

EN

EN

EN



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels,
SEC(2009) 837

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

Proposal for a

**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
establishing an Agency for the operational management of large-scale IT systems in the
area of freedom, security and justice**

and

Proposal for a

COUNCIL DECISION

**conferring upon the Agency established by Regulation XX tasks regarding the
operational management of SIS II and VIS in application of Title VI of the EU Treaty**

IMPACT ASSESSMENT

{COM(2009) 292 final}

{COM(2009) 293 final}

{COM(2009) 294 final}

{SEC(2009) 836}

TABLE OF CONTENTS

COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT	6
1. Titles of proposals	6
2. Document reference number	6
3. Introduction	6
4. Procedural Issues and Consultation of interested parties	7
4.1. Approach and methods applied	7
4.2. Stakeholder consultation	8
5. Problem definition - Challenges	9
5.1. Operational	10
5.1.1. Ensuring effective management of the systems, taking into account their critical character and their 24/7 availability;	10
5.2. Governance	11
5.2.1. Need to ensure that the views of all stakeholders are taken into account and that the roles of the EU Institutions are ensured	11
5.2.2. "Géométrie variable" - heterogeneous group of participating countries (EU Member States with different levels of participation and associated countries)	11
5.3. Financial	12
5.3.1. Need to ensure (cost-) efficient management	12
5.3.2. Need to ensure timely and adequate funding	13
5.4. Legal	13
5.4.1. Importance of effective data protection and supervision	13
5.4.2. Importance of effective mechanisms and redress for abuse or faults causing damage	14
5.5. The need for EU action	14
5.5.1. Subsidiarity	14
5.5.2. Added value of EU action	14
5.5.3. Proportionality	14
6. Objectives	15
7. Policy options	17
7.1. Option 1 – The Baseline option	17

7.2.	Option 2 – The Baseline+ option	18
7.3.	Option 3 – New Regulatory Agency	18
7.4.	Option 4 – FRONTEX	18
7.5.	Option 5 – Europol for SIS II and Commission for VIS and EURODAC	18
8.	Analysing impact and comparing options.....	19
8.1.	Operational.....	20
8.1.1.	Baseline and Baseline +	20
8.1.2.	Regulatory Agency.....	21
8.1.3.	FRONTEX	21
8.1.4.	Europol.....	22
8.2.	Governance	22
8.2.1.	Baseline and Baseline+	22
8.2.2.	Regulatory Agency.....	23
8.2.3.	FRONTEX	24
8.2.4.	Europol.....	24
8.3.	Financial.....	25
8.3.1.	Baseline and Baseline +	25
8.3.2.	Regulatory Agency.....	26
8.3.3.	FRONTEX	26
8.3.4.	Europol.....	27
8.4.	Legal.....	27
8.4.1.	Baseline and Baseline+	27
8.4.2.	Regulatory Agency.....	28
8.4.3.	FRONTEX	28
8.4.4.	Europol.....	29
8.5.	Rating of the options	29
9.	Implementation costs of the main option	33
9.1.	Assessing the costs.....	33
9.2.	Scenarios concerning moving of the systems to a new location	39
9.3.	Adding new systems	41
10.	Preferred option – a new Regulatory Agency	43

10.1.	Scope of the tasks of the Agency	43
10.1.1.	Responsibility for development and management of new systems in the area of freedom, security and justice,.....	43
10.1.2.	Responsibility for technical implementing rules.....	43
11.	Monitoring and evaluation	44
11.1.	Operations	45
11.2.	Monitoring.....	45
11.3.	User support	46
Annex 1 Pre-screening of options		47
1.	The options.....	47
2.	Pre-screening criteria	47
3.	Outcomes.....	48
4.	The final set of options.....	50
Annex 2 Detailed assessment of the remaining five options		52
1.	Operations	52
1.1.	Reliability and quality of service	52
1.2.	Providing adequate management services to Member States authorities, including specific needs of users (Member States).....	53
1.3.	Ensuring flexibility to add other existing and potentially new systems.....	55
1.4.	Capacity to provide the required security levels	56
1.5.	Responsiveness to emergency requirements	57
1.6.	Capacity/flexibility to incorporate new technology and to react to changing demands	58
1.7.	Ability to recruit and retain key skills.....	60
1.8.	Length of time to develop and implement the option	62
2.	Governance	64
2.1.	Responsiveness to the requirements and views of Member States, the Commission and the European Parliament	64
2.2.	Transparency (accountability, decision-making) vis-à-vis citizens and the system's users and supervisory bodies.....	68
2.3.	Effectively adding new Member States	70
2.4.	Responsiveness to the requirements and views of other stakeholders.....	71

2.5.	Degree to which alignment with JHA policy and a broader EU policy is enabled....	73
2.6.	Incorporating ‘Géométrie variable’	75
3.	Finance	77
3.1.	Implementation costs	77
3.2.	Critical mass: exploiting synergies	77
3.3.	Ability to acquire the right funding levels and resources	81
3.4.	Transition costs	83
3.5.	Access to additional funding for incidental extra costs	86
3.6.	Ability to make the necessary investments (OPEX and CAPEX)	88
4.	Legal.....	89
4.1.	Effectiveness in ensuring fundamental rights and freedoms, in particular protection of personal data, respect for private and family life and right to an effective remedy	89
4.2.	Effective liability and redress provisions.....	93
4.3.	Weight of legal requirements to establish effective management	95
4.4.	Avoiding function creep (de jure and de facto)	96
Annex 3 Risk Assessment		99
1.	Baseline	99
2.	Regulatory Agency.....	100
Annex 4 Joint statements of the long-term management of SIS II and VIS STATEMENT 235/06.....		102
Annex 5 Description of the SIS, SIS II, VIS and EURODAC.....		103
1.	SIS and SIS II.....	103
2.	VIS	105
3.	EURODAC	106
Annex 6 Administrative costs		108

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT¹

1. TITLES OF PROPOSALS

Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom security and justice

Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty

2. DOCUMENT REFERENCE NUMBER

COM(2009)...final

Agenda planning reference number: 2008/JLS/018

3. INTRODUCTION

The legal instruments establishing SIS II² and VIS³ entrust the Commission with the operational management of the SIS II and VIS during a transitional period with the possibility to confer some of the tasks related to operational management on national public sector bodies in two Member States. The same legal instruments also provide for the location of the systems in France and Austria. They do not, however, establish which entity should be responsible for long-term management.

The Council and the European Parliament, in joint statements attached to the SIS II and VIS legal instruments, invited the Commission, after completion of an impact assessment containing a substantive analysis of alternatives from the financial, operational and organisational perspective, to present the necessary legislative proposals entrusting an Agency with the long-term operational management of the Central SIS II and parts of the Communication Infrastructure as well as VIS. The statement attached to the VIS Regulation stipulates that the impact assessment for the management of VIS may form part of the impact assessment carried out for the

¹ The Impact Assessment report was adopted by the Impact Assessment Board in March 2008. Therefore, it does not cover the legal developments after that date.

² Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) and Council Decision 2007/533 JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)

³ Regulation (EC) No 767/2008 of 9 July 2008 of the European Parliament and the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

management of SIS II.⁴ In these statements the Commission committed itself to presenting, within two years of the entry into force of the SIS II and VIS legal instruments,⁵ (i.e. by the end of 2008) the necessary legislative proposals to entrust an Agency with the long-term operational management of these systems.

The transitional period should be no longer than five years from the date from which the SIS II legal instruments apply⁶ and the VIS Regulation enters into force⁷ (i.e. it shall finish by 2012). In order for the Agency to be entrusted with the operational management of SIS II and VIS by 2012, negotiations on the legal instruments establishing the Agency should be concluded by 2010.

EURODAC⁸ is currently managed by the Commission and as such does not require a change to its management structure. However, a technical assessment carried out in 2005 indicated that EURODAC would need to be upgraded in terms of capacity by 2008/2009 after the new Member States joined the European Union (EU) in 2004 and 2007. Managing EURODAC, VIS and SIS II together could create substantial synergies and economies of scale. The biometric matching functionality (in the form of the service-orientated architecture of the Biometric Matching System (BMS)) will in the first instance be made available for the VIS. It is likely to be provided at a later stage for SIS II and EURODAC. Accordingly the management solution for EURODAC has been also reviewed in this impact assessment. The SIS II and VIS legal instruments foresee the establishment of a Management Authority for these systems. Therefore, the necessity of establishing it is not assessed as such in this Impact Assessment. The objective of this impact assessment, rather, is to find the most efficient long-term management solution for SIS II, VIS and EURODAC. Since SIS II and VIS are not operational as of yet, the interim solution for the management of the systems, i.e. the Commission entrusting the management tasks to Member State authorities, has been identified as the baseline option (Baseline). However, since the interim management structure itself is not yet in place, it is difficult to acquire exact figures and this impact assessment is mainly based on indicative figures.

Annex 5 describes the above-mentioned systems in a detailed manner.

4. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

4.1. Approach and methods applied

The data-gathering and a large part of the consultation were undertaken through an external study (hereinafter referred to as “the external study”) contracted by the Commission in January 2007. The external study constitutes the main support for this Impact Assessment Report. The problem, objectives and policy options assessed were based on the report from the contractor and on the basis of a desk analysis of appropriate analytical methods and applicable legal documents.

⁴ See Annex 4 for the text of the statements.

⁵ The SIS II Regulation entered into force in January 2007.

⁶ Recital 9 of the SIS II Regulation and Decision

⁷ Recital 4 of the VIS Regulation

⁸ Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention.

An Inter-Service Steering Group, composed of the relevant Commission Directorates General⁹ was set up to support the impact assessment process. The group met in June 2006 to discuss the terms of reference for the preparatory study for the Impact Assessment, prior to its externalisation. The members of the Steering Group were subsequently consulted in writing on each deliverable of the external contractor and on the Impact Assessment Report itself.

The assessment process consisted of two steps: first, the options were assessed with regard to their legality, acceptance by the stakeholders and their ability to include VIS and EURODAC; secondly, on the basis of this pre-screening, five options were identified and evaluated in further detail. A detailed description of the pre-screening process can be found in Annex 1.

The Commission's Impact Assessment Board (IAB) was consulted in March 2008. The Board found that the Impact Assessment report develops a good set of policy options and assesses these on all relevant dimensions. It recommended: a) to improve the methodology used to score the various policy options; b) to assess two options rather than one in further detail; c) to better explain and quantify the occurrence of synergies; and d) to present the procedure and the main results of the various consultations that were carried out in preparing the Impact Assessment report. All these comments have been taken into account in the relevant sections of this Impact Assessment report.

4.2. Stakeholder consultation

The options that were subject to an initial assessment were identified on the basis of discussions on SIS II in the Council working parties.

Twenty seven interviews were conducted by the external contractor in the framework of the preparatory study, involving representatives from the EU Member States, Norway, the European Parliament, the Commission, the European Data Protection Supervisor, the Schengen Joint Supervisory Authority, the European Environmental Agency, FRONTEX, Europol, the Strasbourg C.SIS site responsible for the management of SIS 1+ and industry experts.

The presidencies of the EU between January 2007 and June 2009 (Germany, Portugal, Slovenia, France and the Czech Republic) and those Member States that are hosting and managing the systems (France and Austria) were interviewed. Member States experts were asked specifically to comment on different management structures, their prioritisation of expected impacts, their concerns and constraints, and their requirements for effective management of SIS II. The representative of Norway was asked in particular about the issues linked to the status of the associated countries. The majority of interviewed Member States were of the opinion that the best solution is to establish a new Regulatory Agency. Strong disapproval was voiced over two options: management by the Commission and by one Member State on behalf of all. Moreover, some Member States stated that the competences of the management authority should not be limited to technical operational matters and that the authority should have the mandate to develop its own IT strategy. Almost all

⁹ DG JLS, DIGIT, ENTR, SG, LS, BUDG.

Member States shared the opinion that all JHA systems should be managed by the joint authority.

Consultation also included the SIS II and VIS *rapporteurs* on behalf of the European Parliament, representatives of the European Data Protection Supervisor and the Schengen Joint Supervisory Authority and addressed in particular the following issues: application of the relevant data protection provisions, and the data protection cultures within the institutions which have been proposed to manage the systems.

Representatives of the European Environmental Agency and of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) were interviewed to establish best practices in the governance of Regulatory Agencies, especially concerning activities in non-EU Member States and ways to engage different stakeholder constituencies. Further analysis of EU agencies was conducted to assess the desirable task allocations between the Management Authority and the Commission. Interviewees highlighted that, although existing agencies already have the necessary infrastructure in place, the costs of setting up a new Agency would be similar to the expenditure needed for making adjustments to the existing agencies. Financial autonomy is of critical importance for a newly established Management Authority. Additionally, recruitment may prove rather time-consuming, as very specific expertise is necessary to operate IT systems such as SIS II, VIS and EURODAC.

Interviews were conducted with experts from industry. The latter enabled the inclusion of the suppliers' perspectives of systems and infrastructure, and those of software vendors involved in the development, management and maintenance of large-scale IT systems.

Finally, visits were made to the C.SIS site in Strasbourg and to Europol in The Hague. The visit to Strasbourg focused on operational matters and assessed basic facilities; the Hague visit reviewed the ability and appropriateness of Europol's potential role in managing SIS II and other European large-scale IT systems. Based on the opinion of the majority of interviewed stakeholders, it was concluded that Europol, in its current form, is not well placed to manage SIS II, VIS, EURODAC or BMS. A review of the legal basis of Europol and of the building specifications for the new Europol facility should be carried out before this option could be given further consideration.

5. PROBLEM DEFINITION - CHALLENGES

Currently, only EURODAC is operational and managed by Directorate General DIGIT and Directorate General Justice, Freedom and Security (JLS) of the Commission. The system is located in Luxembourg and in Brussels. The technical assessment carried out in June 2005 identified the need to upgrade the system in terms of capacity after the accession of new Member States in 2004 and 2007. The envisaged upgrade mainly concerns system capacity: due the constant increase in data to be managed, some system devices are working close to maximum capacity and need to be upgraded or replaced. For the same reason, the data synchronisation between the EURODAC Production System and the Business Continuity System

takes several hours and needs to be improved by more efficient data synchronisation technologies and devices.

SIS II and VIS are being developed by the Commission.¹⁰ The legal instruments establishing and governing SIS II (adopted in 2006 and in 2007) and VIS adopted in July 2008¹¹ foresee that the systems shall be located in Strasbourg in France (central unit) and near Salzburg in Austria (back-up unit). The development of the systems in these locations is ongoing.

The systems cannot function without a long-term central Management Authority to ensure continuity and operational management of the systems, and the permanent flow of data.

The nature of the Management Authority is not specified in the legal instruments. However, in joint statements to the SIS II and VIS legal instruments, the Council and the European Parliament agreed that the Management Authority should be "an Agency".

The Management Authority will need to be able to address a number of specific challenges. They can be categorized under the headings of: financial, governance, legal and operational.

5.1. Operational

5.1.1. Ensuring effective management of the systems, taking into account their critical character and their 24/7 availability;

The systems under scrutiny are critical for ensuring a high level of security in the area of freedom, security and justice in which internal border controls have been lifted. Effective management, guaranteeing their uninterrupted availability, is of the utmost importance.

There are several requirements which have an impact on system effectiveness and in ensuring system availability. First of all, the management must be flexible in its access to funds, skills and equipment. Lengthy decision-making procedures should therefore be avoided. Solutions that provide more autonomy, flexibility and co-location of the systems and their management are likely to be the most effective.

The impact of 24/7 operations must not be under-estimated in terms of staffing. If, for example, there is a requirement for 24/7 security management that translates roughly (depending on the labour legislation for the site in question) into 5-7 full-time posts for one profile, then the logic of applying synergies is evident.

¹⁰ Although SIS I is being run and managed by France (located in Strasbourg), it is considered as a different system to the SIS II due to the differences between the two systems in architecture and financing.

¹¹ Article 26(1) of the VIS Regulation provides: "After a transitional period, a Management Authority (the 'Management Authority'), funded from the general budget of the European Union, shall be responsible for the operational management of the Central VIS and the National Interfaces." Article 15 of the SIS II legal instruments provides: "After a transitional period, a Management Authority (the 'Management Authority'), funded from the general budget of the European Union, shall be responsible for the operational management of Central SIS II."

Continuity depends on the sustainability of the organisational structure, the robustness of the systems and infrastructure, guarantees for long-term financing and the ability to retain key expertise and skills.

Environments that have the relevant expertise are likely to provide the best guarantees with regard to ensuring the security of the data. Nevertheless, effective security must also be built into the systems themselves and be appropriate to the system requirements, the users and the data subjects. It should also be taken into account that existing organisations may have legacy systems and processes that are not adaptable to the specific needs of these systems. With regard to physical security, a custom-built facility is likely to best address the security requirements of the systems.

The management solution should also be suitable for managing other existing and potentially new systems in the area of, freedom, security and justice.

5.2. Governance

5.2.1. Need to ensure that the views of all stakeholders are taken into account and that the roles of the EU Institutions are ensured

SIS II, VIS and EURODAC have different stakeholders. On the one hand, the Management Authority must be responsive to the requirements of the users of the systems (in particular Member State authorities); these include security, continuity and quality of service. On the other hand, the Commission, based on the provisions of the Treaty establishing the European Communities, is under an obligation to ensure the correct implementation of the EU budget. The Commission must also ensure that the systems operate in such a way as to support underlying EU policies.

As a co-legislator, the European Parliament must be able to exercise its role of democratic supervision over the legislative process and to ensure that the Management Authority supports EU policies for the benefit of citizens and guarantees the respect for fundamental rights and freedoms. As a budgetary authority, the European Parliament's role is mainly to supervise budgetary expenditure, in order to ensure the accurate and responsible use of EU resources.

5.2.2. "Géométrie variable" - heterogeneous group of participating countries (EU Member States with different levels of participation and associated countries)

SIS II, VIS and EURODAC involve both EU Member States and associated countries (Norway, Iceland, and in the future Switzerland and Lichtenstein). At the same time, some of the Member States (UK and Ireland) participate only partly in the systems or only in some of them or on a different legal basis (Denmark). The Management Authority will need to accommodate these different statuses and horizontal issues relevant to all three systems, whilst at the same time ensuring effective decision-making. This problem may become even more acute with the addition of new systems.

The multi-pillar structure, currently applicable in the area of, freedom, security and justice, will be discarded once the Treaty of Lisbon enters into force. However, the new Treaty will not significantly simplify the situation with regard to the different levels of participation of the UK, Ireland and Denmark. Under the Treaty of Lisbon,

Ireland and the UK will have the possibility to opt out from the entire area of freedom, security and justice and they will be able to choose whether to opt in or out of any individual proposal. Denmark will continue with its existing opt-out from freedom, security and justice. It will be able either to change from a complete opt-out to the case-by-case opt-in applying to Ireland and the United Kingdom. Additionally it will be able to renounce entirely its opt-out (and thus align its position with that of the 24 Member States) whenever it wishes. The Danish government has the freedom to decide if and when, this change should take place, in accordance with its constitutional requirements.

5.3. Financial

5.3.1. Need to ensure (cost-) efficient management

An efficient Management Authority would need to ensure that overall running costs are kept as low as possible and that the productivity of staff and equipment are as high as possible. Thus overhead costs should be kept to a minimum. The management requirements of only one large-scale IT system would most likely not justify many of the overhead functions such as legal support, administration, human resource planning, reporting and relationship management, on-site security, etc. Adding more systems and increasing the scope of the Management Authority's work (e.g. including system development) would increase the operational base and better justify managerial overheads.

Should remote management be considered as an option, namely that the management roles and functions are not on-site, this may lead to extra coordination costs, travel costs and time lost in travelling between the separate locations. It could also result in delays in technical interventions. An extra layer of limited management costs, in addition to the actual operational management at the facility, would occur.

The best way to improve productivity and reduce operational costs is to exploit synergies. This would become possible if all three systems, and possibly other systems, were housed in one location, under one management and running on the same platform. SIS II and VIS share a common technical platform and it is envisaged that the biometric matching functionality will be common to SIS II, VIS and EURODAC. The technical synergies applied during the system development phase will have a knock-on effect during operations, particularly in the area of training, staffing, incident management and maintenance, where knowledge and expertise acquired and deployed for SIS II will also benefit VIS. For example, the SIS II security manager profile could also manage VIS security. If the biometric component of VIS is deployed at a later stage for SIS II and possibly EURODAC, similar synergies and economies of scale will apply from development through to operations.

The cost linked to the physical location of the systems may be substantial. SIS II and VIS are being developed in Strasbourg in France (central unit) and near Salzburg in Austria (back-up unit) in accordance with the SIS II and VIS legal instruments that provide for these locations. The site for hosting SIS II and VIS in France is offered by the French authorities free of charge (the Commission pays only for the office space). Relocation would imply short-term transitional costs, which, however, would be somewhat offset in the long term by the fact that custom-built facilities would

meet all the infrastructure and logistic requirements, including a provision for growth over a certain number of years. This approach would also avoid having to resort to piecemeal solutions, in order to respond to current and future capacity requirements. There is also the possibility that the new facility could be offered, as is currently the case in France. The current hardware is expected to become obsolete in five to six years; thus by 2012 the hardware would also need to be replaced irrespective of whether relocation is involved.

5.3.2. *Need to ensure timely and adequate funding*

Ensuring timely and adequate funding is of the utmost importance for keeping the systems operational and providing a high quality of service. Access to adequate funds would allow use of technology best suited to users' needs. Moreover, given the critical character of the systems, it should be possible to quickly acquire additional resources in case of emergency without long decision-making processes.

In order to ensure sufficient democratic control over the expenditure of the Management Authority, the budget allocation methodology should be transparent.

From a financial point of view, a combined management of first and third pillar activity seems to be unproblematic, as the Financial Regulation applies to all EU budget expenditure and covers both activities.

