms for agreements put in place. The document shows a variety of types of collaboration, with formal or less formal governance models. It aims at gathering feedback from the field on how administrations collaborate.

These cases are also presented in a previous deliverable[4], with the description focusing on the business model. These models cover different forms of collaboration, and the **business models** of these cases are presented in a separate document[5].

The document presents in **section 2** examples of development of re-usable and/or shared tools and re-use of reusable tools. This section is titled "**Shared tools: development and re-use**". It presents examples of organisational or governance models in place to either develop a tool in order to share it, or to re-use an existing tool.

The document presents in **section 3** examples of use of and development of shared services. That section, titled "**shared services: use and development**" presents examples of governance models for shared IT services.

The document presents in **section 4** examples of "**shared developments**", with cases of governance models for collaboration for the development and maintenance of specific common solutions.

Section 5 presents the conclusions, whereas **section 6** lists all the references used for each case description.

The case descriptions follow a presentation template:

| [References]	Name of the case
Short description	
Main stakeholders	
Governance model / mechanisms for collaboration	
Benefits and drawbacks	

---

[4] ISA Action 4.2.5 - D2.2 Business models for sharing and re-use tailored to public administrations' needs
[5] Note: Some of the cases presented in D2.2 are not detailed regarding their governance model in this document, because the governance aspects of these cases are minor, or directly linked to the business model and described together to ease understanding of the model.

2. SHARED TOOLS: DEVELOPMENT AND RE-USE

This section presents governance models for cases illustrating re-use of shared tools. These cases are described in a previous deliverable, focusing on the business models.

2.1. CH: Financing of eGovernment priority projects: selection criteria includes re-use

[1]	CH eGovernment Strategy - Financial incentive for re-use
Short description	The Swiss e-government strategy includes re-use as selection criteria for financing priority projects. This section presents the organisational structure for implementing the eGovernment Strategy.
Main stakeholders	The Steering Committee of the eGovernment Action Plan. The public administrations in Switzerland, National and Cantonal.
Governance model	The eGovernment action plan in Switzerland lists the measures to be taken, in the short, medium and long-term measures for selected priority projects.
	The catalogue of priority projects is regularly evaluated by the Steering Committee and updated. The action plan is reviewed annually by the Steering Committee eGovernment Switzerland and updated. The steering Committee also decides on the allocation of the funds.
	The organisational structure for implementing the eGovernment Strategy is governed as follows (see figure below) by the Framework Agreement under Public Law on eGovernment Cooperation in Switzerland:
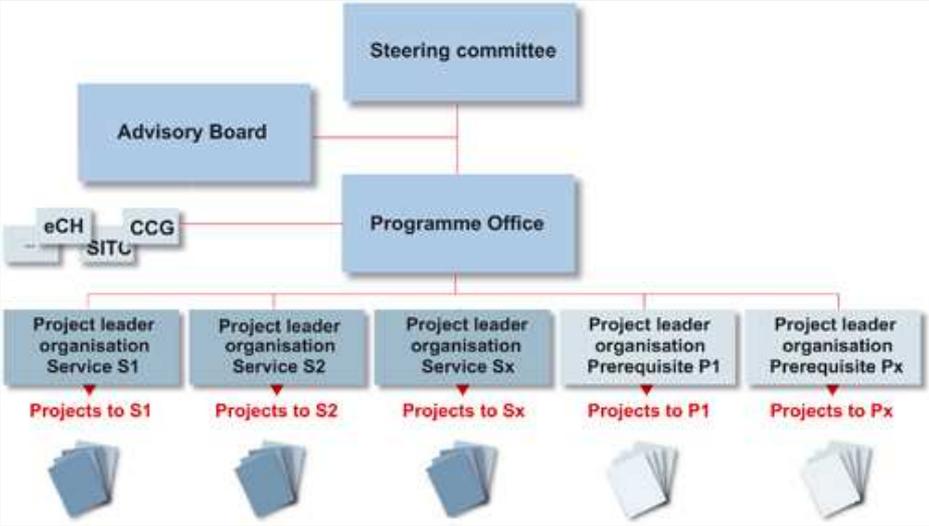
The **Steering Committee** has the following responsibilities and powers:

- It defines and updates the Catalogue of Priority Projects.
- It designates lead organisations for the implementation of priority projects and, where necessary, supports them in the drafting of special agreements.
- It takes note of the special agreements submitted to it by the lead organisations.
- It steers and monitors the implementation of the Strategy, decides on updated planning and implementation instruments, and periodically reviews the progress of implementation.
- It mediates disputes between the contracting parties.
- It briefs the Federal Council, the Conference of the Cantonal Governments (CCG), the Association of Cities, the Association of Municipalities, and other interested bodies on its decisions.
- It designates the members of the Advisory Board.

The **Advisory Board** is composed of a maximum of nine experts from administration, the private sector, and academia. It advises the Steering Committee, the Programme Office, and the organisations in charge of the implementation projects on legal, technical, and organisational issues. The Advisory Board has the following responsibilities:

- It reviews the technical aspects of the upcoming agenda items and projects, and it issues recommendations to the Steering Committee.
- It advises the Programme Office and the lead organisations on the implementation of priority projects with respect to legal (article 6), technical, and organisational questions.

As the administrative unit of the Steering Committee, an eGovernment Switzerland **Programme Office** contained within the Federal IT Steering Unit (FITSU) coordinates implementation of the strategy. The Programme Office has the following responsibilities:

- It prepares the agenda items of the Steering Committee and the Advisory Board and keeps minutes of the meetings. It monitors the implementation of the decisions of the Steering Committee.
- It is the contact point for lead organisations and is responsible for the development of a contact network with the cantons and the involved federal offices.
- It supports the lead organisations in their preparation of special agreements and supplies financing models and sample contracts.
- Through appropriate communication measures, it ensures the necessary transparency. In particular, it maintains and updates the implementation instruments on behalf of the Steering Committee and publishes them on the internet.
- It works together with the Conference of Government Chancellors and the Secretariat of the Swiss IT Conference as a communication and coordination hub for

the cantons and the municipalities.
- It ensures controlling of the implementation of the eGovernment Strategy.
- It observes the eGovernment activities in Switzerland and abroad, and it identifies duplications and potential synergies.
- It submits an annual report on the status of implementation to the Steering Committee.

Due to the diversity of the priority projects in the catalogue, sponsorship and financing are defined in accordance with the applicable demands and, where necessary, set out in a special agreement. For this purpose, the Steering Committee designates **lead organisations** for each priority project. The lead organisations:
- designate their project leaders;
- in cooperation with other participating stakeholders, they are responsible for the law-making concept (article 6 of the framework agreement) and a sustainable financing and organisational concept;
- they guarantee compliance with standards, monitor interoperability of the solutions developed, and regularly report to the Programme Office as part of a monitoring process on the status of work;
- via the Programme Office, they may approach the Advisory Board for technical support;
- via the Programme Office, they may submit applications to the Steering Committee for the financing of projects.

Benefits and drawbacks	The overall model, based on a Programme Management Office approach implementing the IT strategy and including a financial incentive for re-use, proves successful. It provides an overall view of eGovernment projects, and ensures the re-use of existing modules. The overall approach proves effective; however, the take-up by the different stakeholders is very slow.
	There is a need for high efforts in communication about the Programme Office, the eGovernment strategy and the incentives. Awareness raising is a very important element for the effectiveness of the model.

2.2.   BE: IMIO Re-use and pooling of IT

[6][7][8]	IMIO – Re-use and pooling of IT in local authorities
Short description	IMIO (Inter-commune Pooling of organisational IT) is an organisation promoting and coordinating the sharing of solutions and services for local authorities of the Walloon Region of Belgium. Implementing a common strategy at different levels of government, IMIO provides a collaboration platform and promotes a common approach to procurement. In order to do this, IMIO provides shared services and develops re-usable interoperable solutions: - through central purchasing - by developing in-house generic and adaptable solutions, created by pooling new developments under open source licenses.
Main stakeholders	In the Walloon Region of Belgium, 169 (end June 2013) local authorities (including 134 towns, 3 police zones and 2 provinces) buy IMIO services. IMIO is founded and funded partly by the Walloon Region. IMIO participates in the ICEG (Intergovernmental Committee for eGovernment), initiated by FedICT, which meets regularly to coordinate eGovernment initiatives at Federal and Local levels.
Governance model and collaboration mechanisms	In its statement of Regional Policy 2009-2014, the Walloon Government focused on the sharing of developments: "namely joint developments between entities, sharing of methodologies and tools and promote the use of free software that facilitates the sharing IT developments". Another policy aspect is the strategy of the Walloon Government also encouraging the pooling at local authority level, supporting sharing of resources and of practices (methodology, technical developments, needs analysis, training, support), and supporting initiatives to improve their performance and management. In alignment with these goals, IMIO procures solutions on behalf of its members. The strategic goal is to analyze organizational needs and IT needs of local authorities by a collaborative "bottom-up" approach. IMIO proposes frameworks (standards, notifications, interoperability, sources, standard procurement clauses for interoperability of IT solutions) and defines a common framework for interoperability. IMIO also identifies and formalises best practices, and disseminates them as organisational assets (tender specifications, simplified processes, IT strategies). IMIO is an inter-commune cooperative company with limited responsibilities, and was founded on the CommunesPlone project. It has been in operation since 1 January 2012 and is supported by the ten communes part of the CommunePlone and another similar initiative.

The governance structure is based on a management committee a Board and observers of the board. The observers of the board include the Associations of the Walloon Provinces and Towns, the Walloon ministry, and the agency in charge of the reduction of administrative burden.

The IMIO website presents a template document for communes wishing to become a member. This document formalising the decision of a commune to participate in IMIO includes the following articles:

- Article 1

The commune takes part in IMIO SCRL and becomes a member. This aims to promote and coordinate the sharing of organizational solutions, products and IT services for local authorities in Wallonia and more precisely:

1. To provide a consistent supply of IT tools shared and interoperable with Wallonia:

a. either through the centralised purchasing body which purchases quality IT business applications and at an price overall more beneficial to local authorities than if they had bought these applications individually;

b. either by developing in-house generic and configurable computer applications, created in pooling mode under an open source license.

In this context, the structure will manage a portfolio of consistent robust, government-owned and free software solutions. It will also ensure the in-house development of related technical skills, the evolution and sustainability of the solutions and their dissemination in accordance with the free license.

2. To provide organizational solutions tailored and optimized for local authorities (simplified processes, ...).

- Article 2.

The common takes X shares of the capital of IMIO, providing a contribution of EUR X (one unit = 3.71 euros).

This contribution will be released upon receipt of the approval […] by a payment of X euros on the bank account […].

Benefits, drawbacks	The official status of the organisational structure of IMIO as a public body makes their mandate recognised by the other public administrations, and joining very straightforward.
	There is not a very formal governance model for the management of IMIO. This strong governance is not needed, and management is based on experience of the working staff in the previous organisation (Communes Plone).
	The focus is on practical aspects of activities, such as a downloadable form for the communes to easily adhere. The advantage of this model is in its simplicity and focus on operational aspects.

2.3. SE: Procurement framework for re-using free solutions

[9][10][11]	Procurement framework for Open Source
Short description	A model for re-use of existing solutions, the 2010 Open Source Framework Agreement ('Öppna programvaror 2010') for the Swedish public sector is the only Framework Agreement for open source software in Europe.
Main stakeholders	The framework can be used by all parts of the central government, the public education sector, all twenty county councils and 225 out of the 290 Swedish municipalities. There are five suppliers with more than a hundred subcontractors. The subcontractors are experts contributing to the development of existing open source applications and active in open source communities.
Governance model and mechanisms	**Shared procurement** One task of the National Procurement Services (NPS) at Kammarkollegiet[6] is to supply coordinated framework agreements at National, Regional and Local level within the area of ICT & Telecom. The main objective for the NPS is to generate savings for the tax-payers but also to promote optimum conditions for the acquisition and use of ICT within the Public administration and to promote the use of common functions and solutions. In these efforts the interest in innovations and technology-neutral solutions should be taken into consideration as well as the possibilities for small and medium-sized enterprises to place tenders. The NPS never procures contracts for goods or services, instead only framework agreements are procured so that the different public bodies can create their own mini-competitions tailored to their needs. By law, the government cannot decide what a municipality or county council should do. So for each framework agreement procured by the NPS, each of the municipalities and county councils decides if they want the NPS to procure in their name. Governmental bodies are always part of the framework agreements. It's not strictly mandatory to use the framework agreements, but most public bodies favours using them instead of doing their own procurement. Before the procurement of a new framework agreement, the NPS does an extensive pre-study to gather information from the buyers, suppliers and analysts. This pre-study lasts usually 4 to 6 months. It includes: • meetings with current suppliers (if applicable) • meetings with other relevant suppliers • extensive review of the mini-competitions carried out under similar current frameworks to identify the buying

---

[6] http://www.kammarkollegiet.se/kammarkollegiet

---

	behaviours and administrations' needs • meetings or interviews with buyers who have shown great interest in the area, are fore-runners generally or are larger buyers • desk search of current market analysts' reports • sometimes a tailored market analysis is conducted NPS writes the report based on all the collected information, and makes it public on their web site. NPS then decides if there should be a new procurement, taking into account: • the results of the pre-study • the need for a healthy competition among many suppliers • commercially interesting terms for the suppliers • possibility to use the framework agreement up to 4 years **Framework contract and experts:** The primary suppliers could bring in as many subcontractors as they saw fit. This allowed for the experts in the open source communities to be part of the framework as subcontractors. Although every subcontractor must be connected to one or more primary suppliers at the time of the tender, suppliers can switch subcontractors later. Furthermore, suppliers have to be completely transparent about the subcontractors they will be using and what services these subcontractors will provide to the customer. **Financial mechanisms** The suppliers who have a framework agreement report their quarterly sales to NPS. NPS then charges them 0.7 % of that amount as a fee to finance the NPS. The NPS is not tax-funded, although Kammarkollegiet is an Agency.
Benefits, drawbacks	The model is efficient in addressing both the governance of the open source contributions to the community and the governance of a shared procurement. The governance of open source solutions is addressed by specific requests in the tender. Bidders may quote only open source software and show expertise in legal implications. Bidders need to demonstrate involvement in the open source community and active contributions to open source. The governance of the shared procurement, and its "pay back" mechanism builds on the efficiency of the framework contract; the association does not get funding if the framework contract is not used. This shows that the contracting authority takes into account both the needs of the users and the suppliers.

3. USE AND DEVELOPMENT OF SHARED SERVICES

3.1. EU: EC DIGIT e-PRIOR Shared Service

[12][13]	e-PRIOR
Short description	The e-PRIOR platform allows the European bodies and their suppliers to exchange procurement documents in electronic format.
Main stakeholders	The project was started in 2007 by the European Commission - Directorate-Generals for Internal Market (DG MARKT) and for Informatics (DIGIT). Target users: • European Commission DGs, EU Agencies and Institutions, • suppliers, receiving e-Orders and sending e-Invoices (this includes SMEs, who can use the Supplier Portal). All forty Directorate-Generals of the European Commission and nearly all its six Executive Agencies are using ePrior as a shared service with EC DIGIT suppliers for IT goods and services.
Collaboration mechanisms	All EU agencies can have access to the DIGIT ePrior shared service. There is no formal governance model, but governance is addressed through a formal agreement, the Memorandum of Understanding (MoU). Decisions regarding the solution (functionality…) are discussed through an ePrior user group, but specific requests are addressed through the MoU. A very detailed explanation of roles and responsibilities is described in the (MoU) signed with DIGIT by the Agency. The case describes below this MoU (and its supporting documents) and the different roles in detail, as an example of operational collaboration providing governance mechanisms. The purpose of this MoU is the supply by DIGIT of e-PRIOR and its configuration following the agency request. • The roles of the **e-PRIOR** team members –Production manager: responsible for the technical operation and availability of the e-PRIOR modules in collaboration with the data centre. –User service manager: responsible for liaison with users, the parameterisation of the Customers (DG, agency …) and the Suppliers, and for informing them of changes to the system and of system unavailability. –Security manager: Requests to give access rights to new users (Suppliers and Customers) or modify existing ones should be addressed to the Security Manager. –Training and documentation manager: responsible of the training courses and the creation/update of the user documentation. –The courses are organised on demand. –Help desk: handles questions and issues on the e-PRIOR platform, the end-user applications such as the Supplier Portal and the interfaces to local systems (back-offices …). –Business area manager: responsible for organising the

development, improvement and maintenance of the modules which are part of the e-PRIOR Suite.
−Project correspondent: responsible for contacts with external parties. He is the internal representative of the users.
−Financial correspondent: responsible for all financial matters.
−MoU correspondent: responsible for all contractual matters.

- The roles of the **agency** team for e-PRIOR

−The Agency Correspondent is responsible for internal communication related to e-PRIOR on the Customer or Supplier side, both upstream from users to DIGIT in respect of their needs and downstream from DIGIT to users in respect of the overall functioning of and changes brought to the e-PRIOR platform & applications/modules. The Correspondent is the first contact point for functional and operational questions from the users. He is invited to the bi-annual e-PRIOR user group meetings where released and planned changes to the system are presented and discussed. The Correspondent also follows up the implementation of the MoU on behalf of the Supplier or the Customer. This role can be executed by one person or can be shared by two persons (1 IT expert & 1 functional expert for example).
−Project manager: responsible for the technical implementation of e-PRIOR Suite at the agency. If developments are needed on the agency side, this person will liaise with the e-PRIOR business area manager for any technical matter.
−Financial correspondent: contact person for all the financial matters related to the e-PRIOR usage.
−MoU Correspondent: the interface for any contractual matters with the e-PRIOR MoU Correspondent.
−Agency security officer: if access rights to use one of the e-PRIOR modules are needed and if these access rights have to be given by the e-PRIOR Security Manager, the agency security officer requests these access rights.

- The services covered by the fees:
−Coordination and planning meetings, set up of the agreement
−Writing of supporting documentation and their updates
−Put in place the technical environment for e-PRIOR at the agency
−Support to the development/enhancements of interfaces, unit-testing
−Testing the set-up in test, acceptance and production environments
−Follow-up of the production environment (messages, errors, availability, database back-ups ...)
−Security set-up (creation of users & profiles for the used modules)
−Configuring/customizing workflows (actors, steps, rules)
−Opening the interface from/to supplier and/or customer systems
−Support for the access to the infrastructure (network and servers)
−Support for the incidents related to the modules used
−Problem management support
−Bug corrections via change management
−Small evolutionary maintenance
−Installation and running-in small evolutionary changes

–Coordination & communication tasks
–e-PRIOR user group meeting organisation
–Coordination of user tests and release management
–Provision and support of "standard" reports via a dedicated e-PRIOR reporting environment.
–Security Management (add users/access rights) for the modules and the reporting environment
–Maintenance of technical environments e-PRIOR (in relation with DIGIT Data Centre): application servers, databases, etc. – Installation of new releases of the application servers and databases, back-ups etc.
–Hosting of the infrastructure for running e-PRIOR (secured network, application servers, relational databases, single sign-on, e-mail notification servers, reporting environments …)
–Technical and functional upgrades as a result of new releases of the e-PRIOR platform and modules
–Interface maintenance (from and to: ABAC WORKFLOW, ABAC INVOICE, ABAC ASSETS, Local back-offices …)

- The support is specific to either business or IT related issues.