5.4. **Legal**

5.4.1. *Importance of effective data protection and supervision*

Effective implementation and enforcement of data protection rules must be ensured. The SIS II, VIS and EURODAC legal instruments contain specific data protection provisions applicable to SIS II, VIS and EURODAC. Compliance with data protection requirements laid down in the specific legal instrument(s) for each system has to be ensured under every option. Supervision by the European Data Protection Supervisor should be facilitated and effective remedies must be in place. Nevertheless, different management structures may inherently have varying data protection cultures and would therefore be more or less well-equipped to ensure proper implementation of data protection provisions. Under any of the options, data from the systems would be logically separated from each other and would therefore not be merged into one "pool".

Based on interviews with data protection authorities, the following is a non-exhaustive list of conditions that are likely to support an organisation's ability to ensure effective implementation of data protection provisions and enforcement of data subjects' rights:

- Having one legal regime covering all the activities of the Management Authority and all systems under its control;
- Having one supervisory authority – with unrestricted access – covering all the activities of the Management Authority and all systems under its control;
- Supporting the need for an effective and accessible remedy for the data subject, including third country nationals;

- Providing sufficient funds for data protection compliance and ensuring that the technology is used in a way that best guarantees data protection compliance.

5.4.2. *Importance of effective mechanisms and redress for abuse or faults causing damage*

The management of large IT systems such as SIS II, VIS and EURODAC (including the processing of data requiring a high degree of protection) necessitates appropriate provisions to deal with liability issues. In order to comply with its obligations, the Management Authority must be able to act accordingly to redress an abuse, pay compensation and ensure its judicial accountability. Given that data is introduced, modified, added to, corrected, updated and deleted by Member States, the Management Authority should not be made liable for the data itself, but for damages resulting from failures in its management, such as the culpable failure of the communication network, information leaks or from a breach of contract with respect to sub-contractors.

5.5. **The need for EU action**

5.5.1. *Subsidiarity*

The SIS II, VIS and EURODAC legal instruments deal with the issue of subsidiarity, as they clearly define that the national systems will not fall under the responsibility of the Management Authority.

5.5.2. *Added value of EU action*

The objective of establishing a Management Authority responsible for SIS II, VIS and EURODAC cannot be achieved by the Member States alone. Owing to the very nature of large-scale, Europe-wide IT systems and by the reasons of scale and impact of the action, management of these systems can be better achieved at Community level. Without going into a detailed analysis of technical and organisational changes required, the development of a service-oriented architecture of these IT systems would help to maximise synergies and control investment at a realistic level. Managing applications in a single organisational environment is a way of sharing functions in a flexible and cost-efficient way. The daily management of these systems together, in a single organisation, would also bring about significant synergies. A dedicated, specialised organisation would also ensure the highest level of efficiency and responsiveness to the requirements of Member States and other stakeholders.

5.5.3. *Proportionality*

The Management Authority, financed from the general budget of the EU, would be given the competences to manage only the central unit, without having responsibility for the data entered in the systems. Therefore, the central authority's competences are kept to the minimum necessary for supporting effective, secure and continuous data exchange between the Member States. Setting up a dedicated structure should be considered proportionate to the legitimate interests of users and the high-security, high-availability and mission-critical nature of the systems. The activities of the Management Authority are limited to the operational management of SIS II, VIS and EURODAC. Member States are competent for their national systems.

6. OBJECTIVES

The general objective is to establish an appropriate solution for managing SIS II, VIS and EURODAC in the long-term. This solution should meet several specific requirements or objectives.

The table below lists the specific objectives that the Management Authority is to achieve and matches these to the issues that it needs to address, as described in the previous section. Annex 2 contains a more detailed assessment across the criteria.

Table 1. Categorization of specific objectives and issues that need to be addressed by the new Management Authority for SIS II, VIS and EURODAC

Categories	Issues	Objectives	Assessment criteria
Operational	Ensuring effective management of the systems, taking into account their critical character and their 24/7 availability.	Ensuring that the management of the systems will be effective in guaranteeing operational continuity and uninterrupted service, data integrity and security and that it is carried out by a public sector body capable of delivering the quality of service required by the users for each system.	<ul style="list-style-type: none"> - Reliability and quality of service - Providing adequate management services to Member States authorities, including specific needs of users (Member States) - Ensuring flexibility to add other existing and potential new systems - Capacity to provide the required levels of security - Responsiveness to emergency requirements - Capacity/flexibility to incorporate new technology and to react to changing demands - Ability to recruit key skills - Length of time to develop and implement the option
Governance	Current absence of a long-term management solution for SIS II and	Establishing a management and governance structure	<ul style="list-style-type: none"> - Governance which is responsive to the requirements and

	<p>VIS, and likely future needs for a long-term management solution for EURODAC.</p> <p>"<i>Géométrie variable</i>" - heterogeneous group of participating countries (EU Member States with different levels of participation and associated countries).</p>	<p>for SIS II, VIS and possibly other large-scale IT systems in the area of freedom, security and justice that is transparent and accountable to supervisory bodies (European Parliament, Court of Auditors, etc.) and the public at large and provides effective control to a heterogeneous set of participating countries and the Commission in their respective roles.</p>	<p>views of Member States, the Commission and the European Parliament</p> <ul style="list-style-type: none"> - Transparency vis-à-vis citizens, users of the system and supervisory bodies - Effectively adding in new Member States - Responsiveness to the requirements and views of other stakeholders (e.g. suppliers, civil society) - Degree to which alignment with the JHA and a broader EU policy is enabled - Incorporating "<i>Géométrie variable</i>" constraints
Financial	<p>Need to ensure (cost-) efficient management.</p> <p>Need to ensure timely and adequate funding.</p>	<p>Ensuring sound, continuous, efficient and accountable financial management of SIS II, VIS and possibly other large-scale IT systems in the area of freedom, security and justice,, which optimises savings and economies of scale resulting from synergies.</p>	<ul style="list-style-type: none"> - Limiting implementation costs - Critical mass: exploiting synergies - Ability to acquire the right funding levels (running costs) - Limiting transition costs - Access to additional funding for incidental extra costs - Ability to make the necessary investments
Legal	<p>Importance of effective data protection and supervision.</p> <p>Importance of effective mechanisms and</p>	<p>Guaranteeing that management and governance procedures and structures ensure appropriate data</p>	<ul style="list-style-type: none"> - Effectiveness in ensuring fundamental rights and freedoms, in particular protection of personal

	redress for abuse or errors causing damage.	protection and/or liability mechanisms, whilst acknowledging foreseen changes resulting from the planned entry into force of the Lisbon Treaty.	data, and right to an effective remedy <ul style="list-style-type: none"> - Suitable liability provisions - Guaranteeing the avoidance of function creep - Weight of legal requirements to establish effective management
--	---	---	---

7. POLICY OPTIONS

Following a pre-screening of options, as described in Annex 1, a list of five policy options for the long-term operational management of SIS II, VIS, EURODAC and possibly other IT systems in the area of freedom, security and justice, is presented.

All the options with the exception of Europol in its current form (until 2010) will be financed from the general budget of the European Union.

7.1. Option 1 – The Baseline option

The legal instruments governing SIS II and VIS entrust the Commission with the responsibility for interim management of the systems.¹² The management set-up for SIS II and VIS during the transitional phase, before the long-term management solution is established, would be continued as a permanent solution with management functions performed by the Commission, which would entrust two Member States with operational management tasks. EURODAC's day-to-day operational management set-up would also remain as it is, under the responsibility of the Commission.

The two Member States carrying out the management tasks would be paid a negotiated fee for the use of their facilities and for the operational management tasks. A continuation of the interim management solution would require a renewal of the contract entrusting the Member States with operational management. The Commission would remain responsible and accountable for the management of the large-scale IT systems, while the Member States would remain responsible for day-to-day operational management tasks.

¹² The Commission may delegate operational management tasks and tasks relating to implementation of the budget, in accordance with the Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities (1), to national public-sector bodies, in two different countries – Art. 15(4) of the SIS II legal instruments and Art. 26 of the VIS Regulation

7.2. Option 2 – The Baseline+ option

The Commission would entrust the management of SIS II, VIS and EURODAC to Member States' authorities. Option 2 is therefore very similar to the Baseline option, with one main difference: operational management tasks for EURODAC would also be entrusted by the Commission to the two Member States. If in this case EURODAC were to be transferred to the Member States' facilities, more funds would be needed (as there would be an increase in expense) in order to relocate it. This option would require certain legislative changes as the EURODAC Regulation does not foresee entrusting operational management tasks to a Member State.

7.3. Option 3 – New Regulatory Agency

This option envisages the creation of a new Regulatory Agency which would assume responsibility for the long-term management of the SIS II, VIS, and EURODAC. The total cost of setting up and running a new Regulatory Agency would depend on its location and, in particular, on whether or not there is a need for a new custom-built facility. Regulatory agencies are usually governed by a Management Board¹³. Day-to-day management is carried out by the Director and the Management Board. In order to address issues arising from the different constituencies of the three systems, it would be necessary to consider establishing a form of advisory group(s) to support the Management Board on system-specific issues. Given that the Regulatory Agency would have a legal personality it should be independent with respect to technical matters and have legal, administrative and financial autonomy. The Agency could also be made responsible for the development and for the management of other large-scale IT systems. Its responsibilities could further include some of the more technical issues covered by the implementing measures in the legal instruments establishing the systems.

7.4. Option 4 – FRONTEX

This option foresees handing over management of the three systems to FRONTEX. Efficient management of the systems by FRONTEX would most probably require relocating SIS II, VIS and EURODAC to the FRONTEX site or to a facility nearby.

One implication of this option would be the need to change the FRONTEX governance structure to better deal with issues regarding each of the three IT systems. In order to accommodate the inclusion of SIS II, VIS and EURODAC into the FRONTEX management structure, the FRONTEX Regulation would have to be amended. In order to create effective institutional structures for the operational management of the large-scale IT systems, a new specialist department would have to be created within FRONTEX.

7.5. Option 5 – Europol for SIS II and Commission for VIS and EURODAC

Under this option Europol – (currently) a third pillar Agency – would be responsible for managing SIS II and the Commission would manage VIS and EURODAC. The option Europol for all three systems was discarded in the pre-screening process (see

¹³ Communication from the Commission to the European Parliament and the Council, "European agencies – The way forward", COM(2008) 135 final

Annex 1), as at the time the Impact Assessment study was conducted, it was not certain that Europol would become a Community Agency.

Hypothetically, there could have been two ways to accommodate SIS II long-term management in Europol's organisational structure (in force until 2010): Europol could integrate the management of SIS II into one of its departments or a new department could be set up. The latter would be seen as more favourable as it would separate Europol's traditional work from management of SIS II. Another issue to be taken into account is that Europol is located in The Hague and that the relocation of SIS II may be necessary.

Establishment costs related to the necessary transfer of SIS II to the Europol premises could be mitigated if it is adequately planned in the design of the new Europol facilities, anticipated by 2011. The currently applicable Europol Convention provisions do not adequately involve the relevant European Union stakeholders: European Parliament, the Commission, European Data Protection Supervisor or the European Court of Justice.

However, in April 2008 the Council reached political agreement on a proposal for the Decision replacing the Europol Convention. Once applicable in its entirety, as of 2010, significant changes will be introduced in the governance and financing of Europol. However, as negotiations on the new legal basis were ongoing at the time when this Impact Assessment was compiled, the latter only assesses possibilities under the Europol legal framework applicable until the end of 2009.

8. ANALYSING IMPACT AND COMPARING OPTIONS

A traditional impact assessment analyses the economic, environmental and social impacts of different options. However, for the purpose of this impact assessment, specific categories of impact were developed to facilitate an appropriate assessment of the key legal and political issues, as well as the operational and organisational challenges.¹⁴ It is the existence of the systems themselves that may have economic, environmental and, most of all, social impacts. The establishment of the Authority that would manage the systems is not likely to produce any additional significant impacts under these categories. All the systems have an impact on problems such as crime, terrorism, security and fundamental rights. However, their mode of management will not be a differentiating factor between the scales of these impacts.

The following categories of impact criteria were used:

- (1) operational – discusses the effectiveness of management in dealing with procurement, technological requirements, emergencies, providing services to Member State users, etc.;

¹⁴ These criteria correspond to the ones identified in the joint statements of the Commission, the Council and the European Parliament to the SIS II and VIS legal instruments, which specify that the impact assessment should contain a substantive analysis of alternatives from the financial, operational and organisational perspective.

- (2) governance – concerned with accountability of management and the level of control that the EU institutions and Member States may have over management decisions;
- (3) finance – deals with efficiency of operations and ability to assure adequate funding;
- (4) legal – ensures legality of the options and availability of guarantees for data subjects and users.

Under each of these headings criteria were applied to determine the expected individual performance of each option, providing a comparison between them.

The assessment criteria have been listed in Table 1 on pages 22-23. A more detailed description of the impacts and the assessment of the options can be found in Annex 2.

8.1. Operational

8.1.1. Baseline and Baseline +

The current dedicated facility and staff in Strasbourg have a track-record in running SIS I. However, France is running SIS I on an inter-governmental basis. Although the Commission is currently running some IT systems, including EURODAC, management of such systems is not its core task.

Under the Baseline and Baseline+ option, France and Austria would run the systems on behalf of the Commission. A challenge with this option is that the Commission would be controlling the operational management tasks carried out by Member States' public bodies from another location. This may complicate decision-making, particularly in emergency situations.

The Baseline and Baseline+ options would allow continuity in operations and planning, nevertheless in the case of Baseline+, the relocation of EURODAC to the SIS II and VIS location would have to be considered.

Under Baseline options, SIS II and VIS would be located in facilities equivalent to secure bunkers, ensuring sufficient security.

The facilities in Strasbourg and near Salzburg are not future-proof however, and would need to be expanded or replaced if new systems were to be added.

Until now, the facility in Strasbourg has been deeply rooted in the French and European law enforcement community. It would therefore need to adjust to the VIS and EURODAC environments and respective stakeholder requirements. The two layers of management (the Commission and Member States) increase the distance between the management, service providers and users.

The possibility of acquiring highly specialised personnel is rather limited, due to the Commission's recruitment rules and procedures, which favour generalists rather than specialists. However, the recruitment could be delegated to the national public authorities.

This option would not require a long time to be implemented.

8.1.2. *Regulatory Agency*

The Regulatory Agency would allow dedicated, tailor-made solutions in managing SIS II, VIS and EURODAC. Its primary objective would be to provide the best quality continuous service to users.

The Agency would be governed by a Management Board, where Member States would be represented. This option would therefore ensure that the views of the Member States as users of the systems are sufficiently taken into account in the decision-making process.

Initially, the Management Board structure (reflecting the variety of the systems and the "*géométrie variable*") may complicate rapid decision-making, but a new Agency should be able to develop effective mechanisms to deal with emergencies, once it is operational.

The combination of management and development of several IT systems would enable expertise to be pooled. The new Agency would therefore have the potential to become a centre of excellence, well suited to incorporating new technology and responding to changing demands.

When acquiring facilities for the new Agency, the space and infrastructure needed for the development and management of new IT systems could be taken into account. Security would also be built into the organisation, the processes, as well as the facilities hosting the systems from the outset.

Although the Agency would have to comply with EU staff regulations, it would be able to hire more 'temporary and contract agents' than the Commission services and could offer them contracts of unlimited duration.

The process of establishing the Agency from the beginning would take a considerable time (see also section 8.4 for the time required for the adoption of the necessary legal instrument(s)).

8.1.3. *FRONTEX*

Should FRONTEX manage the three systems, it would have a dedicated department created solely for this purpose and a special configuration of the Management Board.

Since it is already an existing Agency, some of the existing departments, such as administration, finance and procurement could be shared. This could save time in comparison with establishing a new Agency. As is the case for the new Agency option, FRONTEX also has a certain amount of flexibility in hiring new staff.

Running SIS II, VIS and EURODAC together would put the organisation in a stronger procurement position, as larger contracts may attract bids of higher quality, allowing more optimal outcomes.

Currently, FRONTEX does not have experience in handling critical high-availability IT systems. The security infrastructure and expertise to provide and ensure the expected quality of service levels would also need to be put in place.

As is the case for Europol, adding new systems (in the area of law enforcement) would require a strong shift of focus towards IT management, which is not among the original objectives of FRONTEX. Adding more IT systems would mean distancing the organisation from its initial objective of strengthening cooperation on external borders. Consequently, the perception of the core tasks of the organisation among its key stakeholders and among the public at large could also change.

Finally, an important element to note is that, to date, FRONTEX has not yet signed the Headquarters' agreement with the hosting Member State.

8.1.4. Europol

Europol is well adjusted to understanding and servicing the needs of the law enforcement community but neither management of IT systems for external borders nor asylum is a priority for the organisation. So far, Europol has not been tasked with providing high-reliability services nor with guaranteeing mission-critical functions on a 24/7 basis, which are necessary for SIS II, VIS and EURODAC.

Decision-making on IT strategy has thus far proved difficult. This would have to be improved for making coherent decisions for, and subsequently taking, rapid actions. Moreover, adding new systems would require a strong shift in focus towards IT management, which is not part of Europol's original objectives. Adding IT systems would mean distancing the organisation from its initial objective of supporting police co-operation. Moreover, the perception of the core tasks of the organisation among its key stakeholders and among the public at large could also change.

Moving the systems may be necessary, in order to allow effective management and exploitation of synergies with Europol's IT department.

Physical security on Europol's premises provides an appropriate environment for a high-security system such as SIS II.

Until 2010 Europol has its own staff regulations and is not bound by the rules applicable to Commission staff. This provides Europol with some flexibility in hiring staff.

A substantial amount of time would need to be invested, in order to implement this option.

8.2. Governance

8.2.1. Baseline and Baseline+

In the cases of the Baseline and Baseline+, the representation of users would be indirect, via the Commission, as it would take place, in particular, in the framework of comitology committees. The European Parliament would have an important role, as the Commission is accountable to it. However, in practice, effective control may

be problematic due to the fact that operational management tasks would in reality be performed by the Member States authorities.

On the other hand, the fact that the Commission would not directly implement the daily management tasks while remaining accountable for them could lead to a decreased level of transparency.

Owing to the wide scope of tasks and given that Member States would be in charge of operational management on behalf of the Commission, this management option would be less recognisable to civil society.

Alignment with policy in the area of JHA and broader EU policy would be ensured, as a result of the Commission's active involvement in management.

The question of '*géométrie variable*' and adding new Member States/users would not be a problem, as there is already an existing framework in the context of comitology.

8.2.2. *Regulatory Agency*

A Regulatory Agency facilitates the appropriate representation of users (especially Member States) in the decision-making structures. The Agency could be given responsibility for deciding on some of the more technical issues covered by the implementing measures in the legal instruments establishing the systems. This would increase the influence of the Member States over operational management in comparison to the Baseline and Baseline+ options.

The Commission's role in the Agency, through its presence in the Management Board as well as influence in particular on the budget and the work programme, would allow the management of large-scale IT systems to be aligned with wider EU policy areas. Furthermore, the European Parliament's tasks of democratic control would be ensured by the institutional mechanisms put in place to meet financial and management reporting obligations to which European agencies are subject.

The Agency would also provide a visible and dedicated structure, which could prove to be a centre of excellence in fostering an active dialogue with user communities, operational constituencies and other industry stakeholders.

A single and dedicated structure would be also more visible and approachable for civil society. It would guarantee simple and transparent management as long as the tasks of the Agency are clearly set.

With regard to the incorporation of the '*géométrie variable*', there would be a need to conclude agreements with third countries participating in the systems. The question of different levels of participation in the three systems could be addressed in the different voting procedures of the Management Board. On the issue of adding new Member States/users, depending on whether they would participate in all or just some of the systems, appropriate solutions would have to be found in terms of membership and voting rights in the Management Board.

8.2.3. *FRONTEX*

For the FRONTEX option, under the current governance structure, the stakeholders (Member States) would retain the possibility of influencing decision-making by the management. The European Parliament would have a similar influence on the decision-making process as in the case of a new Regulatory Agency. FRONTEX could be given responsibility for deciding on some of the more technical issues covered by the implementing measures in the legal instruments establishing the systems. This would increase the influence of the Member States over operational management in comparison to the Baseline and Baseline+ options.

Although FRONTEX is clearly rooted in the area of border control policy, the Commission keeps some competences on the budget, the work programme and the appointment of the Director, which should permit ensuring a sufficient alignment of long-term management of the IT systems with the wider policy areas.

The remit and the governance set-up within this organisation would also have to be adapted to IT management. However, once the IT department had been established, it could become a similar centre of excellence as would be seen in a new dedicated Agency. Management by FRONTEX would ensure a sufficient degree of transparency vis-à-vis citizens, users and supervisory bodies.

Due to its wider remit, FRONTEX could, however, be less recognisable to civil society as the body managing the systems.

FRONTEX has an established system to deal with the '*géométrie variable*' in the context of Schengen cooperation (but not the *Dublin acquis*) but not all the Member States participating in the systems are members of FRONTEX. This would also complicate the addition of new Member States/users.

8.2.4. *Europol*

As regards Europol, until it becomes a Community Agency in 2010, the European Parliament has very limited control powers. Entrusting Europol with the management of SIS II would require the creation of a specific structure, in order to cope with the requirements established in the SIS II legal instruments as regards the powers and responsibilities of the European Parliament and the Commission. Europol could be given responsibility for deciding on some of the more technical issues covered by the implementing measures in the legal instruments establishing SIS II. This would increase the influence of the Member States over operational management in comparison to the Baseline and Baseline+ options.

There are also considerable differences between the competencies of the EU supervisory bodies, in relation to SIS II and Europol, which would result in a more complicated and less transparent structure.

Europol is clearly seen as a law enforcement organisation, which in principle makes it well-aligned with the SIS II constituency. Adding systems from areas other than police co-operation would lead to a change in focus, followed by a changed perception of the organisation. However, given the rather narrow focus of Europol, alignment with the entire JHA remit and wider EU policy would be difficult.

By dividing the management of SIS II, VIS and EURODAC, and entrusting Europol with the management of SIS II only, Europol would have fewer possibilities of becoming a centre of excellence and thus would be less able to interact with suppliers.