–All business questions are handled by the agency (for example via the agency Local Help Desk).
–For IT technical questions, users create incidents in the dedicated support tools[7], specific to the customer portal, the supplier portal or the web service interface.

- Special reporting requests

–The agency can request special reporting functionality. DIGIT analyses the request for its feasibility, further defines its content and designs the report. These high level specifications and designs are proposed to the agency for approval; an estimation of the workload is then presented and once the offer is accepted and paid, the development starts.
–DIGIT retains the right to share the report(s) with others.

- Specific development request

–The agency can request specific developments. Business specifications and their feasibility are then analysed, use cases developed. The process is then similar to the special reporting request described above.
–Any specific development will be integrated in the core version of e-PRIOR and therefore will follow the general release cycle in case of modifications or updates.
– DIGIT retains the right to share the specific development with others.

With regards responsibility, there is no service level agreed on. This is related to the fact that DIGIT does not have any SLA with the Infrastructure services of DIGIT for this specific e-Prior service.

[7] SMT: Support Management Tool of the Commission

Benefits and drawbacks	The mechanisms used for this shared service are based on a practical and operational approach; the use of a Memorandum of Understanding, clearly defining in detail the roles and responsibilities of each party, is the main instrument for governing coloration in this project. The advantage of this model is in its simplicity. The reason for such an approach is that the service was designed for the use of one Directorate General, but it was extended to the use by others without a formal structure; the collaboration aspects were then addressed and described in the MoU. Main changes are discussed in the ePrior user group meetings, and specific requests are provided for.

3.2.   EU: EC DIGIT Infrastructure services provision

[14][15][16] [17][18][19]	EC DIGIT Infrastructure services provision (ISP)
Short description	DIGIT, the Directorate General of IT of the European Commission, Directorate C (Infrastructure services provision) developed a cost model to charge back the provision of its IT services. The current 15 services (consisting of 33 different service elements) include: hosting of IS, Websites, business data processing applications, email, mobile telephony, call center, Wifi services. DIGIT also provides tailor-made services. The cost model follows an activity based costing approach.
Main stakeholders	Users of the services[8] provided by DIGIT are the Directorate Generals of the European Commission, 7 agencies as well as other EU institutions such as the Court of Justice.
Governance Model and Mechanisms	**Governance of the cost model[9] of DIGIT Directorate C - ISP** The cost model is endorsed by the ABM+IT Steering Committee (see below) each time there is a major change. General IT governance of the Commission: ICT is organised along federal lines (following the decentralised structure of the Commission). Each Directorate-General has a local IT organisation with an Informatics Resource Manager (IRM). A central IT function (Directorate General DIGIT) provides common (corporate) services and support. Three central bodies ensure coordination, planning, control standards, decision making, risk management, investment optimisation. They are: - the CPO - Commission Programme Office, hosted by DIGIT. Its duties concern the horizontal activities related to information systems (IS) coordination in the Commission, including the maintenance of the IS architecture framework, of the IS management and development methodology, of a system describing the existing portfolio of IS. - the CTI – (Comité Technique Informatique) for infrastructure follows up the major infrastructure projects and monitors the operational IT services supplied by DIGIT. The CTI-IS (Information Systems) assures the inter-service coordination for all matters related to IS, including the follow-up of the development of major information systems, the coordination of the information systems portfolio and the promotion of best practices. Participants are all DGs' IRMs. - the MAP (Methodology, Architecture, Portfolio) group is a

[8] In 2012, DIGIT C had 346 MoUs with 99 different customers
[9] See ISA Action 4.2.5 Deliverable D2.2 for a description of the cost model

subgroup of the CTI. It steers the Enterprise Architecture, project management and development methodology activities of DIGIT, reviews all project definitions or major updates on IS and assists DIGIT in the elaboration of the Commission's IS development strategy, review of the IT Master Plan and the proposal for allocation of budget.

In 2012, a new set of governance bodies was put in place[10] to ensure that all IT developments match business priorities and that the existing portfolio of the applications is streamlined to ensure maximum efficiency gains. These are:

- The Activity based Management + IT Steering Committee (ABM+IT). The ABM Steering Group brings together Directors General and cabinets responsible for central services. It coordinates strategic questions related to horizontal instruments such as strategic planning and programming and internal control and regularly reviews the adequacy of the Commission's corporate processes. ABM+IT is an extension of the ABM Steering Committee to cover IT matters.
- The High Level Committee on IT (HLCIT) comprises director level representation from the DGs. It follows the work necessary to give effect to the recommendations published in SEC (2010)1182.
- The Information Systems Project Management Board (ISPMB) composed of 7DGs Resources Directors. Its mandate includes to examine of all new IT project proposals over €500,000, advise on corporate and other solutions for DGs business needs, provide information to the ABM+IT steering committee on difficulties encountered with IT projects.

A specific working group focuses on diminishing the costs of the different local data centers and centralising them when appropriate.

Contractual aspects

The Memorandum of Understanding (MoU) is the contractual aspect linking DIGIT with its clients. The client signs a MoU with DIGIT for the use of an individual service. The MoU mentions that the signing parties may carry out an annual joint evaluation of the Project's performance. The amount paid by the client may be reviewed based on the costs actually incurred by DG DIGIT. (The amount is based on the previous year's expenditure.)

The Service Level Agreement (SLA) mentions that the primary mission of ISP is to guarantee the powerful ICT infrastructure essential for the optimum operation of the Institution. ISP follows

---

[10] Following the recommendations of the IT Task force and the Communication "Getting the best out of IT" (SEC (2010)1182).

best industry practices based on ITIL framework, by assuring all functions needed to guarantee the provision of these services in a cost-effective way (planning, budgeting and construction, management and operation, accounting and billing). It guarantees that the provision of these services is guided by Service Level Agreements (SLAs) established in accordance with the needs of the Commission services.

The SLA identifies what is to be delivered by the Service Provider, and what is the quality of the services provided, in terms of specific quality metrics and associated targets. The SLA also addresses Strategic Evolution. In terms of ensuring fine-tuning of the balance point between the service viability and customer satisfaction, the two parties may review and adapt the terms of the present SLA by common consent in the event of exceptional circumstances affecting the "normal" operations of services, such as:

- major changes in the operational environment (for instance: new and enhanced tools and applications, advanced services, application of new technologies and design principles),
- major new service functionalities not previously envisaged,
- major changes on the End-User's population (number and behaviour).

The SLA addresses Infrastructure Change Management, as defined in the ITIL process. The Change Management process facilitates the implementation of changes (new systems, modifications, …) efficiently and with acceptable risks to the existing and the new IT infrastructure. The scope of this process involves changes to any components such as hardware, communication equipment and software, systems software, environments, documentation and procedures. The Change Management process aims at controlling that changes are justified, approved, planned, tested, controlled, reviewed and supported by any efficient communication.

The Service Provider supports the hosting of the services in terms of:

- discussing with the related parties the technical details, interdependencies with existing services, potential risks or opportunities that need to be taken into account,
- gathering business and technical information for the new services,
- identifying the impact on the process for service management, delivery procedures and the applicable SLA,
- providing consultancy and support to the Customer on implementation.

The SLA also details aspects linked to:

- Daily operations/support and maintenance
- Pre-production tests
- Hosting service attributes
- Security management

	• Data protection management • Business Continuity Plan • Hosting Service levels • Defining time and other terms used • Defining performance indicators, metrics and targets • Roles and Responsibilities The Directorate Generals and Agencies are not obliged use the services of DIGIT.
Benefits, drawbacks	A consolidation of the IT infrastructure, as regards organisation and architecture, bring gains both in terms of service (better disaster recovery and resilience) and in terms of resources (better use of staff and available infrastructure). Currently, there are about 400 MoUs signed, some of which are valid only for a year. 5 years ago, there were about 50 MoUs. This high number is linked to a strong rise in IT needs at the Commission, better awareness by other DGs of the availability of this shared infrastructure, and a higher number of available services. The cost model was created in 2009 to provide a tool to provide transparent information on the calculation of the costs. DIGIT is now encouraging the use of standard MoUs for a series of services, which are valid for several years. MoUs will also be grouped by client. This will lower the administrative burden linked to the gradual increase in the number of users and the development of services over the years.

3.3. EU: sTESTA data communication network service

[20][21][22]	EU sTESTA network
Short description	sTESTA - secured Trans European Services for Telematics between Administrations –is a data communication network service. It provides guaranteed performance, high levels of security and has connections with the EU Institutions and agencies and national networks of EU Member States. sTESTA provides services including mail, DNS, FTP and NTP, and a dedicated service and operations centre (SOC) is managing and monitoring 24 by 7 all sTESTA services.
Main stakeholders	sTESTA is a European Community project, financed by the ISA work programme, implemented by EC DIGIT. External contractors provide the network infrastructure and supporting services. sTESTA is currently used by 69 networks at DG level (most of these networks concern systems supporting EU policies and connecting all the Member States), networks at Member State level and 13 networks from other European Institutions. The sTESTA network, framework and infrastructure can be used by many EU public institutions (see description of the cost models, networks and associated services in the deliverable D2.2).
Governance mechanisms	The sTESTA project is financed by the ISA programme. The cooperation structure between the Commission and the Member States reflects the need to work closely together on issues that fall under the shared competence of the Community and the Member States. Actions of the ISA workprogramme (such as sTESTA) are agreed with Member States as represented in the management committee, the CIO committee ("Committee on Cross-border Interoperability), along the lines defined in the comitology procedure. Furthermore, expert groups consisting of national representatives are established to guide the Commission in the implementation of the specific work programme actions and ensure coordination or alignment with national initiatives. sTESTA provides a telecommunications infrastructure called the EuroDomain. Each competent administration is connected to the EuroDomain as a Local Domain. Each Local Domain allows administrations to use a sectoral application, provided in the framework of trans-European communications between administrations and accessible through the EuroDomain. These administrations represent the sTESTA user community. To guarantee the same overall service level between these competent administrations, a common understanding regarding the quality of services is required. A Memorandum of Understanding (MoU) establishes a co-operative working framework with the aim of making EuroDomain and Local Domains available to the sTESTA user community at a minimum mutually agreed quality and security level. Therefore, it is required that each party undertakes the necessary actions to inform its client

administrations of their responsibilities in the context of this MoU.

Sections of this MoU are presented below.
The Commission will provide an infrastructure consisting of:
the EuroDomain, the Service and Operation Centre, the central service domain CSD, AND one sTESTA network access point per Member State: the Local Domain Connection Point (LDCP).
The <u>competent administration</u> (CA) will:
− provide an infrastructure ensuring access to the EuroDomain of the sTESTA user community for which it is responsible;
− host the LDCP;
− apply all appropriate security measures and will impose on any supported sTESTA users any conditions and sanctions necessary to protect the network;
− provide the services in respect of the minimum quality and security requirements;
− designate an administrative contact person, a technical contact person and a security officer for all matters between the CA and the Commission related to the provision and functioning of the LDCP.
Both <u>the Commission and the CA</u> will:
− configure their respective part of the infrastructure […]
− take measures in order to facilitate the interoperability between the EuroDomain and the Local Domain;
− provide a single point of contact for all questions related to the execution of this MoU;
− launch a security accreditation procedure for the relevant part of its domain […] and will designate a responsible entity for the security management;
− take all organisational, physical and logical security measures to maintain their domain […];
− take all necessary security measures to avoid compromising the smooth operational functioning of the other's domain;
− communicate to one another any relevant information about concerns, plans, and changes related to their domain;
− consult one another to take into account new needs of the sTESTA user community or new technology and ensure the efficiency of the services, adapting the capacity of their domain;
− provide support services related to any technical problem occurring in the execution of this MoU.

<u>Annex I: Infrastructure</u>
This annex addresses the hardware and network infrastructure, hosted by the CA which forms the LDCP. It describes the components, mutual responsibilities and related procedures.
<u>Annex II: Services</u>
This annex relates to the sTESTA services provided by the Commission and the CA in order to guarantee a smooth cooperation. It describes the services, availability, service levels, responsibilities, procedures and support.
- service provision under the responsibility of the Commission
  − Central services (DNS, FTP, NTP, SMTP, sTESTA portal)
  − Support: Monitoring of network performance and reports, helpdesk via the SOC for issues linked to connections

between Local Doman and EuroDomain.

– Service Availability. The Commission has several Service Level Agreements (SLAs) with the service provider, described per access point. These also state predefined intervention delays related to the incident criticality. Planned maintenance windows are also detailed.
  • Service provision under the responsibility of the CA
– Support: the helpdesk of the CA provides first line of support for users on their Local Domain and they are the contact for the central sTESTA helpdesk. The details of the support facility must be provided to all users and to the Commission.

Annex III Security

This annex addresses the minimum organisational, procedural, physical and logical security measures that must be put in place, and details the roles and responsibilities of the involved administrations.
  • Organisational aspects cover:
– Responsible entities for the security management in each domain
– Accreditation and clearance
  • Procedures regarding the maintenance of the agreed security levels need to be communicated. No specific methodology is imposed; all procedures can be based on local procedures already in place. They include risk assessment procedures, audit and review procedures, …
  • Physical Security aspects are detailed regarding the facilities hosting related to sTESTA equipment
  • Data and Access Security addresses logical controls to be put in place
  • Breaches of Security Agreement are addressed and cover issues and actions in case of a security breach.
  • Security Level Classifications describes the four official levels of classifications, invariable in all linguistic versions.

Annex IV: Applicable principles for the use of sTESTA by non-community projects

A non-Community project is a project leading to information exchanges between administrations at a European level but whose legal basis is not deriving from a Community legal act. The use of the sTESTA network by Member States in this context is done under some conditions:
  • the Community budget shall not bear any extra cost because of the use of sTESTA by non-Community activities;
  • the aim of sTESTA shall not be compromised in the process.
Consequently, extra costs associated to the use of sTESTA by a non-Community project should be carried by the MSs participating to the project. ISA can refuse a request to use sTESTA when there is a risk that such usage endangers the reliability or security of the network. ISA, after consultation of all relevant Community services, may also refuse the use of sTESTA to projects that are not in line with existing or proposed Community policies.
The practical mechanisms for including a non-community project are

	detailed. They include the two technical situations whereby either a new connection is set up, or a National authority taking part in the non-Community project wants to make use of an existing default connection to sTESTA paid by the Community budget (e.g. the sTESTA connection onto the national network). The fixed amount to be paid for this connection is calculated according to a specific formula.
Benefits, drawbacks	Governance mechanisms are addressed both through the ISA programme management and with specific and detailed modalities in the MoU between the Commission and the users. This dual approach ensures coverage of both strategic aspects and practical aspects.

3.4.   UK: G-Cloud service management framework and governance

[23][24][25][26][27]	UK: G-Cloud service management framework and governance
Short description	The ICT strategy states that the UK government is committed to exploit cloud computing to increase public sector agility and reduce the cost of its ICT. Shared resources, infrastructure and software are provided as a utility, on a pay by use basis, through a common platform – the Government Cloud Store.
Main stakeholders	Central government departments are mandated to consider public cloud first in any IT procurement and the wider public sector is strongly recommended to take the same approach.
Governance mechanisms	**G-Cloud Service Management Framework Model** To be able to articulate how G-Cloud Services are to be procured, delivered, governed and managed across many different types and sizes of user estates and service providers, the G-Cloud team has built a service framework , presented below.

Key
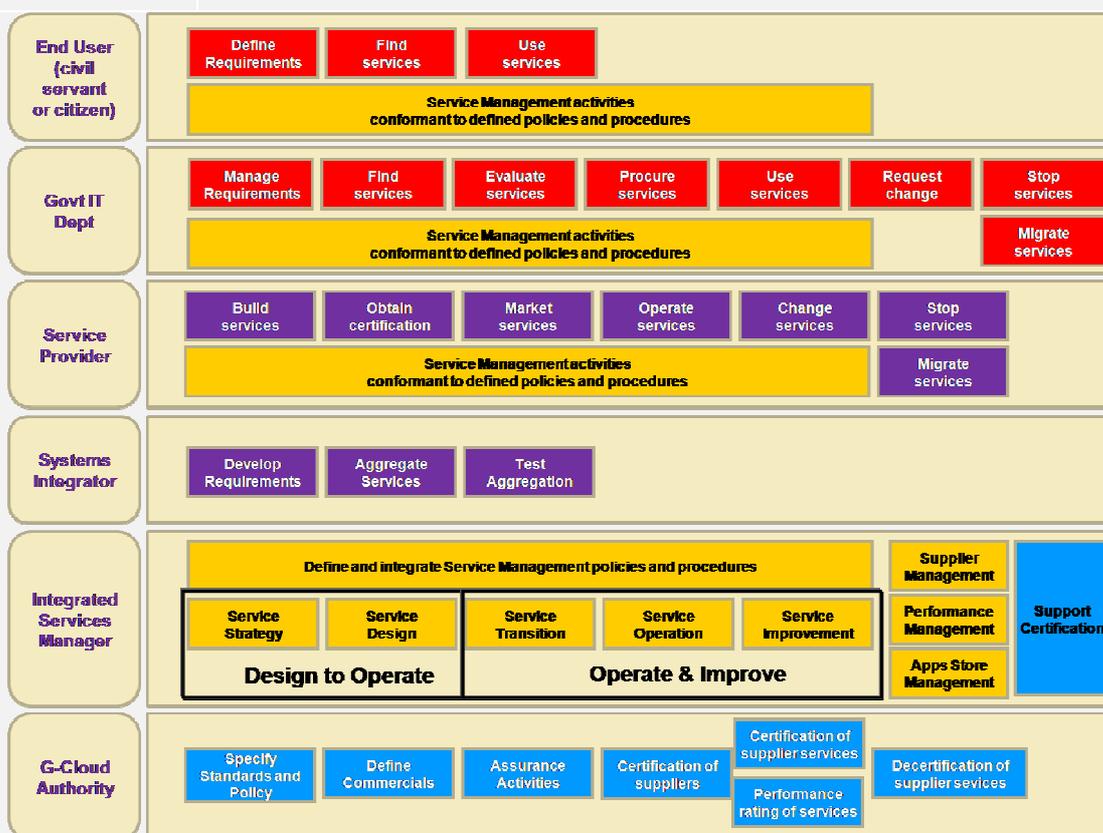
IT service management (ITSM) is performed across the framework as can be seen in the model (coloured in orange). ITSM ensures the continued delivery of high quality services by applying the needed principles, methods, and techniques through the full lifecycle of G-Cloud services; from strategy through design and transition into operation, through to retirement. ITSM is performed within all organisations involved in the G-Cloud.

**Service Management Organisation and Governance Roles**
There are a number of communities within the G-Cloud model, these are presented in the table below.