Membership of Europol is currently limited to the EU Member States. Specific arrangements through cooperation agreements would be required for the membership of associated countries.

8.3. Financial

The main implementation costs for all the options are connected to the running of the systems and will have to be borne under any of the options. It is assumed that both FRONTEX and Europol would have to hire the same amount of staff and obtain new/additional facilities comparable to those that a new Regulatory Agency would have to acquire. The cost could differ depending on the location. However, since the location has not yet been decided, it is not possible to make such assumptions at this stage. A detailed analysis of implementation costs for the Baseline, the new Regulatory Agency and for the FRONTEX options can be found in section 9.

Operational synergies can be obtained if SIS II, VIS and EURODAC are managed by the same authority. This would, in particular, be the case for Baseline+, a new Regulatory Agency and FRONTEX. Technical, logistical and infrastructure costs, such as power, air-conditioning, data centre structural requirements and physical security of buildings could be shared for the systems. This concerns not only initial capital expenditure but also annual (running) costs.

A management structure responsible for multiple IT systems would be better positioned for procurement, as larger contracts may attract bids of higher quality, allowing more optimal outcomes. Moreover, joint management of the systems would require around thirty percent less operational staff than would be the case if the management of these systems were kept separate.

Ancillary costs, such as training and security would have to be replicated instead of shared. Co-location of network installations would entail synergies in installations, management and monitoring. If SIS II and VIS were dissociated, they could not share the BMS technical infrastructure that was intended to interact with both, as a sub-component. Furthermore, it is unlikely that a centre of excellence could be achieved for one system alone. Separation of these systems would lead to the opportunity cost of not having achieved synergies in expertise and know-how in large-scale IT systems.

All the options under scrutiny would be financed from the general budget of the EU.

8.3.1. Baseline and Baseline +

In case of Baseline+ there would be more overall synergies and economies of scale than in the case of the Baseline option, as a result of common management of all three systems. Current facilities in Strasbourg are not future-proof and adding more systems would certainly require either an extension to the current facilities or the purchase of new facilities.

Both options have a solid financial basis, as the financing of the management of the systems would be part of the general budget with the flexibility to draw on wider Community resources (for example transferring the resources between budget lines).

The Baseline and Baseline+ would have low transition costs, although in the case of Baseline+, relocation of EURODAC could prove to be necessary.

For planning and developing an IT strategy, the Commission is likely to depend largely on the operational management provided by the two Member States. It is further dependent on the IT supplier industry, which should in turn ensure that its IT strategy is accurate and that the necessary investments are well planned.

8.3.2. *Regulatory Agency*

Establishing an Agency for the management of SIS II, VIS and EURODAC has a high potential for exploiting operational synergies which would make it very cost-effective. This can especially be achieved if the management roles and functions are on-site, avoiding thus extra coordination costs, travel costs and time lost in travelling between separate locations. The Agency would have an annual budget, established with full involvement of the main users of the system (Member States' authorities). The budget of the Regulatory Agency would be dedicated specifically to IT-system management tasks, which should allow for transparent allocation of the budget and would dispense with the risk of having to compete internally for financial resources.

The budget provides a fixed framework, but possibilities for acquiring additional funding from the general budget of the EU outside the cycle are limited. This curtails intermediate responses to increases in capital expenditure requirements. However, given the combination of accumulated IT expertise, proximity to suppliers and the users of the systems, the Regulatory Agency would be an effective body for developing accurate IT strategies and for planning the necessary investments.

8.3.3. *FRONTEX*

FRONTEX would have a high potential for exploiting overall operational synergies and in the long-term it would prove to be a cost-effective solution. Some synergies could also occur with the existing structure, in particular in terms of support staff (legal and administrative support).

This option would imply high transition costs, contingent on the location of the systems. These costs could be mitigated, to some extent, by the fact that FRONTEX is a well established Agency and the time needed to become operational or learning curve could be shorter than for an entirely new Agency. However, as co-location of the systems and the management would be more cost-efficient in the long-term, it is likely that the systems would be moved to the FRONTEX location. This would require a new facility because the current FRONTEX facilities would not be appropriate for the management of large-scale IT systems.

Similarly to a new Agency, FRONTEX has an annually fixed budget and limited possibilities for to acquiring additional funding from the general budget of the EU outside the budget cycle.

FRONTEX could build effective planning capabilities by accumulating experience in running three large-scale IT systems. However, its Management Board may be less focused and less capable of deciding on matters concerning operational and technical IT requirements, than the Management Board of a new dedicated Regulatory Agency.

8.3.4. *Europol*

The separate management of SIS II, VIS and EURODAC, which would occur should Europol assume management responsibilities for SIS II, would be undesirable as this would result in a loss of substantial synergies. Given that SIS II and VIS were developed using the same technical platform and that resultant positive knock-on effects are expected in areas ranging from training and staffing through to all operational aspects, costs per individual system would be higher. All roles and functions inherent to an individual system would have to be duplicated. However, some synergies could potentially be found with the Europol IT system.

As in the case of FRONTEX, relocation of the systems would be very likely, which would in turn cause high transition costs.

Currently, Europol is funded mainly from Member States' contributions. The limits of these contributions are determined by Europol's budget, as adopted by the Council. Europol has access to a wider funding base, and should be flexible in generating the required income. However, it does not have the solid backing from the EU budget that the other options have. This will change with the replacement of the Europol Convention by EU legal instruments as of 2010, when Europol becomes a Community Agency and will be financed from the general budget of the EU.

Europol's small operational base may entail less learning experience. Therefore, its capacity for strategic IT planning is expected to be lower than under options where SIS II, VIS and EURODAC are combined. Furthermore, the Management Board of Europol is not well attuned to dealing with technical IT matters.

8.4. **Legal**

The data protection regime is not a point of debate for this impact assessment as this regime has been defined in the legal instruments regulating SIS II, VIS and EURODAC.

8.4.1. *Baseline and Baseline+*

The Baseline option would require minor changes to the SIS II and VIS legal instruments. The Baseline+ option would require modification of the provisions of the EURODAC Regulation.

The Commission has a history of setting data protection standards. It is also under strong public scrutiny to protect fundamental rights of EU citizens and third country nationals residing in the EU. However, during the development of SIS II, the supervision by EDPS has proven to be difficult, due to access restrictions and different security regimes of the local facility and the Commission. Practical and cultural barriers to effective supervision by EDPS may be more likely if SIS II continues to be managed by a Member State where national data protection rules and

national supervisory authorities are prevalent. Any management by the Commission would, in principle, imply jurisdiction of the European Court of Justice and the Court of First Instance, respectively. Thus, even operations mandated to the Member States should be covered by the jurisdiction of the Courts. However, a problematic situation arises where operations carried out by national staff might be challenged. Although the Member States in question and their staff would be entrusted with the management of the systems and act in execution of Community tasks, the scope of the liability of the Community under Articles 288 and 235 of the EC Treaty for acts of Member States is far from clear. Existing case law on the question of 'joint liability' suggests a conflict of jurisdiction, which may be confusing from the claimant's perspective. Management by the Commission entrusting management tasks to the authorities of the Member States could result in the perceived potential risk of unlawful access to and use of data by national authorities, which would, at the same time, be users of the systems. The importance of this impact would depend on the Commission's ability to effectively control the operations carried out by the Member States.

8.4.2. *Regulatory Agency*

This option would ensure that the fundamental rights and freedoms are guaranteed by ensuring the appropriate accountability vis-à-vis the European Parliament, the European Data Protection Supervisor, the Court of Auditors, the European Court of Justice and the Commission. Moreover, the Agency could provide a tailored solution to allow the supervisory bodies to exercise their competencies.

The European Court of Justice and the Court of First Instance would have full jurisdiction over the activities of a Regulatory Agency. The Agency would be a separate legal entity and could be held liable. Due to the "*géométrie variable*", establishing a Regulatory Agency would require adoption of a legislative package consisting of several legal instruments.

The Agency would allow the establishment, from the beginning, of a clear separation of technical and operational staff from policy makers and users of the systems, which would help to avoid function creep¹⁵.

It may take three years to have the Agency fully operational, starting with negotiations on the proposals in the European Parliament and the Council. This estimation is in line with the joint statement by the Commission, the Council and the European Parliament relating to operational management of SIS II and VIS (see Annex 4).

8.4.3. *FRONTEX*

This option would ensure that the fundamental rights and freedoms are guaranteed by ensuring the appropriate accountability vis-à-vis the European Parliament, the European Data Protection Supervisor, the Court of Auditors, the European Court of Justice and the Commission.

¹⁵ 'Function creep' or 'mission creep' is the process by which a system that is designed to perform a certain function is used for other purposes

FRONTEX is under full jurisdiction of the European courts and it can be held liable for its own activities.

Nevertheless, some legislative modifications would be necessary: the FRONTEX Regulation would need to be amended. It is estimated that the adoption of the necessary amendments to the FRONTEX Regulation may require as much time as the adoption of the legal basis for a new Agency. This estimation is in line with the joint statement by the Commission, the Council and the European Parliament relating to operational management of SIS II and VIS (see Annex 4).

FRONTEX does not have access to SIS II, VIS and EURODAC data within the context of its current mandate and therefore the risk of a function creep appears to be more limited than for the other options.

8.4.4. *Europol*

The enforcement of fundamental rights and freedoms by Europol might be problematic due to its limited accountability vis-à-vis the European Parliament, the European Data Protection Supervisor (EDPS), the European Court of Auditors, the European Court of Justice and the Commission owing to its third pillar character. This will change when Europol will start operating as a Community Agency as of 2010.

The EDPS will, as of 2010, have a general supervisory competence over Europol. Until then the dual data protection supervision regime would have been complicated to implement.

The liability rules of Europol are rather complex, involving Member States' national legislation.

If Europol were to manage the SIS II, there could be some perceived risk of abuse and attempts to extend the access to data beyond those that are accessible to Europol in accordance with SIS II legal instruments.

8.5. **Rating of the options**

Under each of the criteria, each option has been allocated 1 to 3 stars. One star (*) denotes weak, two stars (**) stands for medium and three stars (***) marks a good performance. In addition, in each of the categories of criteria, the most important criteria have been identified taking into account the tasks of the Management Authority. These criteria have been marked in **bold** in the table showing the results of the assessment. The table below contains the scoring of different options under each impact category. A more detailed assessment of the options under each of the requirements can be found in Annex 2.

	Option 1	Option 2	Option 3	Option 4	Option 5
	Baseline: COM entrusting Member States with SIS II and VIS	Baseline+:C OM entrusting Member States with all	New Regulatory Agency	FRONTEX for all	Europol for SIS II; COM for VIS, EURODAC
OPERATIONS					
Reliability and quality of service	**	**	***	**	**
Providing adequate management services to Member States authorities, including specific needs of users (Member States)	*	*	***	**	*
Ensuring flexibility to add other existing and potential new systems	**	**	***	**	*
Capacity to provide the required security levels	**	**	***	**	***
Responsiveness to emergency requirements	*	*	***	**	*
Capacity/flexibility to incorporate new technology and to react to changing demands	**	**	***	***	*
Ability to recruit key skills	**	**	***	***	***
Length of time to develop and implement the option	***	***	*	**	**
GOVERNANCE					
Responsiveness to	*	*	***	***	*

	Option 1 Baseline: COM entrusting Member States with SIS II and VIS	Option 2 Baseline+:C OM entrusting Member States with all	Option 3 New Regulatory Agency	Option 4 FRONTEX for all	Option 5 Europol for SIS II; COM for VIS, EURODAC
the requirements and views of Member States, the Commission and the EP					
Transparency (funding, accountability, decision making) vis-à-vis citizens and the system's users and supervisors	**	**	***	**	*
Effectively adding in new Member States	***	***	**	*	*
Responsiveness to the requirements and views of other stakeholders	*	*	***	**	**
Degree to which alignment with the JHA policy and broader EU policy is enabled	***	***	***	**	*
Incorporating 'géométrie variable'	***	***	***	**	*
FINANCE					
Critical mass: exploiting synergies	**	***	***	***	*
Ability to acquire the right funding levels and resources (running cost)	**	**	***	***	**
Transition costs	***	***	*	**	**

	Option 1 Baseline: COM entrusting Member States with SIS II and VIS	Option 2 Baseline+:C OM entrusting Member States with all	Option 3 New Regulatory Agency	Option 4 FRONTEX for all	Option 5 Europol for SIS II; COM for VIS, EURODAC
Access to additional funding for incidental extra costs	***	***	**	**	**
Ability to make the necessary investments (OPEX and CAPEX)	**	**	***	**	*
LEGAL					
Effectiveness in ensuring fundamental rights and freedoms, in particular protection of personal data, right to an effective remedy	**	**	***	***	*
Effective liability and redress provisions	*	*	***	***	*
Weight of legal requirements to establish effective management	***	**	*	*	*
Avoiding function creep (de jure and de facto)	**	**	***	**	*

Following the assessment, a new Regulatory Agency and FRONTEX emerge as the most plausible options.

9. IMPLEMENTATION COSTS OF THE MAIN OPTION

This impact assessment includes an integrated ex-ante evaluation in the context of the Financial Regulation¹⁶, in the form of a cost-effectiveness analysis of the Baseline option and the options that score highest in the qualitative assessment: a new Regulatory Agency and FRONTEX. This approach has been chosen due to the fact that the costs of all the options do not substantially differ from one other. This is explained by the fact that the main costs are connected to management of the systems and would have to be borne under each of the options.

The qualitative analysis under the “finance” heading has demonstrated that all of the options, apart from Baseline and Baseline+, where significant investments have been made by the EU during the interim period, would have high start-up costs. Nevertheless, the other options could provide custom-built facilities, which would constitute a more cost-effective solution in the long-term. In this case, the main costs would be linked to purchasing a new site. In the long-term, however, taking into account the depreciation of the facilities, the differences would disappear and the new facilities may prove to be more cost-effective. The results of the ex-ante evaluation are mainly reproduced in Section 8 of this report and in the financial statement annexed to the legislative proposals.

In this section the option of a new Regulatory Agency is compared to the Baseline option and to the FRONTEX option with regard to managing SIS II and VIS. As the inclusion of managing EURODAC in any of the options would imply similar costs, EURODAC expenditure is deemed neutral across all options and is not accounted for in the assessment below. If the Regulatory Agency option is chosen, EURODAC would have to be relocated. The budgetary implication for moving one system from one site is estimated to amount to €238,112¹⁷.

The risks related to these options have been assessed in detail in Annex 3.

The likely administrative costs incurred by Member States, third countries and the staff in the new Regulatory Agency, are estimated to amount to €62,586 per year. These costs have been assessed for the preferred option only, because the burdens are neutral across all options. Regardless of whether an Agency or the Commission and the Member States are entrusted with the long-term management of these systems, administrative burdens would occur both at management and at national level. The long-term management option, as such, does not entail administrative burdens on citizens or enterprises. A detailed assessment of these costs can be found in Annex 6.

9.1. Assessing the costs

The estimated and assumed costs are based on three categories of expenditure:

Capital Expenditure (CAPEX) are non-recurring costs associated with the purchase of an asset which, according the European Commission’s budgetary procedure, will

¹⁶ COUNCIL REGULATION (EC, EURATOM) No 1995/2006 of 13 December 2006 amending Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities

¹⁷ Based on hardware provider’s estimates for the relocation of SIS II and VIS.

come out of one payment from a year's budget in the year of commitment for that asset. Significant capital expenditure is required for building a new or upgrading a current or future facility to accommodate the systems. A realistic estimate is €7000 per 1m² of new floor space.¹⁸ This figure constitutes a rough average of costs per square meter for constructing a central facility, a back-up facility and office space, which are serviced and equipped. The price is likely to be fairly similar in different locations, the only difference being the price per "empty" (non-equipped and non-serviced) square metre. The total floor space required for a new, purpose-built future-proofed facility for large-scale IT systems is estimated to be 1800m² and would therefore cost an estimated €12,6 million.

Table 9 Capital expenditure – Comparative table: Baseline, new Regulatory Agency and FRONTEX

Cost item	Baseline	New Regulatory Agency with a purchase of a new facility	New Regulatory Agency with a facility made available free of charge by a Member State ¹⁹	FRONTEX ²⁰
Training (initial)	1,494,750	1,377,300	1,377,300	1,377,300
Facilities	4,000,000 Up-grading costs of the facility	12,600,000	4,000,000 Adaptation costs of the facility.	12,600,000 ²¹
Total	5,494,750	13,977,300	5,377,300	13,977,300

Source: cost of facilities based on figures for construction of a UK data centre, 15 August 2007 www.datacenterjournal.com and on space requirements as estimated by JLS.B3 for SIS II, VIS and EURODAC, including a provision for an increase in capacity / the number of systems.

With all three options, there is a need for initial training of the staff. In the case of the Baseline option, this would require twenty-seven training days for 75 persons at a daily rate of €90 (labour costs in France as paid by the Commission²²), plus the trainers' fees at about €300,000. The staff must be fully trained on the SIS II, VIS and

¹⁸ In order to arrive at a realistic figure for the capital expenditure on a brand new facility, recently reported costs for a data centre in London were used as a benchmark for these calculations - Data Centre Journal "New Data Centre in UK" 15th August 2007 available at: http://datacenterjournal.com/index.php?option=com_content&task=view&id=1141&Itemid=41 (visited 13th November 2007).

¹⁹ This is a sub-option of a new Regulatory Agency and not a separate option.

²⁰ Capital expenditure related to management of the relevant systems only.

²¹ If the Member State hosting FRONTEX were to make available a facility free of charge, the cost would be €4 million instead of €12,6 million. However, taking into account that for example FRONTEX does not yet have a Headquarters' Agreement with the hosting State, this appears to be unlikely.

²² Contract No 2 with France JLS-B3-2007-07 – Engagement du personnel de la France dans la préparation de la gestion opérationnelle du SIS II

EURODAC systems, even if they have previously worked on large-scale IT systems. With the new Regulatory Agency option as well as the FRONTEX option, there are similar needs for initial training. Twenty-seven training days would be provided for 75 persons at a daily rate of €32 (labour cost in the Commission²³), plus the trainers' fees at about €300,000.

With regard to facilities, if the Baseline option²⁴ were used for executing the tasks of a Management Authority, up-grades (and a possible extension) to the existing facility in the range of €4 million could be necessary.

If the site of a new Regulatory Agency were in another Member State, there would be a need for acquiring facilities. This would most likely be also the case under the FRONTEX option, as the existing facilities would be unsuitable for carrying out the tasks of the long-term management of IT systems. Should new dedicated facilities be purchased, the estimated cost for buildings foreseen for managing and operating these systems is around €12,6 million. There could be a possibility to spread this cost out over several years (lease or loan), thus mitigating the effect on the EU budget.

Should the Member State that would host the location for the new Regulatory Agency provide facilities free of charge, it is very likely that adaptations to the buildings would be required (e.g. security features, upgrades in power supply, air-conditioning), for which an estimated €4 million has been budgeted.

Table 9 illustrates that the most cost-effective solutions in the short to medium term entail retaining the Management Authority in the current countries or the sub-option of the new Regulatory Agency, where the host Member State provides facilities free of charge. In general, in the context of the Regulatory Agency option, management functions and roles are to be located on-site, whereby there would be a need to accommodate 30 additional staff, compared to the existing levels and across most of the options, in order to carry out Agency-related tasks. Under the Baseline option, office space would also need to be added for staff occupying the posts of current Commission (support) staff, dealing with system development, project management, procurement, etc.

Running Costs are costs associated with the ongoing activity to meet a desired level of functionality of the systems. These include costs for physically running the site (air-conditioning, cleaning etc), staffing costs and training, the provision of power, telephony, stationery, and general maintenance of the facility and equipment.

Table 10 Running costs - Comparative table: Baseline, new Regulatory Agency and FRONTEX

Cost item	Baseline	Regulatory Agency with a	Regulatory Agency with	FRONTEX ²⁵
-----------	----------	--------------------------	------------------------	-----------------------

²³ European Commission, DG BUDG, note 24/11/2006, Adonis No 11216

²⁴ However, if it were decided to transfer sTESTA (secured Trans European Services for Telematics between Administrations) crypto management to the Management Authority, such a decision could imply an additional 30 persons to the staff of the Central Unit and entail costs for expansion to hold new systems and staff in these premises (office space, equipment, logistics, infrastructure, training, missions for network trouble-shooting). If such network tasks are transferred, these additional costs would apply across the board to any option chosen.

		purchase of new facilities	facilities made available free of charge by a Member State	
Central Unit (CU) energy	140,000	140,000	140,000	140,000
Back-up to Central Unit (BCU) energy	105,000	105,000	105,000	105,000
CU site running costs	1,130,990 ²⁶	730,000 ²⁷	300,000 ²⁸	1,425,000 ²⁹
BCU site running costs (serviced 240m2 workspace)	182,400 ³⁰	66,667 ³¹	66,667 ³²	164,666 ³³
CU and BCU security and access control	288,000 ³⁴	921,600 <i>16 agents</i>	921,600 <i>16 agents</i>	921,600 <i>16 agents</i>
Connection to sTESTA (SIS II and VIS)	16,500,000	16,500,000	16,500,000	16,500,000
Human resources – 75 operating staff	9,750,000	8,775,000	8,775,000	8,775,000
Human resources – 30	3,510,000	3,510,000	3,510,000	3,510,000 ³⁵

²⁵ Running costs related to management of the relevant systems only.

²⁶ Rent of pre-fabricated serviced and equipped work space of 730 m2, plus parking, site coordinator, cleaning, utilities, telecoms and insurance. Possible up-grading of the facility would entail an additional €200 000 per year over 20 years. France provides the system hosting space free of charge.

²⁷ Annual depreciation over 20 years of purchase of 1800m2 (serviced and equipped, based on cost of €7,000 per m2) and running costs of €100,000 for cleaning, telecoms etc.

²⁸ Adaptation of facilities, written off over 20 years and running costs of €100,000 for cleaning, telecoms etc.