Role	Description
End User	Users (civil servants or citizens) of the G-Cloud services. G-Cloud service providers will be expected to define and communicate standards and operating procedures to the end users of the services (e.g.: how to raise a service request or incident.)
Government IT Department	The retained IT organisations within Government, accountable for delivery of IT to their businesses, users and citizens. They • Hold overall accountability for the delivery of IT service to the business; • Define and manage the IT sourcing strategy for the organisation; • Select G-Cloud services and service providers from those certified and available on the AppStore; • Retain the commercial and information risk for the business; • Accept the risk in integrating services to meet the end-to-end service levels defined by the business. The level of risk accepted will be dependent on the sourcing strategy; • Own and govern the IT/IS architecture for their business. In some cases, the body may also deliver IT services or offer procured IT services to other organisations. That part of the retained function should be considered a Service Provider.
Service Providers	Bodies that deliver G-Cloud Services. Each Service and each Service Provider is certified involving being "tested" against the information assurance, technology architecture, service management and commercial policies and standards. This accreditation for G-Cloud services is carried out by the Pan Government Accreditation service, operating under the authority of the G-Cloud Senior Information Risk Owner (SIRO). A final assessment of the suitability of the service will be carried out by local information risk owners – roughly a final 20% effort. Specifically for service management, the service provider should demonstrate that it is able to deliver and manage the service in a manner consistent with all defined service management policies,

	standards, and agreed service levels.
Systems Integrators	Bodies that build services to meet a new business need by combining hardware and software products, and potentially services from multiple vendors to meet a business requirement. A systems integrator links multiple systems for inputting, processing, interpreting, storing and categorising data to meet a defined business need. As IT services move towards becoming more standard and commoditised, Public Sector spend on systems integration is expected to fall.
Integrated Service Managers	Organisations that will ensure that services are delivered in a cohesive and effective manner, that the defined IT service management processes are adhered to across multiple service providers. An ISM function ensures that the provision of services meets the user requirement in an efficient form. This may include: • Provider of enabling platform management services (including provisioning, billing, AppStore instantiation) • Actively manage elastic services across G-Cloud • Service Desk • Managing the framework for integrated ITSM, including: incident, problem, change management and all other ITIL disciplines in a manner consistent with the Authority published service management policies and standards • Service monitoring and reporting (by provider and e2e) • Continuous improvement • Security assurance • Continuity management • Supporting service certification on behalf of the Authority
G-Cloud Authority	A body having oversight of the G-Cloud. The G-Cloud Authority is responsible for: • Oversight of the G-Cloud • Specifying G-Cloud Policies, Protocols and Standards • Supporting commercial arrangements and framework standards, • Service Design Authority • Information Assurance Standards • Assurance Authority This is based on the PSN[11] authority model. The G-Cloud Authority will be supported by a number of expert communities, including information assurance, service management, commercial management and technical architecture. These communities will define the protocols and standards against which service providers and services will be certified. Business and supplier communities will be expected to actively participate in the governance of the G-Cloud.

---

[11] https://www.gov.uk/public-services-network
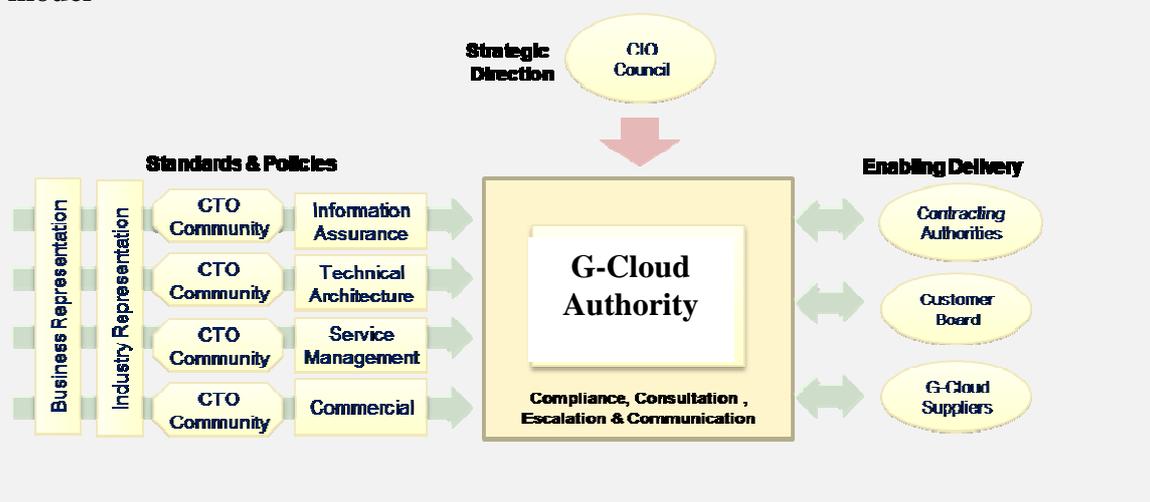
G-Cloud governance model	
Benefits, drawbacks	One of the recommendations on the starting up of the G-Cloud project was to implement a robust governance model underpinned by clear roles and responsibilities and common standards to ensure seamless interoperability and operational effectiveness.
	However, this model has not been implemented completely, due to lack of time, success of the use of G-Cloud (see Deliverable D2.2).
	G-Cloud has now appointed a team nearly double in size; the team will focus on working with the Government Procurement Service (GPS) to help and advise suppliers already on G-Cloud, as well as potential suppliers in the future. It will also continue to work with government and the wider public sector to raise awareness of the programme and its benefits; and it will help government departments understand and use G-Cloud so that they meet their commitments under the public Cloud First policy.
	The main challenge is the service integration. This new environment needs to focus on aspects such as Performance Management, Citizens services, tooling and a service integration model. Business IT services will need to be operated in a regime that, for instance, is wider than a view of service level achievement and looks at measuring usability from a consumer perspective and allows assessment of the performance of the complete service end to end, not just separate components provided by each supplier.
	Service Integration and management of IT services will need to reflect that Citizens will be consumers of government services and will require support and that engagement is necessary to ensure their view of service performance is reflected.
	Common data standards will need to be defined to support tooling requirements. Tooling content will need to be interoperable between suppliers and IT services/components. They will need to underpin automated processes e.g. consumption feeds billing, incident data feeds Service Level measurement, transaction monitoring feeds

performance measurement etc.

A Service Integration model is needed, and would include for instance:

- A thin in-house capability ultimately responsible for the integrated end to end operation and management of quality IT services, underpinned by out sourced integration services for specific elements [e.g. performance monitoring, service desk, service level reporting etc];
- Definition of IT service management processes for use across multiple service providers, delivering services to multiple businesses, in a cohesive and efficient manner:
  o Managing the framework for integrated ITSM, including: incident, problem, change management and all other ITIL disciplines in a manner consistent with service management policies and standards
  o Service monitoring and reporting
  o Continuous improvement
  o Security assurance
  o Continuity management

To ensure new/amended IT services can be operated within the service integration model in place, developers/ projects need to ensure operating requirements are considered when packaging the solution – elements to consider at design include What service integration wrap [if any] is required, and documentation of all components of the service [may be procured from various suppliers] along with the commercial arrangements for each supplier.

4. SHARED DEVELOPMENT

4.1. EU: EC DG TAXUD Sunset project

[28][29][30][31]	**EU DG TAXUD: Sunset project**
Short description	After the completion of the "Sunset project", the National Administrations (NAs) would be responsible for the maintenance and support of the application developed, maintained and supported by the Commission so far. Sunset phase 1 was the collaborative creation of the call for Tender (CfT), with participation and contribution of 14 National Authorities. Sunset phase 2 was the actual publication, evaluation and contract signing, involving four NAs (NL, IE, SE and MT).
Main stakeholders	Co-ordinator (Commission), a main facilitator (NL), National Authorities, a service provider.
Governance models and mechanisms	The Commission was in charge of software (or Transit Applications) which the NAs could operate in order to participate in the Trans-European projects. In 2006, the Commission decided the 'Sunset' meaning the end of the specification, development, deployment and technical support of these applications by the Commission and the hand-over to the NAs, within a transition period of 24 months[12]. Governance aspects related to this case are threefold: 1. The collaboration in phase 1 for creating the CfT 2. The transition phase for the takeover of the application 3. The collaboration in phase 2 and the Change Management Board 1. **Phase 1:** Governance of the collaboration was clarified in a letter of intent, signed by each NA. Excerpts are presented below. The Commission - being the owner of the intellectual property rights of the applications- provided the European countries with the source code to enable the European countries to arrange the future development and maintenance of those applications for themselves. […] a joint tender-procedure would produce more benefits (especially cost reducing, knowledge combined, more interesting for vendors), not only for the countries involved, but also for a more consistent future development of the application. After an inventory among the European countries, the Dutch

---

[12] The increasing requirements expressed by the NAs in terms of better aligning the applications to their needs and fully integrating them in their national environment, led the Commission to this decision.

Taxation and Customs Administration (DTCA) agreed to take the role as facilitator in the tender preparation phase, under the condition that the countries involved share the workload and participate actively. Each Party has the right to end its contribution at any moment, at its own discretion under the condition that its produced products until that moment will be available for the other Parties. Every participating country bears its own costs.

Parties agree to co-operate in the making of the request for proposal (RFP) and to come to a joint understanding of the subsequent tender-procedure. The co-operation between the Parties will be on the basis of equality. The Parties agree to participate actively and divide the workload as described in section Procedure-arrangements. Each Party is and remains responsible that the final version of RFP is in line with the requirements of their national (functional) specifications and its national tender-rules and regulations.

The Parties intend to execute a joint tender-procedure. They shall discuss the method, procedures and the division of tasks to be used in the tender phase. Since the ultimate goal is to select a contractor before the end of 2007 the RFP, and the mentioned discussions, have to be concluded by July 2007 (a detailed planning was made).

The DTCA provides a start-document for the functional and technical part, in which the parties make amendments. The DTCA processes them in an updated version of the RFP, distributed to the parties who send their comments to the DTCA not later than one week before the upcoming meeting, where that version will be discussed. In parallel to this process, discussions about the method, procedures and the division of tasks to be used in the tender phase will be put on the agenda by DTCA. Procedure-arrangements to this phase will be concluded by the Parties in that meeting. The final version of the RFP will be presented to the Parties.