²⁹ Annual cost of office space for 170 staff (rent, water, gas, electricity, cleaning, furnishing). This is however not a fully comparable figure, as facilities dedicated to hosting servers could entail even higher costs.

³⁰ Including power, air conditioning, cleaning and telecoms for SIS II, VIS and BMS €15,200 per month, based on Contract 1 with Austria JLS-B3-2007-008

³¹ 2/3 of CU running costs of €100,000

³² 2/3 of CU running costs of €100,000

³³ 2/3 of FRONTEX offices' running costs of €247,000

³⁴ Contribution to CU security and access control. BCU is provided free of charge.

support staff				
Training	219,000	219,000	219,000	219,000
Insurance of systems and premises	100,000	100,000	100,000	100,000
Information campaign	400,000	400,000	400,000	400,000
Translation	100,000	100,000	100,000	100,000
Travel - meetings and conferences, including committees	100,000	100,000	100,000	100,000
Evaluation and reporting	10,700	10,700	10,700	10,700
Studies and consultants	150,000	150,000	150,000	150,000
Overheads and miscellaneous (15%)	4,902,914	4,774,195	4,709,695	4,893,145
<i>Total</i>	<i>37,589,004</i>	<i>36,602,162</i>	<i>36,107,662</i>	<i>37,514,011</i>

Sources: RAND Europe; SIS II Budgetary Impact Statement; Regulation of the Parliament and the Council on the establishment, operation and use of the second generation Schengen information system (SIS II); Financial Statement: Functioning of the SIS II (p39 – 49); C.SIS budget 7440/1/06 REV 1 LIMITE SIRIS 56 COMIX 275; the Translation Centre in Luxembourg, 2007 prices for translation; French Ministry of the Interior as provided by European Commission on 08/11/2007; extracts from Contract No 1 and No 2 with France and Contract No 1 with Austria for operational preparations; FRONTEX preliminary Draft Budget 2008.

The least expensive option of €36,1 million per annum is a Regulatory Agency, if the Member State hosting the new Management Authority were to provide 1800 m2 of existing facilities free of charge. Some adaptation in such facilities is likely to be necessary. A provision of €4 million has therefore been budgeted for the purpose. The second best option is a new Regulatory Agency, with a cost of €36,6 million a year, if 1800 m2 of new facilities need to be purchased in another Member State. The estimated costs under the Baseline and FRONTEX options amount to €37,5 million per year.

³⁵ FRONTEX is already an existing EU Agency with around 170 staff. Adding 75 new operational staff to FRONTEX for managing the IT systems would require additional support staff. It is expected that some limited synergies could possibly be found with the existing support staff at FRONTEX. but it is difficult to establish this with any degree of precision at this point in time.

Main differences in costs:

The costs related to building or adapting new facilities have, for the reasons of comparability, been written off over 20 years, owing to depreciation. The major source of expenditure under the FRONTEX option is the renting of office space (two floors in an office building) for 170 staff. This figure is not fully comparable with estimations under other options, as rental of facilities dedicated to hosting servers, under the existing contractual terms, would entail even higher costs. Provided FRONTEX were to assume the tasks of the new Management Authority, the most sustainable solution would be to purchase the necessary 1800 m² of dedicated space for the systems. Under the Baseline option, the main cost article is the renting of 730m² of pre-fabricated working space, which over time would have to be up-graded or replaced by a permanent structure. System hosting space is provided free of charge.

Costs for operational human resources (€130,000 per person per year³⁶) are higher in the case of the Baseline option than with the rates applied by the EU to its staff (€17,000 per person per year³⁷). Regarding the support functions, under all options the 30 staff would be recruited at the rates applied by the EU (€17,000 per person per year). The latter rates would be applicable to all staff working in a Regulatory Agency. Although there is an administration division in FRONTEX that supports its activities, around 30 additional staff would be needed to carry out tasks related to managing the IT systems. Some synergies with the existing support staff in FRONTEX could most likely be implemented, but this is difficult to establish at this point in time.

The new Regulatory Agency and FRONTEX options would, however, require the hiring of 16 agents to ensure security and access control to the central and the back-up unit. This is estimated to cost around €4,800 a month per agent amounting to €21,600 per annum.³⁸ At present, in the case of the Baseline option, the Commission contributes approximately €88,000 a year to the security and access control of the SIS central unit (CU) in France. Security on the back-up (BCU) site is provided free of charge by Austria.

The annual connection fees of €16,5 million for the secured, highly available sTESTA network are also an important cost item. With a high-availability and high-reliability system such as this, the energy consumption is significant, as servers must be kept in precise environmental conditions, back-up generators must be kept running and power is needed to run complex security and ventilation systems.

Operational Expenditure (OPEX) denotes the recurring costs associated with functional or evolutionary system upgrades, or any costs associated with developments that add value to the asset. Table 11 presents the annual cost implications for operational expenditure.

³⁶ Contract No 2 with France: JLS-B3-2007-07 – Engagement du personnel de la France dans la préparation de la gestion opérationnelle du SISII

³⁷ European Commission, DG BUDG, note 24/11/2006, Adonis No 11216

³⁸ Calculated on the basis of Contract No 1 between the Commission and France: JLS-B3-2007-03 – Contrat de Service- Préparation de la gestion opérationnelle des parties centrales du SISII et VIS/BMS

Table 11 Overall estimated budget implication for OPEX per annum – same for Baseline, new Regulatory Agency and FRONTEX

Cost item	
Hardware and software refresh	400,000
Developments in system functionality	3,000,000
Total	3,400,000

Source: Budget estimate for C.SIS installation and operating costs for 2007; RAND Europe. For the purposes of this assessment, the cost has been multiplied by two (VIS).

Given that the requirements for SIS II and VIS are defined in the legal instruments governing the systems, it is assumed that the initial investment will be very closely aligned to an initial estimate of capacity. This means that if unforeseen new requirements need to be accommodated then the €400,000 cost for hardware and software refreshment would increase; this would be offset by the costs for accommodating the difference between predicted demand and actual demand.

An additional €3.0 million per year would be set aside for system functionality changes. This sum would accommodate any new or different requirements which may be progressively added.

The costs that regularly occur each year for managing the systems are a combination of OPEX and running costs.

In summary, if the new Regulatory Agency option were chosen, it would not make much of a difference whether the existing Member State running the system or some other Member State were chosen to host the Agency. If the Baseline or FRONTEX options were chosen, then the least costly and most sustainable alternative would be to purchase a new facility, instead of opting for long term rental of workspace or extending the existing sites. In the case of a new hosting country, the latter, in order to become the location for the Agency, could include the necessary site or even a building free of charge in its bid, significantly reducing the costs of the option.

9.2. Scenarios concerning moving of the systems to a new location³⁹

Although the three management options under consideration entail similar costs in the long term, a new facility and relocation of the systems are more likely in the case of a new Regulatory Agency situated in another Member State or with the FRONTEX option. Even though remote management can be considered as an option, namely that the management roles and functions are not on the same site, this may lead to extra coordination costs, travel costs and time lost in travelling between the different locations. It could also result in delays in technical interventions. On the other hand, the concentration of all systems on the same site could raise security

³⁹ The legal instruments governing SIS II (article 4(3) of Regulation (EC) 1987/2006 and VIS (article 27 of Regulation (EC) 767/2008 explicitly provide that the central systems are located in France while their backup systems are located in Austria.

concerns that would have to be addressed. Whatever the solution on the nature of the Management Authority, remote management would lead to extra coordination costs.

In the case of the Baseline option, the Commission could also be offered a facility by another Member State or could procure the provision of a facility and operational management services through a competitive tender among interested Member States.

Potential scenarios are assessed across all options:

- (1) Systems remain in Strasbourg and BCU near Salzburg:
 - (a) New facility in current locations
 - (b) Continuation and expansion of old facilities
- (2) Systems (central and back up central systems) move to new locations:
 - (a) Existing national facilities
 - (c) New facilities

The impact on the general budget of the EU of these scenarios is affected by:

- (b) The choice of management option
- (d) The choice to develop and/or include additional systems
- (e) The occurrence of a process of competitive bidding between Member State ‘providers’

Figure 1: Scenario summary

New Facility	<ul style="list-style-type: none"> •Capital expenditure of new facility •Move logistics •High training cost •Other labour regime (shift patterns, working week, salary levels) •Difference in energy costs 	<ul style="list-style-type: none"> •Capital expenditure of new facility •(limited) move logistics •High learning curve •Better planning •Risk of monopoly pricing •Local embedding (services)
	<ul style="list-style-type: none"> •Capital expenditure of up grade/ adjustments •Move logistics •High training cost •Other labour regime (shift patterns, working week, salary levels) •Difference in energy costs 	<ul style="list-style-type: none"> •Capital expenditure on expansion •Higher maintenance cost •High learning curve •Better planning •Monopoly pricing •Local embedding (services, infrastructure)
Existing Facility	Relocation to other MS	Stay in same MS

Scenario 2 (systems transferred to a new location) is particularly influenced by the contents of the offer, country and local price levels, as well as the availability of support services and infrastructure.

Any scenario involving a Member State as a service provider will result in fluctuations in the overall total cost to the general budget of the EU; these costs are

contingent on the price negotiated between the Commission and the Member States running the systems and the facility. Should there be a move to a new host Member State, initially, this is likely to lead to a reduction in the total cost of the facilities compared to a negotiated price with a *de facto* monopoly supplier.

Scenario 2 (systems transferred to a new location) would entail considerable initial training costs that would however, be neutralised by the fact that staff would also need to be trained under scenario 1 with a steep learning curve. As the geographical quality of Scenario 2 is different from the current provider, then it is highly likely that the staff ratios for 24/7 posts and salary levels would change, both in terms of market-driven core salary and overheads set at organisational level. Training days per employee would be cheaper in case of an Agency and potentially also in another Member State than under Scenario 1. Installation costs as well as the costs of physically relocating hardware and equipment would need to be borne. These costs could be offset in the long term if the facilities were better adapted to needs, thereby reducing expenditure requirements, apart from the initial investment. Figure 1 describes this in more detail.

9.3. Adding new systems

The estimated costs related to adding new systems are similar across all options.

At this stage of development, €5,4 million has been spent on direct system development for SIS II and VIS⁴⁰. An additional €7 million has been spent in total for testing and quality assurance under one contract covering both systems. A total of around €62.5 million has therefore been spent so far on direct system development and testing for both systems. This includes provision of hardware and software and three years' warranty for routine maintenance, after which maintenance must be included in operational expenditure. It is possible that significant capital expenditure for system purchase could be incurred for adapting to these new functional requirements.⁴¹

In addition to the significant costs associated with the capital expenditure on new systems, major functional upgrades can be similarly expensive. These may not have been originally foreseen and the system vendor will therefore charge extra for an upgrade to accommodate new functionalities that have been required by a change in the policy scope of the system. An example of this is in the VIS Budgetary Impact Statement, where costs of €5,6 million were incurred as a result of the requirements being changed in the VIS Regulation.⁴²

Table 12 illustrates the capital expenditure associated with expanding the facility to cope with the arrival of new systems. This does not include capital expenditure associated with the system purchase itself, merely the costs of the facility and infrastructure necessary to house the systems.

⁴⁰ JLS.B3.CPO: financial management tables European Commission 17th October

⁴¹ Examples of other one-off costs that have occurred previously include the €3m to introduce the Portuguese SISone4all initiative (the interim solution allowing the new Member States to join the SIS prior to SIS II rollout).

⁴² Memorandum to the Commission (COMM_PDF_C_2007_1407_1_XX1.pdf)

Table 12 Capital expenditure to accommodate a new system

Cost item	
Provision of additional server space in CU (Strasbourg)	8,722,200
Site preparation Austria - Electricity substation and LAN preparation	200,000
Site preparation Strasbourg (up-grade of electricity provision)	2,300,000
Total	3,372,200

Source: *Financial Annex – Preparation of the Operational management of the central parts of SIS II and VIS/BMS; Memorandum to the Commission (COMM_PDF_C_2007_0528_1_XX.pdf); RAND Europe assumptions*

Table 13 illustrates the capital expenditure associated with adding office space to accommodate system development and the procurement staff to be accommodated in the facility at the start of operations.

Table 13 Costs of adding in administrative office space (associated with system development, procurement staff)

Cost item	
Provision of physical facility	972,840
Additional IT infrastructure work	128,000
Site security (upgrade to existing site)	69,960
Cost of installing (up-grade to existing site)	42,900
Site Co-ordinator (up-grade to existing site)	48,000
Total	1,261,700

Source: *Financial Annex – Preparation of the Operational management of the central parts of SIS II and VIS/BMS; RAND Europe assumptions*

Finally, the capital expenditure on new systems themselves must be considered. Table 14 indicates the likely capital expenditure on: a new system of comparable size and complexity to that of SIS II and VIS/BMS, using a similar or identical technological platform and solution; or significant system development to accommodate major changes in functionality for existing systems.

Table 14 Direct development costs

Cost item	
Direct system development cost	27,742,500

Testing and quality assurance	3,500,000
<i>Total system capital expenditure</i>	<i>31,242,500</i>

Source: JLS.B3.CPO: financial management tables, European Commission 17 October 2007

10. PREFERRED OPTION – A NEW REGULATORY AGENCY

The option that scored highest in the qualitative assessment is a new Regulatory Agency, followed by FRONTEX. Although establishing an Agency may be rather a time-consuming and complex process, in the long-term it is most likely to provide the best quality of service to the users of SIS II, VIS, EURODAC and for possibly accommodating any other systems in the area of JHA, while respecting the legal constraints, the '*géométrie variable*' and ensuring financial stability. In the long-term it is also the most cost-effective solution, even if the start up costs may be high. The ability of the Agency to use all the possible synergies depends largely on its tasks.

10.1. Scope of the tasks of the Agency

10.1.1. Responsibility for development and management of new systems in the area of freedom, security and justice,

In order to increase the operational base and better justify managerial overheads, the Agency should be made responsible for the development and management of new systems in the area of freedom, security and justice, once the decision on their establishment has been taken by the European legislator. Firstly, many of the tasks related to the running of the systems, procurement and project management would overlap for several systems. Secondly, the Agency would have the necessary expertise for developing new systems and hence save on training costs. Finally, the scale of procurement activities could lead to a better negotiating position.

10.1.2. Responsibility for technical implementing rules

In order to ensure efficiency and effectiveness of the systems, it would be preferable to delegate as much responsibility as possible to the Agency, to provide a clear and transparent structure and to keep decision-making close to its implementation. The main body governing the Agency would be a Management Board, with an adequate representation of the stakeholders (Member States, Commission) reflecting their Treaty prerogatives and obligations.

The Agency, however, must be developed within the EU legal and institutional framework which imposes certain constraints, such as the differences in Member States' participation in the systems, as well as their nature and scope. There may also be specific legal constraints in entrusting the Agency with the tasks currently covered by comitology, which directly stem from the EC Treaty and the case law of the European Court of Justice.⁴³

⁴³ Meroni & Co. v. High Authority of the European Coal and Steel Community: Cases 9 and 10/56.

Nonetheless, some of the more technical issues covered by the implementing measures in the legal instruments establishing the systems could be conferred on the Agency. From an operational perspective this may be desirable. Furthermore, from a governance viewpoint, a more active involvement of the users of the system would be preferable, as well as a simple and transparent division of competences. If part of the activities related to the management were outside the control of the Agency and remained with the Commission or the Council, management by the Agency would be less effective.⁴⁴

11. MONITORING AND EVALUATION

Monitoring of the systems' performance will be critical for the success of the project.

The SIS II Regulation and Decision foresee that the Management Authority shall ensure that procedures are in place to monitor the functioning of SIS II against objectives relating to output, cost-effectiveness, security and quality of service. Each year the Management Authority shall publish statistics showing the number of records per category of alert, the number of hits per category of alert and how many times SIS II was accessed, in total and for each Member State. Two years after SIS II is brought into operation and every two years thereafter, the Management Authority shall submit to the European Parliament and the Council a report on the technical functioning of the Central SIS II system and the Communication Infrastructure, including the security thereof and the bilateral and multilateral exchange of supplementary information between Member States.⁴⁵

The draft VIS Regulation and Decision provide similar reporting obligations for the Management Authority, with the exception of the annual statistics.⁴⁶

According to the EURODAC Regulation, the Central Unit (CU) is responsible for drawing up quarterly statistics.⁴⁷ The Commission, as the entity managing the Central Unit, which could be replaced by the same Management Authority established for SIS II and VIS, shall submit to the European Parliament and the Council an annual report on the activities of the CU. The annual report shall include information on the management and performance of EURODAC against predefined quantitative indicators for the objectives set in the Regulation. The Commission shall ensure that systems are in place to monitor the functioning of the Central Unit against objectives, in terms of outputs, cost-effectiveness and quality of service. It shall regularly evaluate the operation of the CU, in order to establish whether its objectives have been attained cost-effectively and with a view to providing guidelines for improving the efficiency of future operations.

⁴⁴ This would be the case under any of the options. For the Baseline and Baseline + the Commission would in any case keep the powers granted to it by the SIS II and VIS legal instruments, whereas the case for FRONTEX and Europol would be the same as for a new Agency.

⁴⁵ Art. 50 of the SIS II Regulation and Art. 66 of the SIS II Decision.

⁴⁶ Art. 50 of the VIS Regulation and Art. 17 of the VIS Decision.

⁴⁷ Art. 3 of the EURODAC Regulation.

For the preferred option, the Financial Regulation⁴⁸ stipulates regular evaluations of activities when these necessitate significant expenditure. In addition, the potential indicators listed below should provide an effective barometer to measure the (operational) criteria used for assessing the impacts of the implemented option. The indicators should also allow effective measurement of performance against these criteria.

11.1. Operations

- Downtime per user and downtime for the central systems
- Staff turnover
- Percentage of time when availability and performance requirements were met
- Total system downtime during the reporting period
- Database status: current size of database in terms of disk space, number of records, and number of alerts, difference with previous month(s)
- Capacity and system load: remaining storage space and percentage of time when processing power/bandwidth/memory use reached various percentage bands (up to 50%, 51%-60%, 61%-70%, etc.)
- Status on infrastructure and environment: percentage of time when environmental requirements were met. If this figure is not 100%, the report must include a description/explanation of the instances where environmental requirements were not met.

11.2. Monitoring

- Number of system events by degree of severity
- Complete list of medium-severity and critical events, with description/explanation of each event and the actions taken
- Percentage of time when the required reaction times to system were met. If this figure is not 100%, an explanation of the causes and suggestions for remedial action should be included
- Average reaction time to medium-severity and critical events
- Number of attempted security breaches
- Number of successful security breaches
- Restitution time after security breaches

⁴⁸ Council Regulation (EC, Euratom) N° 1995/2006 of 13 December 2006 amending Regulation N° 1605/2002 on the Financial regulation applicable to the general budget of the European Communities (OJ L 390/2006 of 30 December 2006).

11.3. User support

- Number of tickets recorded during the reporting month
- Description of the main issues encountered and actions taken
- Detailed description of any major issue(s)
- Ticket resolution percentage
- Average resolution time, statistical distribution of resolution times per quintile
- Collected user feedback on the service provided
- Number of defined service targets achieved (e.g. goals for uptime, etc)

Annex 1 Pre-screening of options

This annex will address the pre-screening of options conducted in the first phase of the study and the final set of options that emerged.

1. THE OPTIONS

The Commission put forward the following initial set of options to be assessed:

- Option 1: Regulatory or other Agency
- Option 2: Management by FRONTEX
- Option 3a: The Commission
- Option 3b: The Commission through an Executive Agency
- Option 4: Europol
- Option 5: Management by one Member State on behalf of all

2. PRE-SCREENING CRITERIA

The options assessed were chosen from the options that appeared in the discussions on SIS II in the working parties of the Council. In the course of the impact assessment the European Parliament and the Council agreed on the legal instrument establishing VIS and on a joint statement relating to the operational management of VIS, in which they agreed that the impact assessment on the long-term management of VIS could form part of the impact assessment for SIS II long-term management. This implies that any solution for SIS II must also provide effective management of VIS. Managing EURODAC together with VIS and SIS II together could create substantial synergies and economies of scale. The biometric matching functionality (in the form of the service-orientated architecture of the Biometric Matching System (BMS)) will in the first instance be made available for VIS. It is likely to be provided at a later stage for SIS II and EURODAC.

The following criteria were applied in subsequent rounds of pre-screening:

- legality,
- broad rejection by key stakeholders, and
- ability to include VIS and EURODAC.

All these options were first assessed on their legality, meaning whether they are compliant with the *acquis communautaire*.

Options that were largely rejected by the key stakeholders were eliminated, on the grounds of lack of political support, which does not preclude that they are unfeasible or even ineffective.

Subsequently, the options were evaluated on their ability to deliver effective and accountable operational management for SIS II, as well as VIS and EURODAC. This criterion allowed options to be eliminated or adjusted.

3. OUTCOMES

Based on the three criteria, the following options were dismissed or adjusted as a result of the initial assessment:

Option 3a - The Commission directly

Key stakeholders: European Parliament and Member States do not support management by the Commission.

The Commission's governance would be based on the comitology procedure. More important decisions would be taken in the framework of a comitology committee composed of Member State representatives with the Commission acting as chair, whereas day-to-day management would be directly exercised by the Commission. Funding would be possible from a budget line under the Commission's operational appropriations. Management by the Commission would also mean that the EC staff rules would apply.

It became apparent during interviews with representatives of the Member States and the European Parliament, that there is no support for an option where the Commission would be in charge of SIS II. Although the interviewed representatives of Member States do not object to the Commission running VIS, Members of the European Parliament were more concerned. Their main concern is that control and supervision of SIS II, and to some extent VIS, would be more difficult if they were managed by such a large organisation as the Commission. Furthermore, experts within the Commission expressed doubts over the appropriateness of the Commission managing large-scale IT systems, as it is not the Commission's core task to be an IT service provider for the Member States. Notwithstanding the negative stakeholder perception of this option, the pre-screening identified management by the Commission as one of the most promising options, due to available support functions, access to staff and funds, growing expertise, critical mass and policy focus. However, because of the obvious lack of political support and even outright resistance, including during the negotiations on the legal instruments establishing SIS II and VIS, it was decided that there would be no merit in pursuing this option any further.

Option 3b - The Commission through an Executive Agency

An Executive Agency cannot be used to run large-scale IT systems such as SIS II

Executive Agencies are regulated by Council Regulation (EC) No 58/2003.⁴⁹ Responsibility and final control over the operation and governance of these agencies is still with the Commission. The Commission must therefore have real control over the operation and the governance of the Agency. The Commission exercises administrative oversight and any act of an Executive Agency which injures a third party should be referred to the Commission for a review of its legality.

These agencies are to be entrusted with certain management tasks relating to one or more Community programmes. They are set up for a fixed period and their location has to be in either Brussels or Luxembourg. They are meant to handle the implementation of grant awards by the Commission under specific programmes, including activities such as launching calls for proposals, evaluating proposals, contracting projects, monitoring the contracts and conducting payments. In practice, this set of criteria excludes an executive Agency from handling a long-term task such as management of SIS II, VIS and EURODAC.

Option 4 - Europol for all systems

The Europol option must be adjusted, as it may prove difficult to accommodate VIS and EURODAC

The replacement of the Europol Convention by a Community legal instrument and the establishment of Europol as an EU Agency as of 2010, could create the legal conditions for Europol to manage SIS II and possibly also VIS and EURODAC. However, at the time when this Impact Assessment was compiled, negotiations on the new legal framework were ongoing and their outcome was difficult to estimate, the situation preceding the start of application of the new legal instruments is analysed in this Impact Assessment.

Europol has experience in running a large-scale IT system, although this is not its prime task. Furthermore, it is part of the law enforcement community and therefore fits relatively well with the SIS II user community. Nevertheless, legal adjustment must be made to ensure data protection supervision by the European Data Protection Supervisor and the effective supervision by the European Parliament and other EU institutions, as foreseen in the SIS II legal instruments.

The legality of Europol managing first pillar systems like VIS and EURODAC, which are linked to the free movement of persons, and the desirability of this option, can be seriously questioned. The user communities for these systems differ from the law enforcement community of Europol. Management of a visa or asylum application information system by a police institution would result in difficulties in aligning the functioning of the systems with the wider objectives of the visa and asylum policies. Europol could, in principle, manage SIS II and possibly other third pillar systems in the future, but a separate solution would have to be found for VIS and eventually EURODAC.

⁴⁹ Council Regulation (EC) No 58/2003 of 19 December 2002 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programmes in OJ 2003 L 11, 16.1.2003.

EURODAC is currently under the responsibility of the Commission. This will also apply to VIS during the transition phase (with the option of entrusting operational management to national public sector bodies in two different Member States) and this solution could be continued.

Some concerns expressed by stakeholders relate to data protection and to the fact that Europol only has access to limited categories of SIS II data. Furthermore, security measures would be required to ensure that the operational management function would not provide access to all the data in the system, including data to which Europol does not have legal access.

Option 5 - Management by one Member State on behalf of all

An EU system financed by the EU budget cannot be run by one Member State on behalf of all Member States

This option basically reverts back to SIS I. However, with a legal basis under EU law and financing from the general budget of the EU, new requirements apply, since the Commission, in line with the Treaty, is not allowed to fully outsource its responsibility for implementing the EU budget.

This would require SIS II to be run as it used to be: on an intergovernmental basis, by direct Member State contributions, outside the EU budget. This is not appropriate for the first-pillar component of SIS II. Similarly, it could be impossible for the first-pillar systems VIS and EURODAC to be managed by an intergovernmental structure.

Apart from the financing, it is also not clear how such a solution would fit into the EU context. If based on EU law, EU law provisions need to apply. There are no provisions for governing Member States' activities without legally involving the EU institutions. This option would therefore probably also require withdrawal of the legal instruments and establishing SIS II outside the EU framework, through an inter-governmental convention or a treaty and this would be in breach of the Schengen Protocol.

4. THE FINAL SET OF OPTIONS

Based on the pre-screening the following list of final options was identified. These are assessed in detail in the body of this report.

- **Baseline:**
 - SIS II: The Commission entrusts management tasks to Member States
 - VIS: The Commission entrusts management tasks to Member States
 - EURODAC: The Commission itself
- **Baseline+:** Member States entrusted by Commission for SIS II, VIS and EURODAC together

- New Regulatory Agency for SIS II, VIS and EURODAC together
- FRONTEX for SIS II, VIS and EURODAC together
- Europol for SIS II and the Commission for VIS and EURODAC

Annex 2
Detailed assessment of the remaining five options

Under each of the criteria, each option has been given 1 to 3 stars, where one star (*) denotes weak, two stars (**) indicates medium and three stars (***) denotes good performance. In addition, in each of the categories of criteria, the most important criteria have been marked in **bold** in the table showing the results of the assessment. The scoring is based on a qualitative assessment, expressing absolute performance and relative performance in relation to the other options.

1. OPERATIONS

1.1. Reliability and quality of service

Delivery of service is affected by the degree to which the Management Authority considers the management of IT systems to be its core task. This allows it to make decisions on resource allocation with the sole purpose of improving system performance and providing the best quality of service to the users of the systems.

The mission critical status of the systems requires considerable redundancy. Therefore, it is important for the systems' supporting infrastructure and staff to ensure 24/7 services under all circumstances. Any management option that would lead to reducing this level of service, due to cost concerns or other objectives, would risk compromising reliability and continuity of service.

Options	Impacts: Reliability and quality of service	Rating
Baseline	<p>The current dedicated facility and staff have a track-record in running SIS I and have provided a sufficient quality of service to the users of the system. However, France is running SIS I on an intergovernmental basis. Under the Baseline and Baseline+ option, France and Austria would run the systems on behalf of the Commission, which would still keep certain tasks. Although the Commission is currently running some systems, including EURODAC, management of IT systems is not a core task of the Commission.</p> <p>Lack of direct relationship between the service provider (Member States managing the systems) and the users of the systems (other Member States) is likely to reduce the quality of service received by the users, which cannot express their concerns directly.</p>	**
Baseline+	Similar to Option 1.	**
Regulatory	The Regulatory Agency would allow dedicated and	***

Agency	tailor-made solutions for management of the systems. Its primary concern would be to provide the best quality of continuous service to the users of the system and it would use all the resources to achieve that.	
FRONTEX	FRONTEX currently has no experience in handling high-reliability services and guaranteeing mission critical functions on a 24/7 basis. The infrastructure and expertise necessary for providing and ensuring the expected quality of service levels would need to be put in place. A new department that would be responsible for the management of the systems would have the same advantages as building a new, tailored Agency. However, it could be somewhat diminished by the fact that management of IT systems does not belong to the original objectives of FRONTEX.	**
Europol	Although Europol has its own IT system, its IT track-record is not yet fully established, especially for high-availability and high-security IT systems that require management 24/7. Adding new systems would require a strong shift of focus towards IT management, which is not part of Europol's original objectives. First of all, this would require strong political will. The more IT systems that would be added, the more political will and detailed discussion would be needed, to realign the core tasks of Europol from its initial objective of supporting police co-operation. Moreover, the perception of the core tasks of the organisation among its key stakeholders and among the public at large would also change.	**

1.2. Providing adequate management services to Member States authorities, including specific needs of users (Member States)

From the interviews with the stakeholders it is clear that continuity and quality of service are the major concerns,⁵⁰ as well as the ability of the organisation to support specific user demands. Further requirements are the ability to develop long-term IT strategy, transparency and provision of consistent and continuous management.

⁵⁰ E.g. from interview with SIS II project manager and s-TESTA project manager, 9 March 2007; SIS II Annual Financing Decision 2007 (Budgetary Impact Statement) – Memorandum to the Commission (COMM_PDF_C_2007_0528_1_XX.pdf) 22 February 2007, Brussels; and VIS Annual Financing Decision 2007 (Budgetary Impact Statement) Memorandum to the Commission (COMM_PDF_C_2007_1407_1_XX1.pdf), 30 March 2007, Brussels.

This criterion requires management to be flexible in its access to funds, skills and equipment. It is also influenced by the timeliness of responses to requests and thus specific in-house expertise for a 24/7 service and effective Information Technology Infrastructure Library (ITIL) processes, with high levels of operational autonomy of management to make its own executive decisions. The options that score high on quality of service are also best positioned to deliver this criterion, although it goes further, as it also requires responsiveness and understanding of the user community. Organisations that can muster the best IT skills and those that are actively involved with the user community, and understand their interaction with the system and specific needs and priorities, would therefore be preferred.

Options	Impacts: providing adequate management services to Member States' authorities, including specific needs of users (Member States);	Rating
Baseline	Concerns have been voiced about delays in the development phase of SIS II. ⁵¹ Management by the Commission increases the distance between the management service provider and users. The Commission in its institutional role may have its own policy objectives, which could interfere with its responsiveness to the wishes of Member States. It should be noted that these concerns are typically raised by Member States for SIS II and have not been voiced in the context of VIS or EURODAC.	*
Baseline+	Same as option 1	*
Regulatory Agency	A new Agency may develop both the technical skills and the desired focus and understanding of the user community. If actively managed, its dedicated objectives could allow it to become a focal point for the user community for the pan-European aspects in the medium to long term.	***
FRONTEX	FRONTEX is likely to be well adjusted to needs relating to the area of border control. However it is currently not attuned to the requirements of the law enforcement community. However, with time, pooling IT expertise, providing a dedicated department and a special setting of the Management Board could bring this option closer to the new Regulatory Agency.	**
Europol	Europol should be well-positioned to service the needs of its users, as it is embedded in the EU law enforcement community. However, the situation for EURODAC and VIS would be as for option 1.	*

⁵¹ Expressed in interviews by MEPs and Member States representatives

1.3. Ensuring flexibility to add other existing and potentially new systems

With the expansion of current systems and the addition of new systems there will be a stronger lock-in of the chosen option and location, i.e. the barriers to changing or adjusting the management will increase. Consideration therefore needs to be given in advance to what kind of systems may be included and how this portfolio is reflected in the chosen option. In practice, this means that the management must be suitable for managing all current and future systems in the field of justice, freedom and security, including police cooperation, border control and migration.

From the governance perspective there may be limits to how many different constituencies (law enforcement, migration, border crossing) can be serviced through one organisation. If the variety in scope of the systems increases further, the ‘common denominator’ moves more closely to pure IT expertise, with less value for the stakeholder communities that depend on these systems. Thus the ability to service a broader set of IT systems is reflected in the scope of the Management Authority’s remit and the level of service that the Management Authority is expected to deliver.

Adding new systems has consequences in terms of extra space requirements for equipment, operational staff and supporting infrastructure. In addition, the capacity of the supporting infrastructure, such as generators and air conditioning, must be sufficient or at least should allow for appropriate upgrades. The facilities used in the interim period are assessed as being inadequate for housing any new systems beyond SIS II, VIS and EURODAC II (once SIS I is phased out). The office space is already insufficient for SIS II and VIS development and currently accommodated through temporary solutions.

Options	Impacts: ensuring flexibility to add other existing and potentially new systems	Rating
Baseline	<p><u>Future proofing</u>: the current facilities are not future proof and would need to be replaced or expanded. The cost of this impacts the general budget of the EU. The dependency of the Commission and the Member States on the services of one Member State would grow as new systems are added. The interim solution is not designed to be permanent.</p> <p><u>Scope of systems</u>: the Commission is able to provide consistent management for a great variety of systems, as it covers the full range of related policy areas and has policy coordination procedures in place. Thus there would not be an alignment problem.</p>	**
Baseline+	Same as option 1.	**
Regulatory Agency	<p><u>Future proofing</u>: a custom-built site would allow more systems to be incorporated in a synergetic manner.</p> <p><u>Scope of systems</u>: an Agency could manage a broad range of systems, if it had the right governance structure</p>	***

	to ensure involvement of the various user communities and policy constituencies. This is important for ensuring legitimacy of decision-making covering a wide range of areas – especially given the sensitivity of the justice, freedom and security domain.	
FRONTEX	<p><u>Future proofing</u>: Adding systems would require a strong shift of focus towards IT management, which is neither the original objective of FRONTEX nor currently within its mandate. First of all, this would require strong political will. The more IT systems that were added, the more political will and detailed discussion would be needed, to realign the core tasks of FRONTEX from its initial objective of strengthening cooperation at external borders. Moreover, the perception of the core tasks of the organisation among its key stakeholders and among the public at large would also change.</p> <p><u>Scope of systems</u>: FRONTEX’s remit in border management and its operational management would be adjusted to the requirement to manage large-scale IT systems in other policy areas.</p>	**
Europol	<p><u>Future proofing</u>: adding systems would require a strong shift of focus towards IT management. This is not Europol’s original objective.</p> <p><u>Scope of systems</u>: Europol would not be suitable for running a joint IT management centre for systems concerning a policy area other than police cooperation.</p>	*

1.4. Capacity to provide the required security levels

The security requirements in all three systems are rather similar⁵².

Environments that have a culture of security are likely to implement adequate security requirements. However, security is not only linked to the management of the systems. Effective security must essentially be built into the system itself and be appropriate to the requirements of the system, the users and the data subjects. This must be ensured and is not limited to a single option. Existing organisations may have processes that are not well adjusted to the specific needs of SIS II, VIS and EURODAC.

In terms of the physical security, a custom-built facility is likely to better address the security requirements of the systems.

⁵²

While the SIS II legal instruments (Art. 16 SIS II Regulation and Decision) and the VIS Regulation (Art. 32 VIS Regulation) define 11 security objectives in very similar wording, the EURODAC Regulation only mentions seven objectives (Art. 14). Nevertheless, in spite of the different wording, the security standards in all three systems seem to be similar.

Options	Impacts: capacity to provide the required security levels	Rating
Baseline	The existing facilities are firmly embedded in the security structures of their host nations. They are built to ensure the highest security levels.	**
Baseline+	Similar to Option 1	**
Regulatory Agency	A new Agency has the possibility of building security into the organisation, its processes and in facilities that host the systems from the outset.	***
FRONTEX	FRONTEX has no experience with handling mission critical IT systems and it would need to put in place the security infrastructure and culture to provide and ensure the expected quality of service levels. However, after some time, it could be comparable with a new Regulatory Agency.	**
Europol	Europol has an existing security infrastructure for its systems and its premises. This police environment is likely to have a keen focus on security, as it is part of the organisation's culture. The facilities are embedded in the security structures of the host nation.	***

1.5. Responsiveness to emergency requirements

Emergencies such as attacks and security breaches require operational management to respond quickly and effectively. In such cases the quality of business continuity plans is essential, as well as direct access to the necessary resources (human resources, finance, and technology). In the interim period the back-up site might not have 24/7 staff available, which requires a rapid relocation of the off-duty shift from Strasbourg to Salzburg, in the case of an emergency at the back-up site. This situation may not provide the necessary level of guarantees for continuity of service, due to the travel time and access to the location of the back-up unit. A critical assessment of the provision of services and location of the back-up unit should be assessed against the background of a thorough threat analysis and risk assessment.

Lengthy decision-making procedures should be avoided. Solutions that provide for more autonomy, flexibility and co-location of the systems and management – and thus score well on quality of service provision – are likely to be the most effective. Furthermore, the concentration of specific expertise through the bundling of systems under one management should strengthen shared experience and organisational learning to deal with emergencies.

Options	Impacts: responsiveness to emergency requirements	Rating

Baseline	Decision-making could be carried out directly by the Commission or together with operational staff, without having to go back to the Member States for agreement. A challenge is that the Commission would be controlling the operational management tasks carried out by Member States' public bodies at another location. A rapid response by the Commission to a request for support from operational management would require a transparent and trusted relationship between the Commission and the Member States that run the facilities. In practice, rapid decision-making involving a number of large administrations may prove time consuming.	*
Baseline+	Same as Option 1, but EURODAC would benefit from 24/7 support.	*
Regulatory Agency	Initially the Management Board structure may complicate rapid decision-making. However, a new Agency should be able to develop effective mechanisms to deal with emergencies, once it is well established.	***
FRONTEX	It emerged that the decision-making procedures in FRONTEX can lead to lengthy discussions (e.g. language regimes), which are not conducive to delivering timely and appropriate instructions for management to respond to. ⁵³ Thus current decision-making at FRONTEX is likely to prove an obstacle, as long as no dedicated IT committee or board exists. If such a committee were to exist, decision-making would be similar to a new Agency.	**
Europol	Current decision-making on IT strategy has proved rather difficult ⁵⁴ . IT strategy and IT management are not Europol's main priorities, but with a transfer of SIS II and future systems in the area of law enforcement this could change.	*

1.6. Capacity/flexibility to incorporate new technology and to react to changing demands

The ability to adjust to changing demands and new technology depends largely on the quality and expertise of the contractors and the ability of management to assess the contractors' recommendations and requests. For this purpose, management could hire separate contractors, but ultimately management itself must be able to assess its

⁵³ In the interview with FRONTEX desk officer the example was raised of rigidity of decision making processes and the delays in adopting the Work programme

⁵⁴ As indicated during interview at EUROPOL

own requirements and the available technological solutions, otherwise it would become overly dependent on its suppliers.

Therefore, the technical expertise of the Management Authority, the effectiveness of the procurement and contracting processes and the availability of funds are important factors. The management must not only be able to assess recommendations for updates and requests from service providers, but it should also be able to translate effectively the policy objectives of the Commission and the Member States and the service requirements into technical specifications. The management should retain the responsibility for strategic IT planning and scheduling of updates to the system.

It is important that links exist between the technical aspects of operational management and policy-making. Such links ideally require the involvement of key stakeholders (the Commission and Member States) in managing the system. On the one hand, this would ensure that policymakers are aware of the technical possibilities and limitations, which would allow for a constructive but critical assessment of proposals to make technical adjustments to the system. Furthermore, it would facilitate clear, executable decisions for management to implement. On the other hand, such links may help technical operational management to be more aware of the political context and service requirements that the system is supposed to support.

Options	Impacts: capacity/flexibility to incorporate new technology and to react to changing demands	Rating
Baseline	<p><u>Strategic IT planning:</u> EU funding, based on an annual work-programme and budget, would allow for more continuity and thus simplify the development of a strategic outlook.</p> <p><u>Independence towards IT suppliers:</u> for the Commission it could be difficult to hire and retain the required level of technical expertise to effectively assess the procurement processes and to offer sufficient independent response to technology providers and the operational management at the facility. The inherent bias towards generalists can be mitigated, as the Commission has the possibility to hire temporary agents and deploy national experts⁵⁵. However their temporary nature may lead to discontinuity costs, such as loss of expertise and loss of an effective network of suppliers.</p>	**
Baseline+	Similar to Option 1, but scale advantage in adding EURODAC under one management and running it on the same network as VIS and SIS II. Better leverage of operational expertise.	**
Regulatory Agency	<u>Strategic IT planning:</u> a dedicated Agency would potentially become a centre of excellence in management of large-scale IT systems. Depending on the mandate	***

⁵⁵

Interview with representative of DG Budget

	<p>given to the Agency, it would be well-positioned to develop an effective IT strategy.</p> <p><u>Independence towards IT suppliers:</u> as such, it is also expected to be able to develop the capacity to effectively assess new technologies and requirements for updates to the systems.</p>	
FRONTEX	<p><u>Strategic IT planning:</u> FRONTEX would need to develop necessary skills to effectively and independently conduct effective IT planning.</p> <p><u>Independence towards IT suppliers:</u> there is no track record of required technical expertise and IT procurement skills within the organisation, as it is not geared towards the management of large-scale IT systems. However, if FRONTEX were made responsible for SIS II, VIS, and EURODAC its capacity in this regard would be similar to a new Regulatory Agency.</p>	***
Europol	<p><u>Strategic IT planning:</u> developing an IT strategy proved cumbersome in the past. Europol's in-house skills may not be matched by the IT competence and interest of the Management Board in its current composition.</p> <p><u>Independence towards IT suppliers:</u> Europol's potential for further acquisition of expertise in procurement and contracting would be limited, as it would only take on SIS II and not VIS or EURODAC. As new systems in the area of law enforcement were developed and entrusted to the management of Europol, this disadvantage could be eventually reduced.</p> <p>For VIS and EURODAC, the Commission is also not likely to benefit from the increased learning curve associated with running a number of systems within the same organisation. It would be difficult to retain the skills that were acquired during the interim period.</p>	*

1.7. Ability to recruit and retain key skills

The management of complex IT systems such as SIS II, VIS and EURODAC and the delivery of effective services require critical technical expertise. Management must be able to translate policy objectives and implementation rules into technical specifications. Even though many tasks for designing, maintaining and running SIS II are likely to be outsourced to private providers, management remains responsible for supervision, security and, most importantly, procurement. Thus the ability to hire and retain key capabilities and resources is a central criterion for establishing effective management.

The Management Authority would have different ways of recruiting staff: fixed employment, temporary contracts, seconded national experts and consultants. The

different options allow a certain element of freedom to choose between these alternatives, depending on staff regulations.

Aside from the need to attract and retain key IT and procurement specialists, there is a need to attract experts at short notice, in order to provide rapid response to the needs of Member States or emergencies.