2. **The transition phase of the takeover** was managed using the ITIL[13] methodology for identifying all the processes inside the project and specifying which of these are transferred from the Commission to the NAs.

The project is split into two levels of activities and responsibilities. The first level is the Trans-European level, where the basic activities are shared among the Commission and the NAs and are related to:

−Co-ordination and Planning;
−Specifications, (update of documents which are the tools for the implementation of the project);
−Monitoring and Reporting (availability of the national transit

---

[13] ITIL is the acronym for the "IT Infrastructure Library". It is a de-facto standard in the area of service management. It comprises a number of best practice guidelines for service management, which describe what, rather than how.

applications...)

−Service Desk, Service Support and Service Delivery (ITIL
   processes) on the level of specifications and operations

The second level is the Applications level, where the activities are
distributed to the Commission and the NAs.

The figure below presents the activities and responsibilities not
affected by the sunset (marked in black), and those affected (in
orange). The process owner sets up and manages the process. The
implementer implements the process and executes the activities
related to it.

	Process Owner		Implementer	
Service Desk	DG TAXUD	NAs	DG TAXUD	NAs
	✓		✓	
Service Support	DG TAXUD	NAs	DG TAXUD	NAs
1 Incident management	✓			✓
2 Problem management	✓			✓
3 Change management	✓			✓
4 Release management	✓			✓
5 Configuration management	✓			✓
Application Management	DG TAXUD	NAs	DG TAXUD	NAs
1 Application Development (Specifications, Programming, Testing)		✓		✓
2 Application Operations		✓		✓

Labels:

	Function	✓	remains as before
	Process	✓	transferred to the NAs

3. The collaboration in phase 2 and the **Change
Management Board**

The takeover option chosen was *"Group Development & Support +
National Adjustments"* were all NAs would take over together led
by a Development & Support Committee. All NAs in the Committee
have equal say[14]. One contractor is assigned for the development
and maintenance of the future applications. The contractor
develops "mother" and "child" applications. Every NA can specify
its own national needs to be developed in the child applications.
Each NA signs a contract with the contractor and an extra contract
for its pure national needs. The content of each contract is the
same except from some minor clauses related to differences in the
national laws. The connection between the contracts exists in the
statement that a common **Change Management Board** (CMB)
comprising the four countries has the right and power to order
changes to the contractor. A Change Management Board Procedure
is fully documented. Each participating administration is
represented by two representatives with mandate in the CMB. The
contractor is also member of the CMB.

2.1 Organisation

The CMB is organised as follows:

---

[14] This collaborative model is described in detail in ISA Action 4.2.5 Deliverable D2.2.

- The role of chairman and secretariat rotates between the member countries. To ensure effective operation both roles must be filled by one country for their term of office (one year).
- Each country provides two people, one with business/procedural knowledge and the other with ICT knowledge.
- There is at least one formal meeting per annum to agree common changes. Binding decisions are made at this meeting only. Prior discussions may take place using conference calls or emails.
- The agenda, list of items for decision and any other documentation are circulated 4 weeks in advance of the meeting.
- The change proposals are submitted in a prescribed format to the secretariat. Proposals must include sufficient information to allow an informed decision to be reached.
- Proposals can be agreed or rejected at the meeting. The secretariat will ensure that agreed proposals, together with the required implementation date, are submitted as a formal Common Change Request to the contractor. Rejected proposals can still be submitted separately by an individual country via the National Change Manager (NCM) mechanism.

A request for change can be submitted by customs authorities, IT departments, the contractor, traders or DG TAXUD.

Requests from the national Customs authorities, IT department or traders are first to be agreed at national level.

Change request (CR) procedure - roles and responsibilities

The letters in the different columns have the following meaning:

R – Responsible (Needs to Act)

A – Accountable (Only one person is Accountable)

C – Consult

I – Inform

CR procedure	National Change Manager	Change Management Board	Contractor
Create a change request & Produce Call & assignment of category	RA	I	I
Analyse change	I	I	RA
Assess of proposed changes from both business and technical perspective	I	RA	I
Estimate the impact of the change on installed applications and infrastructure & resources	I	I	RA
Confirm the agreement to change	I	RA	I
Select a technical solution answering the needs	I	RA	CI

Provide planning for the implementation of the selected solution (testing included)	I	RA	CI
Assess of the risk	I	RA	CI
Provide back-out/ Fall-back strategy	I	RA	CI
Implementation of the Change Request (docs & applications)	I	I	RA
Approve or reject the change request for production	RA	I	I
Prepare and install the applications in the production environment	RA		I

In practice

There are change requests or functionalities supported by only one or all countries. This occurs because although there is one common customs regulation, the way it is implemented in the countries differs. As a certain number of NAs collaborate, costs are shared[15].

There is one Contracting Authority per country. The Contracting Authorities are the Revenue Commissioners (IE), the Customs Department (MT), the Dutch Taxation and Customs Administration, the Swedish Customs Administration. The co-operating National Administrations (NAs) agreed, that the single point of communication for the tender is the Contracting Authority of Sweden. The starting and closing date and time for submitting the tenders are the same for all participating Contracting Authorities. The Call for Tender and consequently the Agreement is governed by the national law of each Contracting Authority. Per Contracting Authority there is one Agreement. The objective is to engage one contractor for all Contracting Authorities. This is a corporate Call for Tender, meaning that when once a company tenders in the Call for Tender, its tender is valid and common for all Participating NAs. A Company being a legal entity can send one tender only, for this corporate Call for Tender. The received tenders will be evaluated in a common way. Any NA provision will be covered in the specific national agreement between the NA and the contractor. Each Contracting Authority will take part in the Evaluation Committee. The selection rules are very clear in order to assess if the Tenderer is capable of serving so wide a community. The contractor will sign one contract per NA.

Benefits and drawbacks	The CfT serves collaborative development between NAs and it concerns software built by the Commission and handed over to the NAs. Therefore certain points of the CfT are characteristic and serve explicitly this nature.
	The CMB, procedure of reporting and handling of change requests are detailed. The CfT includes a Change Management System. It

---

[15] This is developed in Deliverable D2.2 Business models

also includes hand-over missions and trainings.

Specific legislation on collaborative procurement is needed to clarify unclear aspects in the collaborative procurement process, because of differences in each MS's legislation. Because of this, only 4 NAs participated in the CfT. Specificities of National legislation had to be taken into account, for instance the fact that in Sweden, tenders had to be opened by a Swedish authority in Sweden.

Guidelines on joint procurement are presented in the deliverable D2.3.

4.2. EU: EC DG TAXUD Collaborative implementation of the Customs Code

| [31][32][33][34]	EC DG TAXUD: Customs Code[16] - Collaboration and governance
Short description	A study from DG TAXUD clarifies a global work plan (IT Master Plan - ITMP) for the full Modernised Customs Code[17] implementation. It focuses on collaboration between Member States (MSs) and the EC.
Governance model	The EU customs IT is challenged with the high redundancy, complexity, divergence and overall cost. MSs need to increase working more in a collaborative manner to address with these issues. The ITMP study identified potential savings if some willing MS collaborate to implement IT projects, so as to reduce their national implementation costs. In this context, DG TAXUD still needs to develop the reference architecture, the collaboration methodology and terms of reference, setting up the governance, etc.
	However, during this study, collaboration activities were launched with the objective to explore collaboration opportunities and forms amongst the MSs, including:
	• Collaborative development of a complete EU Customs Reference Architecture through an Architecture Group with a number of MSs;
	• A pilot collaboration project driven by the MSs to explore the feasibility and the method of collaborative working (i.e. Customs Warehousing collaboration pilot project).
	During the ITMP study, MSs have expressed the need for a clear governance structure *within each working team*, including the aspects of governance, Reference Architecture and tools. MSs have emphasised that the commission's participation is important for the success of the collaboration to provide the necessary steering and coordination. DG TAXUD has provided limited steering and coordination in the scope of the Customs 2013 Program for the abovementioned collaborative activities. Future collaboration activities will be carried out in line with the scope of the FISCUS 2020 program which is currently negotiated.
	It is relevant however to mention that the ITMP will be governed according to the Multi Annual Strategic Plan (MASP) overall governance framework[18].

---

[16] The Modernised Customs Code (MCC) was adopted in 2008 in order to simplify and streamline the customs processes and procedures for the benefit of both customs authorities and traders. What come along are the large-scaled changes in the european Customs Systems at national as well as on European Commission level, implied by the implementation of the MCC.

[17] Regulation (EC) No. 450/2008 of the European Parliament and of the Council of 23 April 2008 laying down the Community Customs Code (Modernised Customs Code), OJ L 145/1 of 4 June 2008. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:145:0001:0064:EN:PDF

[18] http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/e-customs_initiative/annex_3_governance_scheme_en.pdf

---

The Governance Scheme for the Implementation of the MASP and its related Electronic Customs Projects is a three-layered Governance model.