Options	Impacts: ability to recruit key skills	Rating
Baseline	<p>The bulk of operational staff is employed by the French government and this is expected to continue if the interim period is extended indefinitely. The Commission's staff is involved with governance, decision-making and systems development. The possibility to acquire highly specialised personnel is rather limited, due to the Commission's recruitment rules and procedures, which favour generalists rather than specialists. However, recruitment of the staff could be delegated to the national authorities.</p> <p>Hiring 'contract agents' is limited to a maximum of 3 years. Moreover, there are ceilings on the number of such external resources.</p> <p>Regular rotation of staff at the Commission could provide a continuity risk, as crucial skills at the top management level may be lost. As most operational staff members are working under contract with the French government, this concern does not apply.</p>	**
Baseline+	Similar to Option 1	**
Regulatory Agency	<p>Although the Agency would comply with EU staff regulations⁵⁶ it may hire more 'temporary and contract agents' than the internal Commission services. Moreover, contract agents in an Agency can be employed for indefinite period.</p> <p>Agencies tend to be flatter organisations with less expertise on budgetary and legal matters. Such needs are catered for by the Commission services.</p> <p>Staff retention is expected to be high due to specific skill acquisition.</p>	***

⁵⁶ According to Article 17 of the Regulation, "Staff Regulations of officials of the European Communities", the Conditions of employment of other servants of the European Communities and the rules adopted jointly by the institutions of the European Communities for the purposes of applying those Regulations and Conditions shall apply to the Agency's staff

FRONTEX	Similar to option 3 (Regulatory Agency)	***
Europol	Europol has its own staff regulation and is not bound by the Commission Staff regulations. It can hire people on temporary contracts.	***

1.8. Length of time to develop and implement the option

The transitional period for SIS II management should end at the beginning of 2012. It is also likely that the transitional period for VIS will end in 2012. This determines the time period in which the Management Authority must be established.⁵⁷ Delays would affect the ability to plan a timely transfer or relocation to a new facility.

The process of establishing the management has three phases:

- (1) preparatory process – writing the proposal for the legal act, conducting the impact assessment including *ex-ante* evaluation, inter-service and stakeholder consultations (start 2007, adoption by Commission in 2008)
- (2) legislative process – adoption of the legal act in co-decision procedure involving Council and Parliament
- (3) implementation process – financing and implementing the actual management structure and supporting infrastructure (hiring staff, setting up committees, building facilities).

The time horizon of 2012 should be sufficient for all the options, therefore the relevance of this criterion is now less pertinent for differentiating between the appropriateness of the options. The preparatory impact assessment study for the Program for Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business and Citizens estimated the total time to establish a new Agency at 43 months. In the case of FRONTEX, the establishment (from drafting the proposal until the Agency became operational) took approximately 30 months.⁵⁸

The preparatory process is the same for all options, as it was decided up-front that an impact assessment would be required to help determine the choice of option. Important differences are likely to occur in the length of the legislative process and variations in the difficulty of setting up the management.

⁵⁷ Paragraph 9 of the Preamble to both instruments (Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II), OJ L381/4 of 28.12.2006, and Council Decision 14914/06 of 12 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II) establish that the transition period during which the EC is responsible for the operational management of C.SIS (having the right to delegate some responsibilities to two public sector bodies) should not last longer than five years from the entry into force of the instruments. The regulation entered into force on 17 January 2007.

⁵⁸ Interviewees consider the period for setting up FRONTEX as the minimal period necessary for setting up any Agency.

An existing Agency will take less time to implement the necessary management structure, as it has expertise in hiring staff and facilities and infrastructures in place, although the latter might be inadequate and require substantial up-grading. An existing Agency might already be able to start preparations while the legislative process is still ongoing, whereas a new Regulatory Agency would need to start from scratch. First, the Agency's budgets needs to be established and incorporated into the general budget of the EU. There is no authority to hire staff, as all depends on the appointment of a Director and the establishment of internal rules and procedures which, in a new institution, is a sequential process with unavoidable bottlenecks.

Options	Impacts: Length of time to develop and implement the option	Rating
Baseline	<p><u>Allocation of resources:</u> management by the Commission would be the fastest option as the structures and resources are available and can be internally re-allocated at (relatively) short notice, also, the budget could be established within existing appropriations of DG JLS.</p> <p><u>Length of decision-making process:</u> it would require minimal adjustments to existing legal basis, as the transitional solution needs to be made long-term.</p>	***
Baseline+	<p><u>Allocation of resources:</u> similar to Option 1, though there may be rival offers from other Member States that could slow the process down.</p> <p><u>Length of decision-making process:</u> the transfer of EURODAC is likely to be dealt with in the revision of the EURODAC Regulation and should not require separate legislative action. Thus it will not take extra time. In any case the transfer of EURODAC is not critical to the establishment of the long term management of SIS II and VIS.</p>	***
Regulatory Agency	<p><u>Allocation of resources:</u> if the Agency were able to retain the current staff and facilities, it would significantly reduce the implementation time.</p> <p><u>Length of decision-making process:</u> setting up an Agency is time-consuming. It is expected to take anywhere between three and four and a half years, depending on the legislative process and the actual implementation. The negotiations on the legal instruments establishing a new Regulatory Agency are expected to be a lengthy process. The multi-pillar complexity is likely to give rise to different views on the appropriate governance format - in particular the role of the Member States and the Commission in the Management Board - and the Agency's tasks. A debate</p>	*

	on the location of the new Agency could also take time.	
FRONTEX	<p><u>Allocation of resources:</u> The length of the implementation phase depends largely on what will be decided on the location and the retention of current staff and facilities. Developing a fully new infrastructure in Warsaw with new staff is likely to take significantly longer than a solution whereby the Strasbourg site and staff were maintained. In any case, since the Agency already exists some of the time can be saved with comparison to setting up a completely new Agency.</p> <p><u>Length of decision-making process:</u> The FRONTEX Regulation would have to be amended and it could take some time to negotiate.</p>	**
Europol	<p><u>Allocation of resources:</u> the new Europol facilities that are now being developed would have to be adjusted to host SIS II. Depending on the status of development at the time a decision is made on the long term management for SIS II, (and VIS and EURODAC), this would either require a very time-consuming and costly redesign or be effectively incorporated in the planning.</p> <p><u>Length of decision-making process:</u> As the basic act of Europol and its legal status will change, it might therefore require a substantial amount of time to be implemented.</p>	**

2. GOVERNANCE

2.1. Responsiveness to the requirements and views of Member States, the Commission and the European Parliament

The chosen option should be designed to best serve the individual roles and interests of key stakeholders, in particular the EU Member States and associated countries, the Commission and the European Parliament. For Member States, the key factors are that the Management Authority is able to accommodate specific requests and that management is responsive to the requirements of the users of the systems.⁵⁹ Member States in their own capacity and/or through the Council will seek to retain control, or at least an important role, in deciding on these matters – especially in the case of SIS II, the predecessor of which used to be outside the EU framework and under full control of the Schengen Member States.

The founding Treaties oblige the Commission to ensure correct implementation of the general budget of the EU. The Commission has also been given responsibility for implementing certain tasks in the SIS II and VIS legal instruments. It is also restrained by Article 54(1) of the Financial Regulation in its ability to delegate its

⁵⁹ As noted in interviews with Member States.

responsibilities and therefore has a legal obligation to retain a certain level of control. Beyond these legal parameters the Commission's concern is that the management of SIS II, VIS and EURODAC remains aligned and supportive of the broader policy agenda. The Commission has the right of initiative and as such is the main institution responsible for policy initiation, whereas the European Parliament and the Council is the EU Legislator. There is an interest in ensuring that the system is operated in such a way that it optimally supports the underlying policies and that policy-makers take into account the capabilities and limitations of the system.

The European Parliament must be able to perform its primary supervision functions in the legislative process as co-legislator and budgetary authority. The European Parliament's main concern is to be able to supervise the correctness of budget expenditure and the responsible use of EU resources, and to ensure that the Management Authority is supporting EU policies for the benefit of EU citizens and that fundamental rights are well protected. To enable the European Parliament to fulfil this role, the management needs to be transparent and fulfil reporting requirements, as confirmed in the legal instruments establishing the systems. Its role consists of an *ex-ante* influence through the annual budgetary procedure, *ad interim* involvement by receiving regular reports and briefings, and an *ex-post* control through the process of budget discharge. Sometimes the European Parliament requests the nomination of a representative and/or observer on management boards and management committees (e.g. the European Environmental Agency) but any executive role goes beyond the formal duties of the European Parliament. For the purposes of this study, it is suggested that the budgetary and budget discharge rights of the European Parliament, as well as a right to question the main responsible person of the Management Authority and to receive regular reports, is sufficient to fulfil the European Parliament's statutory supervisory function.⁶⁰

Options	Impacts: responsiveness to the requirements and views of Member States, the Commission and the EP	Rating
Baseline	<p><u>Influence of Member States:</u> control resides with the Commission, with no direct influence of Member States on operational management other than through the comitology procedure</p> <p><u>Influence of the Commission:</u> the Commission is charged with developing and running the system and is fully accountable for its execution, even though this is entrusted to two Member States. The Commission is in control but is not a beneficiary of the system and will be brokering the interests of the users.</p> <p><u>Influence of the European Parliament:</u> through its supervision over the Commission, the European Parliament has effective oversight and control over</p>	*

⁶⁰ In the interviews, Members of the European Parliament (MEPs) and Member States agreed with this approach.

	the management of SIS II, VIS and EURODAC, but may find that in practice, management by a Member State leads to concerns over transparency.	
Baseline+	As with Option 1	*
Regulatory Agency	<p><u>Influence of Member States:</u> it is likely to favour the role of Member States, through the Management Board. The Agency could be given responsibility for deciding on several issues related to the operational management. This would increase the influence of the Member States on the operational management compared to the Baseline and Baseline+ options.</p> <p>This option would be acceptable to national police authorities as the new Agency would cover both first pillar (border control) and third pillar aspects (police and judicial cooperation in criminal matters).</p> <p><u>Influence of the Commission:</u> the Commission retains varying degrees of influence over certain functions through implementing measures. These are discussed in the comitology, which also involves Member States. This concerns, inter alia, the determination of the regions for the roll-out of the Visa Information System, if such a Commission decision still needs to be adopted to cover all the regions (Art. 48(3) of the VIS Regulation). This decision requires different policy deliberations like the risk of illegal immigration, threats to the internal security of the Member States and the feasibility of collecting from all locations in a region.</p> <p>For certain other critical tasks the Commission may be assigned a direct responsibility; e.g. budget, work programme and appointing the Director.</p> <p>The Commission should continue to be responsible for some tasks related to the Communication Infrastructure (network) of SIS II and VIS: tasks relating to implementation of the budget; acquisition and renewal; contractual matters.</p> <p><u>Influence of the European Parliament:</u> clear financial and management reporting by the Agency gives the European Parliament a transparent insight into its operations, thus facilitating its</p>	***

	supervisory tasks.	
FRONTEX	<p><u>Influence of Member States:</u> the current influence is high. However the governance structures of FRONTEX may need to be adapted to accommodate decision-making as required for operational IT management. FRONTEX could be given responsibility for deciding on some of the more technical issues covered by the implementing measures in the legal instruments establishing the systems. This would increase the influence of the Member States on the operational management compared to the Baseline and Baseline+ options.</p> <p>However, the acceptability of this option by national police authorities is questionable as the current activities of FRONTEX only cover first pillar (border control) and not third pillar aspects (police and judicial cooperation in criminal matters).</p> <p><u>Influence of the Commission:</u> the Commission has two representatives in the Management Board. It approves the work programme and proposes candidates for the post of the executive Director. It has also an important role in the establishment of the budget.</p> <p>In the future, adoption of implementing measures like the determination of the regions for the roll-out of the Visa Information System and certain tasks related to the Communication Infrastructure (network) of SIS II and VIS should remain with the Commission (similar to the Regulatory Agency option).</p> <p><u>Influence of the European Parliament:</u> the European Parliament's influence is similar to Option 3 (Agency), however the budget and the operational reporting of the IT management will be less visible, being only part of the total activities of FRONTEX.</p>	***
Europol	<p><u>Influence of Member States:</u> Member States have full control over Europol and there is already a solution at the level of the Management Board for dealing with IT issues. Europol could be given responsibility for deciding on some of the more technical issues covered by the implementing measures in the legal instruments establishing SIS II. This would increase the influence of the</p>	*

	<p>Member States on operational management compared to the Baseline and Baseline+ options.</p> <p><u>Influence of the Commission:</u> it has currently a limited influence over Europol.</p> <p><u>Influence of the European Parliament:</u> its role would be rather limited as Europol has been established as a third pillar Agency and – as with FRONTEX - it will not be dedicated to IT management, making public scrutiny more difficult.</p>	
--	--	--

2.2. Transparency (accountability, decision-making) vis-à-vis citizens and the system's users and supervisory bodies

The more systems with different legal instruments there are the more complicated decision-making within the Management Authority is likely to become. This complexity is compounded when the legal bases fall under different ‘pillars’, as is the case with SIS II. This could impact the governance structure, voting rules and rules of procedure. The Lisbon Treaty will change this situation as the pillar structure will be abolished.

The SIS II and VIS legal instruments determine the reporting requirements of the Management Authority, thus reporting would be the same under all options. The format for reporting the execution of the work programme and presenting the budget will follow standard EU procedures, and thus will be easily accessible to EU policymakers and supervisory authorities.

If an institution combines policymaking, services development and operational management down to procurement, it would acquire substantial control over the most critical steps in developing and managing these systems. From the perspective of accountability, a separation of functions would be preferable as responsibilities become clear and decisions over allocation of funds become more transparent. There is an obvious trade-off with policy coherence.

The effective unrestrained access of supervisory authorities, notably the Court of Auditors and European Data Protection Supervisor, is a legal requirement to ensure transparency.

Options	Impacts: transparency (accountability, decision-making) vis-à-vis the citizens and the system's users and supervisors	Rating
Baseline	<p><u>Transparent management:</u> The fact that the Commission is not directly implementing the daily management tasks, while remaining accountable for them, could lead to a decreased level of transparency.</p> <p><u>Reporting and supervision:</u> management under control of the Commission will ensure effective</p>	**

	<p>reporting and substantial guarantees for control, and fraud prevention (European Parliament, OLAF, Court of Auditors). The same rules apply to the operational management by two Member States, as this is an execution of the Commission's responsibility, for which it is fully accountable.</p> <p><u>Concentration of control:</u> notwithstanding the guarantees and established practices, management by the Commission would imply that the Commission acquires substantial control over all aspects of the systems, which reduces the checks and balances that would be prevalent with more involvement of the Member States. Furthermore, the integration of parts of operational management and coordination functions in a large organisation as the Commission will make it more difficult to monitor.</p>	
Baseline+	Same as Option 1	**
Regulatory Agency	<p><u>Transparent management:</u> a Regulatory Agency will have a Management Board, for which membership and voting procedures need to be established. The Board will need to represent various constituencies of the different systems. The tasks of such a board must be delineated with respect of the Commission's responsibilities and comitology procedures.</p> <p><u>Reporting and supervision:</u> it may be expected that a dedicated Management Authority will allow better financial oversight as all expenditure will be accounted for in the budget of the Regulatory Agency. It would also need to comply with the same rules as the Commission, and be supervised by the same organisations (European Parliament, OLAF, Court of Auditors).</p> <p><u>Concentration of control:</u> a Regulatory Agency involves all stakeholders and provides the best guarantee to distribute control among Member States (Management Board) and the Commission (direct and through comitology).</p>	***
FRONTEX	<p><u>Transparent management:</u> management by FRONTEX is similar to a new Regulatory Agency, in the sense that it has a comparable management and governance structure and it also needs to comply with the same rules as the Commission, and is supervised by the same organisations (European Parliament, OLAF, Court of Auditors).</p>	**

	<p><u>Reporting and supervision</u>: FRONTEX has many other activities and it would be more difficult to single out the SIS II, VIS and EURODAC related activities and expenditures.</p> <p><u>Concentration of control</u>: similar to Option 3</p>	
Europol	<p><u>Transparent management</u>: having two different regimes for the management of SIS II and other Europol activities, implies the need to isolate all functions and activities relating to SIS II, otherwise there may be gaps or overlaps in both regimes.</p> <p><u>Reporting and supervision</u>: whereas the SIS II legal base clearly defines the competence of supervisory bodies over the management of SIS II, the oversight by European Parliament, OLAF, European Data Protection Supervisor, national data protection authorities, over Europol as a whole is limited. As with FRONTEX, Europol has many other activities and it would be more difficult to single out the SIS II, VIS and EURODAC related activities and expenditures. If SIS II were to be managed by Europol and VIS by the Commission, this would allow oversight authorities to compare (whilst taking into account the differences of the systems) the management performance in both systems. Currently no performance benchmarks are readily available.</p> <p><u>Concentration of control</u>: control over VIS, SIS II and EURODAC will differ, thus effectively reducing any one organisation's control. However for SIS II, the control will be firmly with the Member States, without an effective role for the Commission and the European Parliament.</p>	*

2.3. Effectively adding new Member States

Any new State joining the systems brings with it legal, governance, technical, operational, and possibly even political consequences. These impacts are likely to be the same for all options and do not help to differentiate between them. A new Member State is obliged to apply the *acquis* and has the same rights and obligations as all other Member States. Associated countries would also need to adopt the *acquis* and would be offered a regime similar to existing associated countries like Norway and Iceland.

From the governance perspective, the impact of a new member participating in a system is determined by its status (EU Member State or not) and the level of involvement (opt-ins and opt-outs). Incorporating new members into a dedicated structure is easier than accommodating them within an existing organisation with

another remit, governance structure and potentially other members. It is hardly foreseeable that a new member would participate in VIS, and/or SIS II, and/or EURODAC without also being a member of the hosting organisation. This means that a potentially cumbersome alignment of the participation rules in the hosting organisation may be necessary.

Options	Impacts: effectively adding in new MS	Rating
Baseline	Absorbing new Member States in existing Commission practices and procedures.	***
Baseline+	The same as option 1	***
Regulatory Agency	Membership and voting rights in the Management Board need to be determined, taking into account the extent to which the new member is participating in the systems. Once the Agency is established, the existing rules should be relatively easy to apply to a new Member State.	**
FRONTEX	<u>Complexity</u> : potential complexity in (non-)dual membership issues	*
Europol	<u>Complexity</u> : potential complexity in (non-)dual membership issues	*

2.4. Responsiveness to the requirements and views of other stakeholders

Effective and up-to-date technology management requires a close interaction with service providers, system developers, and other crucial suppliers of IT equipment and software from the private sector. There is no formal role for non-state actors in any of the options.

Firstly, any Management Authority would be looking for active technological support and direct interaction with the users of the systems, to ensure that the best solutions are provided that are the state of the art in quality of service, security, data protection and which correspond to the needs of the users.

Secondly, management should be able and willing to respond to and engage with the representatives of data subjects and civil society organisations to ensure that data protection standards are met, and that (perceptions of) the organisation's data protection record is positive. Finally, the Management Authority should inform the public at large of its activities and objectives beyond the formal reports to the European Parliament and other instruments, such as the annual work programme.

Options	Impacts: responsiveness to the requirements and views of other stakeholders	Rating
Baseline	<u>Interaction with IT supply industry</u> : a permanent and interactive constructive dialogue with systems' and	*

	<p>technology suppliers is complicated by the Commission's lengthy procurement procedures. The Commission policy on internal rotation of staff may also imply that less long-term relationships and networks develop with the stakeholder community.</p> <p><u>Accessibility (e.g. for civil society):</u> the Commission as a very big organisation is not easy to approach and target for specific issues. Moreover, the Member States' authorities which are in practice carrying out the operational management tasks are less likely to be responsive to interaction with stakeholders other than those directly involved with the testing and running of the systems, as this would be the Commission's prerogative.</p>	
Baseline+	Same as Option 1.	*
Regulatory Agency	<p><u>Interaction with IT supply industry:</u> it would become a centre of excellence for large-scale high-availability and high-security IT systems and thus attract and engage with the community of suppliers and users of such systems. Its relationship with suppliers is possibly more transparent than with the Commission, where one supplier may be servicing many different departments. Implementation of procurement rules can be more targeted to its needs than in the case of the Commission.</p> <p><u>Accessibility (e.g. for civil society):</u> a single dedicated structure is likely to be more visible and approachable. Through the direct involvement of the Member States in the governance of the Regulatory Agency the network function of the organisation is substantial from the outset.</p>	***
FRONTEX	<p><u>Interaction with IT supply industry:</u> it currently serves a specific constituency in the border control area, which has only partial overlap with the users of the SIS II, VIS and EURODAC. Once the IT department is established, it is likely to have some of the same advantages as a dedicated Agency as it combines various systems and is likely to become a centre of excellence. As FRONTEX' remit will remain wider than managing IT systems, its procurement rules are likely to be less adapted to the specific requirements linked to the purchase of software, systems and IT consultancy.</p> <p><u>Accessibility (e.g. for civil society):</u> its wider remit also makes it less recognisable to the outside world</p>	**

	(including civil society) as the responsible organisation for management of large-scale IT systems in the area of JHA.	
Europol	<p><u>Interaction with IT supply industry</u>: Europol will have less opportunity to develop into a centre of excellence for management of IT systems than the other options that benefit from joint management of VIS, SIS II and EURODAC.</p> <p><u>Accessibility (e.g. for civil society)</u>: Europol is well aligned with the constituency of SIS II, and should be accessible to this community. It is visible and recognisable, as a police organisation to the outside world and will be prepared to communicate and engage as such.</p>	**

2.5. Degree to which alignment with JHA policy and a broader EU policy is enabled

Decisions on new functionalities of the systems, access categories or anything that would have impact on the legal instruments establishing the systems would be made by the European Parliament and the Council. This is beyond the scope of the operational management. What is relevant is that the operational management is aware of the policy context and the objectives that the system is supposed to support and how this may evolve over time. In particular, in designing an IT strategy, it is important to consider what future developments in the systems should be taken into account.

To reduce the risk of functional disconnection between (general) EU policy objectives in justice, freedom and security and the working of the systems, formal links between policy development and operational management are required. Having both functions within the same institution would probably be the best guarantee for consistency and effective translation of policy into operational and technical requirements. However, this may raise concerns about the accumulation of power within one institution or organisation.

In addition, the joint management of all three systems, with consistent decision-making and governance structures and procedures can also be considered as an important step towards alignment with the broader EU policy.