The organisational structure is limited to three main layers in order to enhance coherence and coordination, to reduce duplication and bureaucracy and to ensure commitments at the appropriate levels.
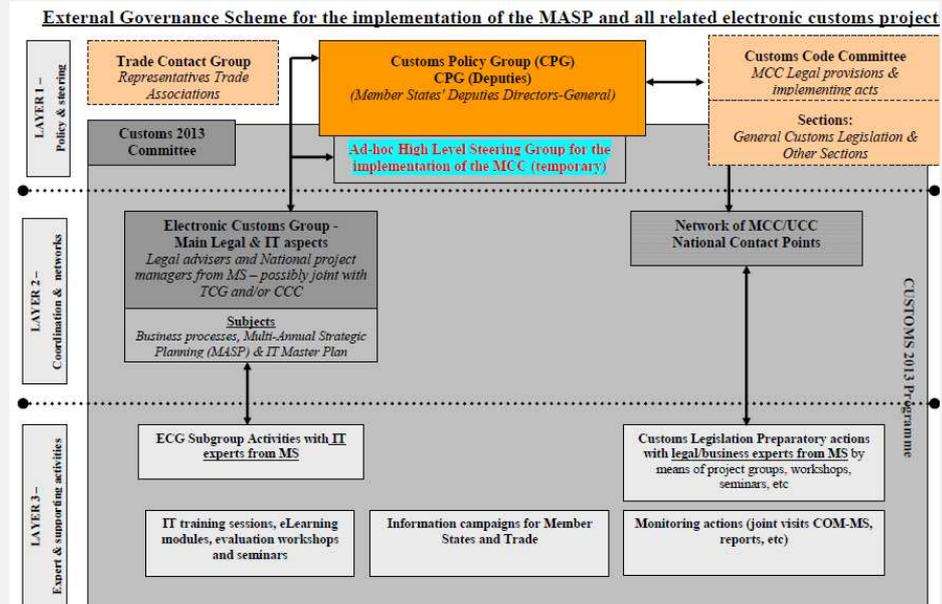
The following bodies assist the Commission and the MSs in their responsibilities as regards the strategic direction, preparation, implementation and follow-up of the electronic customs initiative:

►Layer 1: Policy and Steering
Bodies: Customs Policy Group (CPG) / Customs Code Committee / Customs 2013 Committee/ Trade Contact Group
The CPG acts as a steering body for the electronic customs strategy and coordination. It defines strategies, ensures the coherence of activities related to electronic customs, oversees and coordinates legal and operational aspects as well as IT developments, steers the implementation activities of all stakeholders, endorses the MASP, ensures agreed deadlines are respected, provides high level scrutiny of major initiatives, particularly where there are resource implications at national or Union level.

The CC Committee provides information and consultation/exchange of views on legal aspects, as well as formal consultation on implementing provisions/acts in accordance with the comitology rules.

The Customs 2013 Committee takes on an overall coordination and monitoring role of the programme activities and related budget expenditure. However, given the large variety and quantity of activities, steering groups are created to carry-out the coordination function for specific activity areas.

The members of the Trade Contact Group are representatives of the

main international associations involved in customs related activities at the European level. The status of the trade representatives within the TCG is of a "consultative" nature. Structured dialogue between Commission and trade occurs on a regular basis.

►Layer 2: Coordination and Networks

Bodies: Electronic Customs Group (ECG)/ Network of MCC/UCC contact points (non active).

ECG includes middle management representatives from all Member States / Candidate Countries with competency in legal, processes & BPM, project management, operational, planning and IT technical aspects and being mandated by their administration. The role of the ECG is to agree with the Commission on the implementation of electronic customs projects as defined in the MASP as regards

- ensuring coherence between the customs legislation and the implementation of electronic customs (e.g. standardisation of data elements and messages);
- preparing and establishing a suitable and interoperable IT environment responding to the requirements of electronic customs (e.g. harmonisation of interfaces);
- ensuring coherence and consistency between all projects related to electronic customs and between the projects and the MASP;
- improving the dialogue with trade on complex customs issues.

The ECG also assist the Commission in the establishment and updating of the MASP implementation plan.

►Layer 3: Expert and Supporting Activities

Bodies and related activities: Electronic Customs Group – technical subgroups, IT training sessions & eLearning modules, customs legislation preparatory actions, monitoring actions evaluation workshops and seminars, information campaigns, etc.

This layer includes delegates from some or all Member States / Candidate Countries having expertise in a specific electronic customs related subject and having been mandated to work on the issue.

The role of the ECG subgroups is to agree with the Commission in:

- the implementation of all electronic customs projects as defined and scheduled in the MASP as regards the functional requirements and technical specifications;
- the preparation and execution of corrective and evolutive maintenance activities related to existing IT systems based on the agreed change management procedure and updates of functional and technical specifications.

Other activities are carried out as defined in the approved Customs 2013 action proposal.

Benefits and drawbacks	During the ITSM study, the Customs Reference Architecture has served as a key instrument for the collaboration. IT is essential from the following perspective: • Facilitate the discussions and decisions by providing a

common language;
- Identify services candidates for sharing/reusing and opportunities for collaboration;
- Enable collaboration projects between MS based on a common reference of services;
- Fix unambiguously the scope the project in terms of services;
- Provide a planning basis for future projects.

The benefits of defining an overall governance frame for electronic customs (as described above) are listed below:
- High number of stakeholders with divergent needs and prerequisites;
- Very broad and far reaching initiative with many different aspects to be analysed, discussed, agreed upon and implemented within an ambitious timeframe;
- Substantial amount of Union and national budgets required to finance the preparation and implementation of electronic customs; considerable need for human resources at Union and national level
- High degree of interdependence between electronic customs (legal, processes & BPM, IT, other operational aspects such as training, communication, etc) and related areas (risk management, tariff, customs controls, etc)
- Importance of defining roles and responsibilities in order to ensure that all parties engage to meet the prefixed deadlines (electronic customs can only succeed if each Member State implements each phase at the same time).

Responsibilities are clearly and explicitly defined for each layer and for each body involved.

4.3. EU Municipalities: Shared development

[36][37][38] [39][40][41]	Shared development among EU municipalities
Short description	Many cases of municipalities in Europe sharing development of common IT solutions. This section presents the governance models and mechanisms of two municipality associations: Frikomport in Norway and Sambruck in Sweden. OpenMairie in France is a similar case, but the organisation focuses mostly on the business model and the economic actors involved. This case is described in detail in Deliverable D2.2 Business models. eBourgogne in France is a large community of municipalities sharing common platforms with an organised common procurement through a Public Private Partnership. This case is detailed in Deliverable D2.2 Business models. The cases of Frikomport and Sambruck are presented together as they address municipal sharing and re-use in different ways, and provide complementary practices.
Main stakeholders	**Frikomport**: The Kongsberg region includes 7 municipalities, collaborating in several areas. In 2006, the Region developed a portal to administer courses for municipality staff (Frikomport). It is currently reused by 70 municipalities and organisations. **Sambruck** is a non profit organisation, founded in 2005 to collaborate about and "co-use" e-services, increase the purchasing powers for smaller members. It has over 100 members, including Municipalities, Government Agencies, and Public Organisations.
Governance model and mechanisms	**Frikomport**: The focus is on building a sustainable community, and on user collaboration. The basis for the cooperation is founded around FriKomPort. By organising themselves in an association, the members can ensure that the value chains of the different projects are interdependent, ensuring re-use and benefits. The FriKomPort community is supported by a portal - http://friprogforeningen.org/ – providing news, project descriptions and code, links to all installations, an electronic helpdesk system, a description of new features. The development of new features is decided following the vote by the reference group who are members paying a voluntary annual development fee. The new release is then made available to all members. In some cases, new functionality is developed by a user in their «local» installation; this functionality was then implemented in the main version, financed by the annual voluntary fee. **Frikomport sharing model** Ideas for solution enhancement can be submitted by all users. The reference group chooses a subset of proposals and then votes for which ones to be implemented in the solution, provided as software as a service. The new features are also available in the downloadable open source solution, available to all.

The reference group is elected during the annual user conference.
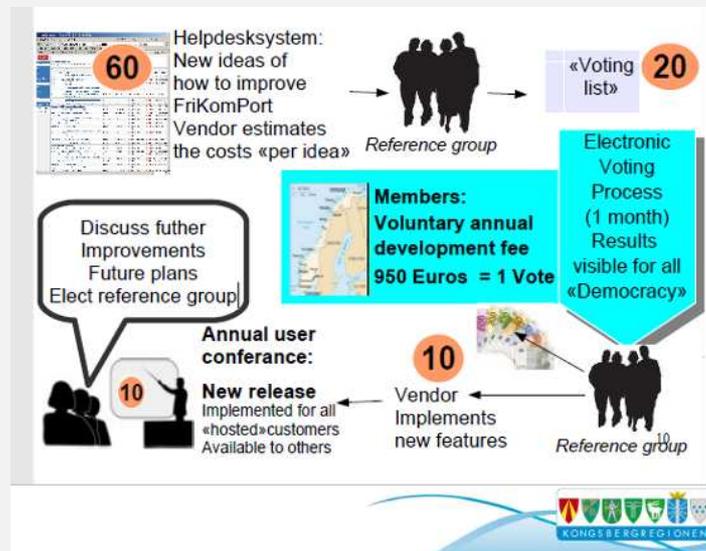
Sambruck Collaboration Framework Process model

Sambruck Members initiate a project. Sambruk creates the project, using the Sambruck Collaborative Framework (SCF) which provides regulations regarding the project, membership and result. Sambruck also finds financing and prepares for procurement. The Supervisory Board consists of financing project members. It is responsible for the evaluation, management and development of a solution. It is also responsible for financing the maintenance and development, signing agreements with third parties (as participants or supplier) and provides the terms for use and distribution of the solution (ie. license).
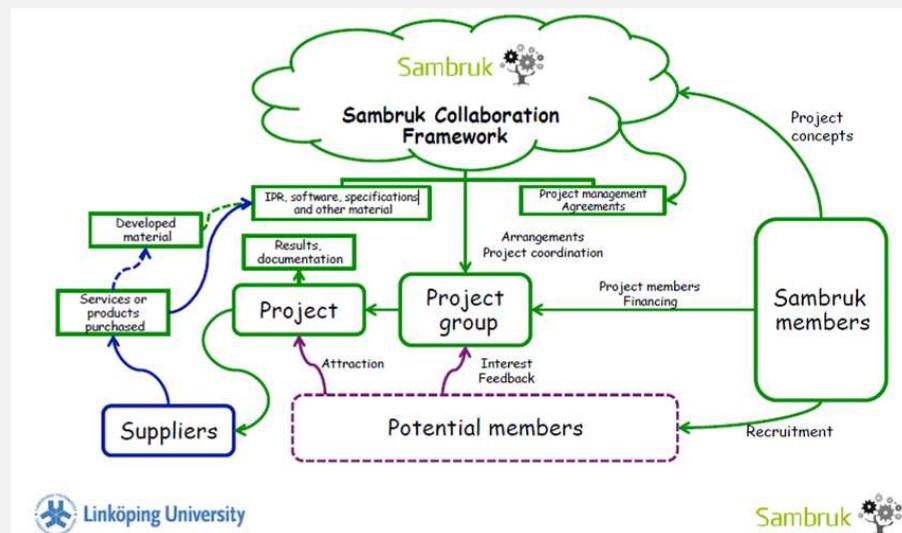
Sambruck Collaborative Framework (SCF)

The SCF clarifies the relationship between financing members and suppliers. The SCF consists of regulations and agreements covering important phases of

common development. Various aspects of development, such as copyright, the type of materials to be developed, the use and management of developed material are considered.

The SCF promotes collaboration; it deals with all types of "material", including developed software, re-used software, use of frameworks, documents (specifications for RFI, RFP, RFQ, etc.). It regulates copyright and other rights; it ensures the access of the material by members, and ensures that the material can't be made proprietary against the wishes of the project members.

The SCF retains the copyright – this minimizes illicit exploitation and protects the users from suppliers' changes. It also provides for making the solution open source, based on approval of the financing members. These standard agreements can be tailored to each specific situation and type of material. The framework itself can be adapted, and will have an open license.

The default licensing is open source, which enables participation of non-members, enables innovation beyond Sambruk. Suppliers can be changed throughout the life cycle of the solution. The SCF also provides for commercialization, based on financing members approval; the copyright is still retained by Sambruk.

Benefits and drawbacks	**Frikomport** The initial project (Frikomport) was supported by the municipalities during their working hours, requiring an initial investment borne by a small number of municipalities and some volunteer work. The current model needs to be more formalised, especially regarding the collaboration between administrations; the association needs more predictable financing and support. It is typically a bottom-up initiative with high buy-in, but limited funding. The solutions are hosted as a service, this delivery model is very successful. **The Sambruck Collaboration Framework** is the outcome of a research project named BOSSANOVA (Business Models for Open Source Software New Opportunities for Customers and suppliers). Results from the initial diagnosis (longitudinal case studies 2005-2008 in a Swedish network of 80 collaborating municipalities, and a survey 2008 to all Swedish national and local authorities) indicated that Swedish municipalities do not use open source to a large extent, and that experience sharing and a supporting framework were needed. As a solution, the SCF was suggested. The framework was developed and implemented in the form of action research. Evaluation of this implementation indicated two major conclusions. First, this approach could strengthen the community, in so that the user-driven innovative solutions stayed under the control of the user organization. This prevents that the results of the customer's own development efforts in collaborative projects unintentionally are transferred to supplier companies, and need to be re-purchased. Second, the approach can work only if both customer-side and supplier-side can take advantage. An open attitude to enhance fulfilment of the supplier's drivers, such as commercialization opportunities, is needed from the customer's side.

5. CONCLUSION

The following section presents the conclusions drawn from the real life cases of governance models and mechanisms for sharing and re-use described in this document.

The document showed concrete examples of very different types of collaboration for common IT solutions, and governance and collaboration mechanisms put in place to support this collaboration.

Each initiative has a governance model or formalised collaboration mechanism, whatever the scale of the initiative.

The level of formalism of the link between the collaborating bodies varies; it can be a simple letter of intent, an MoU, an SLA, a formal governance organisation or even a formal legal structure.

Initiatives of sharing or re-use focus on their main goal: generate savings. The formalisation of governance is not always addressed as a priority, and sometimes these aspects, which would enhance collaboration, are underestimated or addressed later in the project. Some cases show that governance models are not fully applied in practice, as the project needs to focus on operational aspects first.

However, all cases are successful in their sharing or re-use initiatives and we can identify good practices. For example, a Collaboration Framework, as in the Sambruck case, which can be adapted to each project, can prove to be useful. Another example is the state-of-the-art governance structure used by DG TAXUD for Multi Annual Strategic Plan (MASP) overall governance framework. The efficiency of a detailed and comprehensive MoU is shown in the case of e-Prior.

Guidelines for agreements between administrations presented in another Deliverable (D2.3) aim at detailing aspects to be covered in sharing or re-use projects.

6. REFERENCES

[1]. Interview with Project Manager - Programme Monitoring Swiss eGovernment

[2]. Swiss eGovernment Action Plan http://www.egovernment.ch/fr/umsetzung/aktionsplan.php

[3]. Swiss eGovernment catalogue of priority projects http://www.egovernment.ch/en/umsetzung/katalog_vorhaben.php

[4]. Organisational structure for implementing the eGovernment Strategy http://www.egovernment.ch/en/organisation/index.php

[5]. Framework agreement on eGovernment cooperation in Switzerland http://www.egovernment.ch/en/grundlagen/rahmenvereinbarung.php

[6]. Interview with a manager at IMIO (http://www.imio.be/)

[7]. Model for deliberation for a commune to participate in IMIO: http://www.imio.be/presentation/adherer/imio-projet-de-deliberation-affiliation-imio-communes.pdf

[8]. Statement of Regional Policy 2009-2014, the Walloon Government http://gouvernement.wallonie.be/publication/declaration-de-politique-regionale-2009-2014

[9]. (Joinup – 2012) Public Open Source Software Procurement Models – The Next Generation http://joinup.ec.europa.eu/sites/default/files/studies/Public_Open_Source_Software_Procurement_Models_The_Next_Generation.pdf

[10]. (Melin 2012) Presentation of the Framework Agreement of the Swedish Government to Procure Open Source –video http://www.youtube.com/watch?v=7mz2D1B5hl0

[11]. Interview with procurement officer managing that framework.

[12]. Pan European Public Procurement: Enabling its implementation within the European Union institutions, agencies and other bodies, and facilitating its adoption across the Member States - Francisco Garcia Moran (2012) http://www.ippa.org/IPPC5/Proceedings/Part2/PAPER2-4.pdf

[13]. Interview with DIGIT e-PRIOR project officer

[14]. Interviews with EC DIGIT Directorate C - Head of Unit and Head of Sector - Administrative and Financial Coordination

[15]. (2010) DIGIT Cost Model Extension – Final Report

[16]. Interview with EC DIGIT 01 (e-Commission, Methodology and Programme Office)

[17]. DIGIT - IT Governance structures at the European Commission

[18]. SEC(2004) 1267 - Communication to the Commission on the improvement of information technology governance in the Commission.

[19]. SEC(2010) 1182 – Communication to the Commission of 7.10.2010 - Getting the Best from IT in the Commission

[20]. Interview with EC DIGIT sTESTA project officer

[21]. sTESTA Memorandum of Understanding with Agencies

[22]. Description of sTESTA on ISA website http://ec.europa.eu/isa/actions/02-interoperability-architecture/2-4action_en.htm

[23]. Ref: (2010) UK Cabinet Office, Data center strategy, G-Cloud and appstore programme phase, Service management, organisation and governance approach.

gcloud.civilservice.gov.uk/files/2013/05/Service-Management-Framework.doc

[24]. http://gcloud.civilservice.gov.uk/public-cloud-first/

[25]. http://gcloud.civilservice.gov.uk/service-integration/

[26]. http://gcloud.civilservice.gov.uk/supplier-zone/accreditation/#process

[27]. What's next – http://gcloud.civilservice.gov.uk/2013/07/16/g-cloud-next-phase/

[28]. Interview with DG TAXUD Sunset project owner

[29]. (2009) DG TAXUD - TRANSIT COMPUTERISATION PROJECT – Collaborative procurement for the CDTA-NO

[30]. (2007) Public European Call for Tender Services - Maintenance software CDTA/NO

[31]. Interview with DG TAXUD – IT Strategy, Planning and Workprogramme Manager - Enterprise IT Architecture & Strategy Sector

[32]. (2010) DG TAXUD - IT Master Plan Study Report

[33]. Regulation (EC) No. 450/2008 of the European Parliament and of the Council of 23 April 2008 laying down the Community Customs Code (Modernised Customs Code), OJ L 145/1 of 4 June 2008. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:145:0001:0064:EN:PDF

[34]. (2012) DG TAXUD - Governance Scheme for the Implementation of the MASP and its related Electronic Customs Projects. http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/e-customs_initiative/annex_3_governance_scheme_en.pdf

[35]. (2012) DG TAXUD IT Strategy http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/e-customs_initiative/annex_6_it_strategy_en.pdf

[36]. (2013) Presentation: The Friprog Association - Britt Inger Kolset - Coordinator of a regional ICT-program in the Kongsbergregion, Norway Project Manager of FriKomPort, General Manager of the Friprog organization http://joinup.ec.europa.eu/sites/default/files/FriKomPort_Granada_120112_Britt-Inger_Kolset.pdf

[37]. Website of Friprogforeningen – the Norwegian free software association http://friprogforeningen.org/

[38]. Website and source code of the FrikomPort project https://projects.knowit.no/display/FRIKOMPORT/Fri+KompetansePortal

[39]. Sambruck Collaborative Framework http://www.sambruk.se/ramverk/ramverkforsambruksmaterial/projektdokument.4.6fa04b8c12eede97bff80006109.html

[40]. Sambruk Collaboration Framework – presentation by Thomas Rosenfall - Linköping University and Sambruk http://www.sambruk.se/download/18.78e67851135cb0d063d2b8d/OSEPA_march_2012_sgmThomas.pdf

[41]. Interview with Thomas Rosenfall