Options	Impacts: degree to which alignment with EU policies is enabled	Rating
Baseline	<p><u>Alignment with a wider EU policy</u>: management by the Commission is likely to ensure optimal coherence across all EU policy fields – including beyond the sphere of justice, freedom and security - due to the use of methods of internal coordination and information.</p> <p><u>Alignment with the justice, freedom and security</u></p>	***

	<p><u>policy</u>: DG JLS, as the primary policy-making DG in the area of freedom, security and justice, currently also manages EURODAC and the development of VIS and SIS II. It will remain the authority which deals with the joint SIS II and VIS facility in the interim period and is (directly or through comitology) responsible for all tasks entrusted to the Commission by the SIS II, VIS and EURODAC legal bases. Thus consistency and coherence of policy and operational management is expected to be high. Even if daily management of the systems were carried out by two Member States, which may be influenced by national instead of EU policy contexts, the Commission has full operational responsibility and should be able to effectively assert its control.</p>	
Baseline+	Same as Option 1	***
Regulatory Agency	<p><u>Alignment with a wider EU policy</u>: The Commission's role in the Agency through its presence in the Management Board, as well as influence in particular on the budget and the work programme, would allow the management of large-scale IT systems to be aligned with wider policy areas.</p> <p><u>Alignment with justice, freedom and security policy</u>: similar to alignment with wider EU policy</p>	***
FRONTEX	<p><u>Alignment with a wider EU policy</u>: similar to <u>Option 3</u></p> <p><u>Alignment with justice, freedom and security policy</u>: although FRONTEX is not competent to develop policy, the organisation and its constituency are clearly rooted in the area of border control. It may therefore be expected that it has a natural tendency toward these policy areas, which may lead it to be less sensitive towards, or unaware of, broader issues of EU policy (in justice, freedom and security and beyond). However, the participation of the Commission in the Management Board and its role in approving the work programme could ensure that the wider context of JHA policies is taken into account in the decisions regarding the management of SIS II, VIS and EURODAC</p>	**
Europol	<p><u>Alignment with a wider EU policy</u>: is likely to be difficult given the narrow focus of Europol. This is</p>	*

	<p>the only option where the systems are managed by different institutions. This reduces the potential for consistency and coherence, which may be achieved through joint management.</p> <p><u>Alignment with justice, freedom and security policy:</u> Europol's objectives are complementary with those of SIS II. Thus it is expected that 'thematic alignment' would not raise too many problems. There may be an issue with Europol's investigative nature, which may lead it to seek a broader use of SIS II as an investigative tool, a purpose for which it has not been designed. Moreover, the minimal involvement of the Commission in decision-making in Europol, would make alignment with wider justice, freedom and security policy more difficult.</p>	
--	---	--

2.6. Incorporating 'Géométrie variable'

No option provides for an equal position for non-EU Member States. Between the options, however, there are differences in the possible level of involvement by non-EU Member States. The form in which this happens could be a memorandum of understanding or a clause in the general association agreement between the EU and these countries.

The VIS and SIS II legal instruments are characterized by a similar '*géométrie variable*'.⁶¹ As regards EURODAC, the '*géométrie variable*' is different. The UK and Ireland took part in the adoption and application of the EURODAC Regulation.⁶² Originally Denmark was not bound by it⁶³ but later concluded an international agreement with the European Community and therefore participates effectively in EURODAC. Switzerland will be an associated member once the agreement between Switzerland and the Community signed in 2004 is ratified and enters into force.

The *géométrie variable* needs to be accommodated at the level of comitology, Council working parties and, in case of an Agency, the Management Board. In all these cases it will be difficult to find common voting procedures for decisions which concern all systems – e.g. election of the Director, rules of procedure, investment in common infrastructure – which would take account of the variation in status of the participating countries. System-specific issues could allow for procedures that take the *géométrie variable* into account, however in practice this will lead to complicated agendas with Member States joining and leaving discussions, depending on the subjects under discussion.

The new Treaty will not entail significant changes with regard to the participation of the United Kingdom, Ireland and Denmark and the associated countries in decision-making.

⁶¹ Recitals 22–28 VIS, 27–36 SIS II.

⁶² Recital 20 EURODAC Regulation

⁶³ Recital 21 EURODAC Regulation

Options	Impacts: incorporating ‘ <i>Géométrie variable</i> ’	Rating
Baseline	Management by the Commission does not allow non-EU Member States much influence over decision-making, as whilst they are participating in the comitology committees, they do not have the right to vote. In practice most concerns of associated countries are taken into consideration in a seemingly satisfactory manner. Participation of non-EU Member States would require an additional specific agreement to be negotiated in the context of the general association agreement between the EU and these countries.	***
Baseline+	Similar to Option 1 but bringing EURODAC under joint management creates more complexity as its membership differs from VIS and SIS II.	***
Regulatory Agency	<p>Agreements between third countries and the European Community, providing for the adoption and application of Community law in the relevant area, are necessary.⁶⁴ Such participation may be established through an Arrangement between the European Community and the relevant country.⁶⁵</p> <p>A new Agency could copy effective practices from FRONTEX, and provide even better <i>ad hoc</i> solutions, dealing with the particularities of the three systems. The rules of procedure established by the Board may contain specific clauses on the</p>	***

⁶⁴ An example for such a non-EU Member States participation is Turkey’s membership in the European Environmental Agency based on an Agreement between the European Community and the Republic of Turkey that has been approved by Council Decision 2001/594/EC of 18 June 2001 on the conclusion of the Agreement between the European Community and the Republic of Turkey concerning the Republic of Turkey's participation in the European Environment Agency and the European environment information and observation network in OJ 2001 L 213 of 07.08.2001.

⁶⁵ Arrangement between the European Community and the Republic of Iceland and the Kingdom of Norway on the modalities of those states' participation in the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (OJ L 188 of 20.2.2007, p. 15).

	participation of these countries.	
FRONTEX	Participation may be established through an Arrangement between the European Community and the relevant country. ⁶⁶ FRONTEX has an established system to deal with the 'géométrie variable' in the context of Schengen cooperation (but not the Dublin acquis) but not all the Member States participating in the systems are members of FRONTEX.	**
Europol	Membership of Europol is currently limited to the EU Member States. Adding associated countries would require putting in place some specific arrangements.	*

3. FINANCE

3.1. Implementation costs

The main costs for all the options are connected to running the systems and will have to be borne under any of the options. It is assumed that both FRONTEX and Europol would have to hire the same number of staff and obtain new/additional facilities comparable to those a new Regulatory Agency would have to acquire. The price might differ according to the location but, since it has not been decided yet where the systems and their management should be located, it is difficult to make any assumptions on this matter. A detailed analysis of implementation costs for the baseline option and the preferred option is available in section 9 of the Impact Assessment Report.

3.2. Critical mass: exploiting synergies

The prime influencing factor is the co-location of management and operational staff. Operational, organisational and security arguments support this approach. Technical reasons, including the dependence on the Biometric Matching System (BMS), would require a decision to co-locate the systems. High security requirements do not allow remote access to the systems, which limits the possibility to work off-site. From an organisational point of view, there are very few tasks that do not require direct daily contact with operations; examples would be procurement, legal issues, financial planning, accounting, external representation and interaction with main stakeholders. These are all tasks with varying time requirements, usually spread over different profiles. The senior facility manager – equivalent to the current Director of the Strasbourg facility – would need to be on-site to allow management of human resource matters, decision-making in emergency cases, maintenance of relationships with the local security environment (police), and so forth. As the highest-ranking official would be on-site, it would make little sense to set up a new entity in another location for the few tasks that could be delivered remotely.

⁶⁶ idem

The key drivers of synergies are the possibility of sharing a common facility (e.g. sharing capital and operational investments and running costs between a larger number of systems), a common technology platform, and the utilization of common overhead and support functions and accordingly, the ratio of operational staff versus overhead staff.

The management of the three systems by the same authority would allow important savings. Technical, logistical and infrastructure costs, such as: human resources, power, air-conditioning, IT data centre structural requirements and physical security of buildings could be shared for the three systems. This concerns not only one-off capital installation costs but also annual (running) costs.

The following savings resulting from a common management structure for SIS II and VIS have been identified so far:

- An entity that is responsible for multiple IT systems would be better positioned to take care of procurement, as larger contracts may attract bids of higher quality, allowing more optimal outcomes.
- If SIS II and VIS were managed together, it is estimated that around 75 staff would be required (around 39 for SIS II, 20 for VIS, 10 for BMS and 6 administrators for the back-up site) to operate the systems.

If the management of the systems were separated, it is estimated that 106 persons in total would be necessary (39 for SIS II, 39 for VIS, 20 for BMS and 8 administrators for the back-up sites).

All ancillary costs, such as training and its coordination would have to be replicated instead of shared. For instance, the security guards (24/7/365) and other ancillary staff would have to be replicated for each of the systems and on multiple sites, involving significant costs:

- Co-location in terms of network installations demonstrates the synergies to be had in terms of installations, management and monitoring. Although SIS II and VIS have separate networks and equipment is installed separately for each system at the central sites, SIS II and VIS share the same management platform for their cryptographic devices and they also share the same monitoring tools. Dissociating the two systems in terms of location would require a duplication of the management platform, the monitoring tools, and of course the staff needed to manage and monitor the networks. Other network-related costs incurred by such a move would include the potential extension of the network and the added complexity and cost of on-site interventions such as if and when faults occur on the lines or equipment.
- If SIS II and VIS were dissociated, they could not share the BMS technical infrastructure that was intended to inter-act with both, as a sub-component. The offer price for BMS-VIS was €15.8 million and - if the same infrastructure were to serve SIS II (i.e. all systems co-located at the same site) the offer price for SIS II was €3.9m. This would mean that, in case of the separation of the two systems, the costs for BMS-SIS II could be the equivalent of those for VIS, i.e. €16 m (approx) instead of €3.9m.

Furthermore, it is unlikely that a centre of excellence could be achieved for one system alone. Separation of these systems would lead to the opportunity cost of not having achieved synergies in expertise and know-how in large-scale IT systems.

Finally, adding EURODAC and any other large-scale IT systems would increase the synergies in installation and running costs, as well as in staff numbers. It is also planned that EURODAC, in the future, will use BMS. Managing it separately from the SIS II and VIS would therefore mean duplicating equipment costs.

Synergies and likely costs will be dealt with in more detail in section 5.1.

Options	Impacts: Critical mass – Exploiting synergies	Rating
Baseline	<p><u>Synergies in overhead cost:</u> synergies in overhead costs could be limited as similar roles and functions would be required in the Commission and the French authorities (legal, financial, procurement)</p> <p><u>Synergies in operational staff:</u> other than with the Baseline+ option, the potential increase in staff requirements due to the up-grade of EURODAC to EURODAC II cannot be absorbed in the SIS II and VIS management.</p> <p><u>Synergies in shared facilities:</u> maintaining facilities for EURODAC; moreover, the current facilities are not future proof and will not allow new systems to be added.</p>	**
Baseline+	<p><u>Synergies in overheads:</u> similar to Option 1 but no dedicated operational Commission staff required for EURODAC.</p> <p><u>Synergies in operational staff:</u> operational staff requirements for EURODAC likely to be absorbed by the operation that is running SIS II and VIS.</p> <p><u>Synergies in shared facilities:</u> all three systems in one facility. The current facility is not future-proof. This option allows for attracting other Member States to offer a facility. Creating some competition should reduce price and increase pressure to invest in a new custom-built facility, which is future-proof.</p>	***
Regulatory Agency	<p><u>Synergies in overheads:</u> setting up a new Agency with a full governance structure, acting semi-independently from the Commission and the Member States, would probably create some cost inefficiencies in the short term, as there are likely</p>	***

	<p>to be sub-critical/under-utilised corporate and support functions, if only three systems reside under its control. With the addition of new systems an optimal balance could be reached.</p> <p><u>Synergies in operational staff:</u> can be optimally exploited by a dedicated Regulatory Agency.</p> <p><u>Synergies in shared facilities:</u> any initial redundancies will probably be exploited by future developments in the area of freedom, security and justice,</p>	
FRONTEX	<p><u>Synergies in overheads:</u> similarly to setting up a new Regulatory Agency, FRONTEX would probably have to set up a separate directorate dedicated to SIS II, VIS and EURODAC management activities. There could be some gains in overheads in the horizontal functions (human resources, procurement, legal). However, since 75 additional staff would be necessary to manage VIS and SIS II, the impact of effectively doubling the workforce should not be underestimated, in terms of organisational change, added overheads and shift in core tasks. It is also likely that additional support staff would have to be made available, since at the moment FRONTEX only has sufficient administrative resources to deal with its existing 170 staff.</p> <p>The synergies in procurement and a better bargaining position would also be limited, as the management of the systems is significantly different to the core business of FRONTEX and therefore the scope of procured goods and services would be different.</p> <p><u>Synergies in operational staff:</u></p> <p>The same as in the case of a Regulatory Agency</p> <p><u>Synergies in shared facilities:</u> if the systems are relocated to the FRONTEX location, the synergies with the existing structure would be limited. FRONTEX would have to ensure a similarly secure location to the one in which the systems are currently located (equivalent of secure nuclear bunkers). A new facility would address the current and future requirements for hosting large scale IT systems in the area of freedom, security and justice.</p>	***

Europol	<p><u>Synergies in overheads:</u> As Europol would not be entrusted with the management of VIS and EURODAC, the synergies would be even less notable than in the case of FRONTEX, although there would possibly be some limited synergies with Europol's own IT system. At the moment Europol has around 470 staff and, as in the case of FRONTEX, adding 75 new staff could result in disequilibrium if the support functions are not strengthened.</p> <p><u>Synergies in operational staff:</u> some synergies would be likely with the existing IT department; however separation of VIS and EURODAC means that a lot of operational synergy potential is lost.</p> <p><u>Synergies in shared facilities:</u> a joint facility would avoid doubling maintenance and security costs, and increase efficiency concerning the use of air-conditioning, emergency generator capacity, etc. However this option would mean that VIS and EURODAC would be located elsewhere, thereby foregoing many of the synergies that a single location would offer, e.g. a common network and a common technical platform.</p>	*
---------	---	---

3.3. Ability to acquire the right funding levels and resources

The system must have the capacity to ensure continuity and be able to absorb emergency situations. This requires a substantial annual budget for running costs for facilities and staff. These redundancies should be maintained and safeguarded against cost cutting exercises. It is likely that a dedicated facility can effectively defend this position, whereas in larger organisations there will be competition for the available resources. This could be especially the case where the management of IT systems is not a core activity and where additional pressure to release the redundancies in favour of cost-savings can be expected.

Options	Impacts: ability to acquire the right funding levels and resources (running cost)	Rating
Baseline	<p><u>Sustainability of funding level:</u> the contribution to the SIS II/VIS/EURODAC operational management is part of the general budget of the EU. This provides a solid financial basis. In the budget it is visibly identified for this purpose, facilitating stakeholders to monitor the Commission's budget allocation to these tasks. Nevertheless the Commission is under pressure to reduce costs and any activity that is under its direct responsibility will be affected.</p>	**

	<p>Any Commission option would be funded from the DG JLS operational budget, which is renewed annually. Overall funding levels would be assured for periods of 7 years, in line with financial perspectives. However, the Commission may be confronted with continuous political pressure to reduce human and financial resources, which could impact the number of staff in the Commission in supervisory and management functions, with the risk of losing effective control over operations</p> <p><u>Financial flexibility</u>: various budget lines feeding the VIS, SIS II and EURODAC operations and the development of future systems. The Commission has a degree of flexibility to move funds across budget lines.</p>	
Baseline+	Same as Option 1	**
Regulatory Agency	<p><u>Sustainability of funding level</u>: an Agency would have a dedicated budget line in the general EU budget, which would give it significant financial stability. Agencies have their own financial rules based on the framework Financial Regulation for agencies. In practice Regulatory Agencies comply with the Framework Financial Regulation (FFR)⁶⁷. Deviation from the FFR is only allowed after agreement by the Commission.</p> <p><u>Financial flexibility</u>: budget procedures in an Agency are relatively rigid and follow an annual plan. However, a clear, dedicated budget, with full involvement of the key stakeholders (Member States) that are likely to defend the Agency's appropriate funding as it concerns a direct service to them, could provide a sufficient degree of</p>	***

⁶⁷ COUNCIL REGULATION (EC, EURATOM) No 1995/2006 of 13 December 2006 amending Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities

	flexibility.	
FRONTEX	<p><u>Sustainability of funding level</u>: several sources of funding⁶⁸ provide FRONTEX with a degree of flexibility, but also planning uncertainty.</p> <p><u>Financial flexibility</u>: the budget procedure and annual planning are rigid, leading to uncertainties in the availability of funds. The budget for SIS II/VIS/EURODAC would be part of the overall budget of the Agency, and as such more difficult to identify. Furthermore, running IT systems is not a core function for FRONTEX, thus it is expected that there would be internal competition for resources.</p>	***
Europol	Similar to Option 4 (FRONTEX) though currently Europol is financed from various sources.	**

3.4. Transition costs

Transition costs are directly related to the transfer of the system or its management to a new location and the delay in establishing a new Management Authority. There are moving costs, costs of loss of expert knowledge, costs of risk involved with relocating (discontinuity potential, failure of the system, potential network failure, and damage to equipment), investments in new infrastructure, staff training, legal costs, etc.

The SIS II and VIS legal instruments (Articles 4(3) and 27 respectively) explicitly determine Strasbourg (FR) for the main facility and Sankt Johann im Pongau (AT) for the back-up facility. However, under some management options relocation of the systems would be required, or at least highly desirable, to ensure co-location of management and operational activity. As relocation is an important driver of transition costs it is necessary to assess the basis on which such relocation would occur. Theoretically the operational and managerial tasks could be split, allowing the Management Authority to be in another location from the systems. Most operational functions including the site manager (Director) are location-based. Most activities are on the system and the database, which in part is due to the strict security requirements that ensure limited access. The few support functions (legal, financial, procurement) that could be provided from a distance may not justify setting up a dedicated separate structure, as these are likely to be under-utilised. There seems little justification for having these functions outside the location where the Director resides.

⁶⁸ Article 29.1 of the FRONTEX Regulation specifies that the revenue of the Agency shall consist, without prejudice to other types of income, of:

- a subsidy from the Community entered in the general budget of the European Union (Commission section),
- a contribution from the countries associated with the implementation, application and development of the Schengen *acquis*,
- fees for services provided,
- any voluntary contribution from the Member States.

Finally, a split of locations would result in substantial extra coordination costs, travel costs and time lost in travelling between locations.

In case of relocation the main cost will be the investment in the new facility. However, it is likely that under all options a new facility or at least a substantial update of existing facilities will be required, as the Strasbourg facility is not equipped to house the necessary staff numbers. Nor is it equipped to cope with new or bigger systems from a technical infrastructure point of view. Thus France would also need to build and provide a new facility that is future-proof.

Therefore the investment in facilities would not differ widely between the options.

The timing of the relocation of the systems may also affect the depreciation schedule of the hardware; leading to either a delay in investment (which usually leads to more continuity and maintenance costs) or early write-off of existing equipment if is not yet depreciated when the new facility goes live. However, hardware is only part of the infrastructure as a whole and its replacement shall not be seen as the only determining factor of a possible relocation.

These transition costs can be considerable, but are one-off costs and therefore less relevant for determining which option to choose, even though they may differ substantially from option to option.

Finally, the relocation of EURODAC is likely under all options. More precisely, the successor system (EURODAC II) will be running on the sTESTA network as does the current EURODAC and will be supported by a version of the BMS (which has a service-oriented architecture) and, thus sharing more features with SIS II and VIS than at present. Maintaining a separate infrastructure for a system such as EURODAC is not cost-effective, and would not make sense from a technical and operational management perspective.

Options	Impacts: transition costs	Rating
Baseline	<p><u>Low transfer cost expected</u></p> <p><u>Re-location</u>: under any option a new facility is likely to be required in the longer run, but as it would remain in the same location and as there is local experience in building such a facility, the planning of its design and construction and of the transfer of systems during the transition period would be facilitated.</p> <p><u>New facility</u>: initially no immediate investment in a new facility would be needed, but office space limitations at the Strasbourg site are already a problem and there also is a lack of space for hosting new systems.</p>	***

Baseline+	<p><u>Low transfer costs expected:</u> EURODAC would need to be transferred, but costs would be expected to be limited as the transfer could coincide with the development of the new EURODAC II.</p> <p><u>Relocation/New facility:</u> the main difference is that under the Baseline+ option the Commission may decide to tender the service contract leading to competition among Member States which would like to host the systems, which could lead to a lower price.</p>	***
Regulatory Agency	<p><u>Re-location:</u> transfer of management to a Regulatory Agency does not automatically imply relocation of SIS II and VIS central units. The Regulatory Agency could be set up in Strasbourg. The SIS II and VIS back-up sites in Austria (as defined locations in the respective legal instruments) would not be impacted. However, this option would have an impact on EURODAC currently managed in Luxembourg and Brussels.</p> <p>There may be resistance to this solution, as there has been pressure in the Council that new Agencies will be set up in the new Member States. Moreover, there could be other Member States than France offering existing or new facilities. The remote management of the systems, where the administrative functions are separated from the site hosting the SIS II, VIS and EURODAC could be considered as an option. However, there are not enough administrative functions/positions to justify splitting management from operational tasks on the system. This would only lead to extra coordination costs, travel costs and time lost in travelling between the separate locations.</p> <p><u>New Facility:</u> the investment in a new facility would initially be higher in the case of re-location, but as stated the current facility would need to be replaced anyway in the medium to long-term to accommodate staff for all the systems. Furthermore, a custom-built site would have lower operational expenditure and running costs and thus would be cheaper in the long-term.</p>	*
FRONTEX	<p><u>Relocation:</u> management by FRONTEX (Warsaw) would not explicitly require relocation of the CS-SIS, CS-VIS to Warsaw, as some central management functions can be separated from operational tasks –</p>	**

	<p>thus creating a separate management layer in Warsaw. Alternatively the Strasbourg facility could be run as a separate FRONTEX department, with the site manager (Director) reporting directly to the FRONTEX Director. Thus ideally the systems would also be transferred under this option, with all the consequences of relocation that were mentioned previously (human resources, legal, continuity risk), but with the advantage of having a custom-built facility.</p> <p><u>New facility:</u> as in previous options, initially dependent on a decision to relocate, but a new facility would be needed in any case.</p>	
Europol	<p><u>Relocation:</u> as with the FRONTEX option; relocation of SIS II to Europol's seat in The Hague would be expected, though start-up should be smoother given Europol's existing expertise, staff and infrastructure for managing IT systems.</p> <p><u>New facility:</u> as new Europol facilities are currently under design, the specifications for integrating the SIS II would need to be determined soon. If not, this would have to be retro-fitted, potentially increasing the cost and leading to higher running costs down the line.</p>	**

3.5. Access to additional funding for incidental extra costs

Any Management Authority would need to be in a position to respond in an appropriate and timely manner to emergency situations or requests from Member States to accommodate specific events (like the G8, or the World Football Championships). This assumes that the Management Authority will need to be able to absorb these incidents within its existing resources or have rapid access to extra resources, if the need exceeds the regular level of a security reserve that could be retained on the annual budget.

Funding from programme appropriations provides more scope for increase or adjustment than from the administrative appropriations of the EU budget. However in the case of additional funding a larger organisation such as the Commission or Europol may be more flexible as it can shift operational funds between budget lines. Other means of financing are permitted and thus the Member States could decide to contribute directly to the financing of additional requirements outside the annual work programme of the Management Authority.

Annual work programmes generally do not provide for rapid access to additional Community funds in the case of emergencies or sudden requirements.

Options	Impacts: access to additional funding for extra costs	Rating
---------	---	--------

Baseline	<p><u>Access to finance</u>: more latitude to re-allocate funds throughout the year – due to limited margins in the general EU budget, or budget of the DG JLS - than organisations with fixed annual budgets.</p> <p><u>Speed of decision-making</u>: the Commission has the advantage of being able to decide more rapidly, than a structure where the Member States would all need to agree. However, this advantage presupposes that cooperation with the Member States responsible for operational management is effective and efficient.</p>	***
Baseline+	Same as Option 1	***
Regulatory Agency	<p><u>Access to finance</u>: Agencies have annually fixed budgets and work programmes, and have little means of acquiring additional funding from the general budget of the EU, outside the annual budget cycle. Also an Agency would be able to attract resources outside the general budget of the EU; e.g. if the service is delivered to a specific Member State that Member State can be asked to allocate extra resources.</p> <p><u>Speed of decision-making</u>: within the restrictions of the annual cycle a dedicated Agency is likely to be best equipped to receive and direct such funds to specific tasks in a transparent manner.</p>	**
FRONTEX	<p><u>Access to finance</u>: the procedure for establishing an annual work programme can be an obstacle to effective execution. Delays in adoption could render it difficult to commit funds in a timely manner.</p> <p><u>Speed of decision-making</u>: the work programme is a rigid instrument that is difficult or (practically) impossible to change during the year due to heavy procedures.</p>	**
Europol	<p><u>Access to finance</u>: Europol is financed mainly from Member States' contributions. The limits of these contributions are determined by its budget adopted by the Council. It is therefore able to tap into a wide funding base, and should be flexible in generating the required funds.</p> <p>It does not however, have the solid backing from the EU budget that the other options have.</p> <p><u>Speed of decision-making</u>: in general Europol's decision-making processes are complex, though the</p>	**

	Director has large discretionary powers, which could support more rapid and effective decision-making.	
--	--	--

3.6. Ability to make the necessary investments (OPEX and CAPEX)

Beyond finding adequate resources for covering the annual costs of managing the systems, running the facility and dealing with incidents and specific requests, the system itself (the IT system comprising databases, applications and servers) requires regular updates and even replacement.

The Management Authority must therefore have access to funds that sometimes are largely superior to the annual running costs of the systems and the facility. The Management Authority should be able to plan ahead and define an IT strategy to allow the users and direct stakeholders to agree in time to the need and appropriateness of these investments in order for them to release the funds. As a prerequisite the Management Authority must be able to analyse and determine the investment levels required.

Options	Impacts: ability to make the necessary investments (OPEX and CAPEX)	Rating
Baseline	<p><u>Raising additional funds</u>: the Commission proposes the annual EU budget and should be well - positioned to get agreement on necessary expenditure and allocate the required means. Thus access to resources is likely to be strong under this option.</p> <p><u>Planning capability</u>: for planning and developing an IT strategy, the Commission is likely to depend largely on the operational management provided by two Member States and the IT supplier industry.</p>	**
Baseline+	Same as Option 1	**
Regulatory Agency	<p><u>Raising additional funds</u>: access to funding may be more difficult as the Regulatory Agency does not decide the overall level of its own budget, which remains the prerogative of the Commission followed by the European Parliament's approval. The annual budget provides a fixed frame, which is rigid and does not allow intermediate responses to increases in capital expenditure requirements.</p> <p><u>Planning capability</u>: depending on the task division, the Regulatory Agency can be an effective body to develop sound IT strategies given the combination of accumulated IT expertise, closeness to suppliers and the users of the systems.</p>	***

FRONTEX	<p><u>Raising additional funds</u>: FRONTEX also faces the rigidities of the annual budget cycle; and it does not determine its overall budget.</p> <p><u>Planning capability</u>: it could build effective planning capabilities through accumulating experience in running three large-scale IT systems. However the Management Board may be less focused and able to decide on matters concerning operational and technical IT requirements, than the Management Board of a dedicated Regulatory Agency. Thus strategic resource planning is expected to be weaker.</p>	**
Europol	<p><u>Raising additional funds</u>: Europol is funded by a variety of sources and does not (yet)⁶⁹ have the solid backing from the general budget of the EU that the other options have.</p> <p><u>Planning capability</u>: its small operational base may entail less learning experience; therefore capacity for strategic IT planning is expected to be lower than in options where more systems are combined. Furthermore the Management Board of Europol is not well attuned to deal with technical IT matters. Previous experience in developing and agreeing IT strategies has shown inconsistency and delays in decision- making⁷⁰.</p>	*

4. LEGAL

4.1. Effectiveness in ensuring fundamental rights and freedoms, in particular protection of personal data, respect for private and family life and right to an effective remedy

The SIS II and VIS legal instruments define the applicable data protection regimes. The European Data Protection Supervisor is responsible for checking that the Management Authority's personal data processing activities are in conformity with applicable rules⁷¹ In the case of both systems the national supervisory authorities and the European Data Protection Supervisor are obliged to cooperate⁷² For EURODAC, the European Data Protection Supervisor has the task of monitoring the activities of the central unit and the lawfulness of the transmission of personal data to the Member State by the central unit. All legal instruments foresee that records of data-processing operations are kept for the purpose of monitoring⁷³ All legal instruments

⁶⁹ The replacement of the Europol Convention will change this
⁷⁰ Difficulties to establish IT strategy for Europol in interview with Europol staff
⁷¹ Art. 42 VIS, Art. 45 SIS II Reg., Art. 61 SIS II Decision.
⁷² Art. 43 VIS, Art. 46 SIS II Reg., Art. 62 SIS II Decision.
⁷³ Art. 34 VIS, Art. 12 SIS II Regulation and Decision, Art. 16 EURODAC Regulation.

give any person the right to obtain information on the data relating to them, to request that inaccurate data is corrected and that unlawfully stored data is deleted.⁷⁴ If those rights are refused, the concerned person can bring, under all legal instruments, an action or a complaint before the competent authorities or courts.⁷⁵

While the SIS II Regulation prohibits that data is transferred or made available to third countries or to international organisations, the SIS II Decision allows, under conditions specified in the Decision, the exchange of data on passports with Interpol and allows access to certain categories of alerts to Europol and Eurojust. A prohibition on transferring data or on making them available exists in the VIS Regulation and the VIS Decision as a principle. An exception is foreseen, under cumulative conditions in the VIS Regulation solely for the purpose of proving the identity of third-country nationals, including for the purpose of return and in the VIS Decision for the purposes of the prevention and detection of terrorist offences and other serious criminal offences in an exceptional and urgent case. The EURODAC Regulation forbids transfer of data to the authorities of third countries. The transfer can, however, be allowed in the framework of a Community agreement on the criteria and mechanisms for determining the State responsible for examining an application for asylum.

The legal requirements on privacy and data protection as described in the legal instruments establishing the systems are binding for every potential option and therefore are not differentiating factors. Compliance with data protection requirements laid down in specific legal instrument for each system has to be ensured. More important than reviewing the actual rules is to assess the effectiveness of oversight, and factors influencing the internal data protection culture and awareness of the Management Authority. Another determining factor is the ability to withstand pressure from third parties to gain access to the data or to compromise the system. In addition it should be noted that the perception of the (risk of) abuse of personal data should also be avoided where possible, as this can undermine the trust of data subjects and public authorities in the Management Authority (which will be discussed in the section on mission creep). Furthermore, the political concerns around data protection particularly in the European Parliament make it an important issue.

Any situation where there are more systems with different rules is likely to create complications for effective data protection (although not impossible to organise). Further complications can be expected if the host organisation has its own existing data protection regime and supervision authorities, other than foreseen under the three systems.

Another factor that determines the effectiveness of data protection in practice is the European Data Protection Supervisor's ability to have unlimited and timely access to the systems and premises. Finally, to avoid the perception of mission creep and abuse of personal data, it is preferable that the Management Authority itself does not have right of access to the data, except in cases where it is exposed to the data in the cause of regular technical and operational activities.

⁷⁴ Art. 38(1) (2) VIS, Art. 41 SIS II Regulation, Art. 58 SIS II Decision, Art. 18(2)(3) EURODAC Regulation.

⁷⁵ Art. 40 VIS, Art. 43 SIS II Regulation, Art. 59 SIS II Decision, Art. 18(11)(12) EURODAC Regulation.

Options	Impacts: effectiveness in ensuring fundamental rights and freedoms, in particular protection of personal data, respect for private and family life and right to an effective remedy	Rating
Baseline	<p><u>Protection of fundamental rights and freedoms:</u> management by the Commission would ensure one common regime and supervisory structure; and the instalment of all the necessary data protection procedures. The Commission has a history of setting data protection standards and is sensitive to these issues. It is also under strong public scrutiny to protect fundamental rights of EU citizens and third country nationals residing in the EU.</p> <p><u>Access by supervisory bodies:</u> during the development of SIS II supervision by the EDPS has proven to be difficult due to access restrictions and different security regimes of the local facility and the Commission. Whilst this is in no way a given, practical and cultural barriers to effective supervision by EDPS may be more likely if the SIS II is managed by a Member State where national data protection rules and national supervisory authorities are prevalent.</p> <p><u>Resisting pressure to provide unlawful access:</u> it is expected that the Commission, given its size and political power will be best placed to resist outside pressure to provide access to the data or to compromise the system. Under the baseline option it will depend on the Commission's ability to effectively control the operations by the two Member States.</p>	**
Baseline+	<p><u>Protection of fundamental rights and freedoms:</u> same as Option 1, though the transfer of EURODAC would increase consistency and uniformity. Handling of EURODAC data would be exposed to some of the risks associated with management by a Member State at arms-length from the Commission.</p> <p><u>Resisting pressure to provide unlawful access:</u> same as Option 1</p>	**
Regulatory Agency	<p><u>Protection of fundamental rights and freedoms:</u> This option would ensure that fundamental rights and freedoms are guaranteed by ensuring the appropriate accountability vis-à-vis the European Parliament, the European Data Protection Supervisor, the Court of Auditors, the European Court of Justice and the Commission. Moreover, since the Agency would be designed and established from scratch, it could provide</p>	***

	<p>a tailored solution for the access of the supervisory bodies.</p> <p><u>Resisting pressure to provide unlawful access:</u> to resist outside pressure a dedicated Agency for technical and operational management may lack the political power and expertise. Furthermore, its limited scope and emphasis on technical skills is likely to reduce the Agency's capacity to correctly assess the larger (political) interests at stake.</p>	
FRONTEX	<p><u>Protection of fundamental rights and freedoms::</u></p> <p>This option would ensure that fundamental rights and freedoms are guaranteed by ensuring the appropriate accountability vis-à-vis the European Parliament, the European Data Protection Supervisor, the Court of Auditors, the European Court of Justice and the Commission. FRONTEX does not manage IT systems yet and thus has no experience with the data protection issues of handling large amounts of sensitive data. However, it is used to deal with sensitive classified information as such. It is already under the supervisory responsibility of the EDPS and therefore access of the EDPS to the facilities should not pose any problems.</p> <p><u>Resisting pressure to provide unlawful access:</u> FRONTEX is currently not used to this environment and not trained to deal with these interests and pressures and therefore there might be a risk of not ensuring compliance with data protection requirements applied to each system.</p>	***
Europol	<p><u>Protection of fundamental rights and freedoms:</u> Europol could have some problems in ensuring fundamental rights and freedoms, due to its limited appropriate accountability vis-à-vis the European Parliament, the European Data Protection Supervisor (EDPS), the European Court of Auditors, the European Court of Justice and the Commission because of its inter-governmental character.</p> <p>As the EDPS does not assume a supervisory competence over Europol (Europol has a functioning data protection regime and supervision is provided by the Joint Supervisory Body) the dual data protection supervision regime would be complicated. Assessment of the quality of the current regime and its implementation differs between observers (interviews with Members of the European Parliament, and representatives of the EDPS and Europol). If Europol</p>	*

	<p>managed SIS II there would be a number of regimes for the entire organisation.</p> <p>EDPS would only have access to the SIS II. The joint supervisory body would have to interact with EDPS, which could make supervision difficult in practice.</p> <p><u>Resisting pressure to provide unlawful access:</u> any organisation involved with law enforcement and police investigation might wish to have access to as much information as possible. As such Europol has a strong incentive to want to have full access to all available SIS II data, even though this is restricted by the SIS II legal acts. (see function creep section).</p>	
--	---	--

4.2. Effective liability and redress provisions

The provisions on liability (for damages caused to persons or to the system) are similar in all legal instruments. There are, however, significant differences in the current liability clauses in the potential hosting organisations (Commission, FRONTEX and Europol), which may affect the specific liability clauses in the legal instruments establishing the systems.

Liability provisions need to be clear: for the management to determine its legal risk; and for all third parties that may have reason to litigate to know their rights. Such liability provisions must allocate responsibility in case of damages under tort or breach of contract. It must be clear which judicial bodies have jurisdiction and under which law the liability proceedings will fall.

Options	Impacts: Suitable Effective liability and redress provisions	Rating
Baseline	<p><u>Jurisdiction of Community Courts:</u> management by the Commission would, in principle, imply jurisdiction of the European Court of Justice and the Court of First Instance, respectively. Thus, even the operations mandated to the Member States should be covered by the jurisdiction of the Courts. However, there might be a situation of jurisdictional conflict (see below).</p> <p><u>Guarantees for litigating parties:</u> the liability of the Commission provides the best guarantees to litigating parties trying to execute their rights. However, a cumbersome situation arises where operations of national staff are challenged. Although the Member States in question and their staff are entrusted with the management of the systems and although they act in execution of a Community task, the scope of the</p>	*

	Community's liability for acts of Member States is far from clear. Existing case law ⁷⁶ on the question of 'joint liability' suggest a conflict of jurisdiction which, from the claimant's perspective, may be confusing.	
Baseline+	<p><u>Jurisdiction of the Community Courts:</u> same as option 1, though the transfer of EURODAC implies that it comes under the control of a Member State organisation, which may, again, cause a situation of jurisdictional conflict.</p> <p><u>Guarantees for litigating parties:</u> same as Option 1</p>	*
Regulatory Agency	<p><u>Jurisdiction of the Community Courts:</u> full jurisdiction of the ECJ and the CFI over all of the Agency's activities.</p> <p><u>Guarantees for litigating parties:</u> an Agency is its own legal entity and can be held liable.</p>	***
FRONTEX	<p><u>Jurisdiction of the Community Courts:</u> in the case of FRONTEX, Article 19 of the Council Regulation (EC) No 2007/2004 confirms jurisdiction of the European Court of Justice: a) in case of non-contractual liability; and b) to give judgement pursuant to any arbitration clause of contracts concluded by the Agency.</p> <p><u>Guarantees for litigating parties:</u> similar to Agency</p>	***
Europol	<p><u>Jurisdiction of the Community Courts:</u> the liability provisions are more complex as Europol is a third pillar instrument with no central legal responsibility. Under the Europol Convention, each Member State is liable in accordance with national law. Only the Member State in which the activity giving rise to the damage occurred can be subject of an action. Consequently, the damaged party shall apply to the Court having jurisdiction under national law of the Member State involved. If the damage resulted from the failure of another Member State or Europol, they shall reimburse the amount to the Member State that has been the subject of an action.</p> <p><u>Guarantees for litigating parties:</u> the Management Board is responsible for resolving disputes over such repayments. Europol's contractual liability follows the law that governs the contract.</p>	*

⁷⁶

ECJ, C-5,7,13-24/66 – Kampfmeier v. Commission [1967] ECR 245

4.3. Weight of legal requirements to establish effective management

All the relevant legal instruments will require modification to accommodate the long-term management solution, though there are differences in the scope of the changes.

In the case of VIS and SIS II the long-term management solution - has deliberately been left open by referring to a 'Management Authority and depending on the solution - this term should be specified. Amendments would be required in the legal instruments governing the systems, as well as those governing the recipient organisations, where these are existing organisations.

As regards SIS II, all proposals for long-term management require a dual legal basis, including modifications to the existing SIS II legal instruments, if they are submitted before the Treaty review enters into force.

The involvement of non-EU Member States may add extra legal weight to the options where a negotiated change of the association agreements would be required between the EU and the country in question, as this is a separate legal process that needs to be concluded.

Options	Impacts: weight of legal requirements to establish effective management	Rating
Baseline	<p><u>Complexity of legal process (nature of intervention and delays):</u> the legal requirements are relatively limited in establishing the baseline option as the long-term solution.</p> <p>However, the SIS II and VIS legal acts need to be amended, where they state that the delegation to two Member States by the Commission is an interim solution and the 'Management Authority' would need to be specified.</p>	***
Baseline+	<p><u>Complexity of the legal process (nature of intervention and delays):</u> same as Option 1, but a review of the EURODAC Regulation would be required. This could cause limited extra legal requirements if this review could be integrated in the planned review of EURODAC.</p>	**
Regulatory Agency	<p><u>Complexity of the legal process (nature of intervention and delays):</u> a Regulatory Agency will need to be established from scratch, which is a relatively long political and legislative process estimated to last at least 30 months (taking FRONTEX as a benchmark). This requires new legal instruments setting up the Regulatory Agency and adjustments to the EURODAC, VIS and SIS II legal instruments.</p>	*

FRONTEX	<p><u>Complexity of the legal process (nature of intervention and delays):</u> Management by FRONTEX would entail the renegotiation of the FRONTEX Regulation. This would be complex as it would need to accommodate the third pillar elements of SIS II, but not impossible.</p> <p>The SIS II, VIS, EURODAC legal instruments would need to be changed to define FRONTEX as the Management Authority and to determine the specifics of the relationship between FRONTEX and the systems.</p>	*
Europol	<p><u>Complexity of the legal process (nature of intervention and delays):</u> the Europol Convention would need to be amended, to accommodate the SIS II management and particularly all first pillar guarantees and requirements; thus increasing the legislative effort needed.</p> <p>The VIS legal act would need to be amended, where it states that the delegation to two Member States by the Commission is an interim solution, as it would become permanent. In SIS II and VIS the ‘Management Authority’ would need to be specified.</p>	*

4.4. Avoiding function creep (de jure and de facto)

‘Function creep’ or ‘mission creep’ is the process in which a system that is designed to perform a certain function is used for other purposes. Function creep is not inherent to any of the options and as such is not a pertinent differentiating element. However, it may be more likely under certain options, where the management is carried out by users of the system who have access to (parts of) the data, or who have a role in policymaking.

The first category concerns situations where the legal basis of a system determines which data is or is not accessible to an organisation. If this organisation were to manage the system, in practice it would have full access to all data. To avoid the organisation abusing this position, appropriate technical, legal and organisational measures could be implemented. For the second category, there is the risk that a Management Authority, which has a policy responsibility, could be tempted to seek a broader or different use of the data under its control to support its policy ambitions. Although all these issues can be addressed through legal and technical means, the perception of likely function creep would be stronger in certain options.

Moreover, any Management Authority that is responsible for managing more than one system must guarantee the integrity of the data and ensure adequate controls and processes for data protection, in order to avoid data flow between the systems without an explicit legal basis for such an exchange. Physical, geographic and

organisational separation of the systems, databases and infrastructures usually provide very good (*de facto*) barriers to the exchange of data.

On the other hand, there may also be some benefits in joint management, as this would allow the establishment of one common and consistent data protection framework, with common rules and one supervisory authority. Such common rules facilitate employees' compliance, as well as supervision by the European Data Protection Supervisor.

Options	Impacts: avoiding function creep (de jure and de facto)	Rating
Baseline	Geographic separation between EURODAC on the one hand and VIS and SIS II on the other hand as well as technological separation between all the systems are de facto barriers to sharing information across systems. The current facilities still need to prove their ability and willingness to provide full and immediate access to EDPS, without being restrained by national security restrictions. There may be a risk of perception that policy interests and objectives of the Commission or the national authorities involved may trigger the management's interest to access and use data for which there is no legal basis.	**
Baseline+	The transfer of EURODAC would remove the geographic, technical, and organisational divisions between it and SIS II, VIS, thus increasing the (perceived) risk of function creep. The remainder is the same as Option 1.	**
Regulatory Agency	One single dedicated management solution should be able to ensure a strict and clear separation of technical and operational staff from policy makers and users of the data in the system. Setting up a new Agency would allow the establishment of all the necessary safeguards to avoid function creep. However, having one organisation running three or more systems may create the perception that the systems are interconnected and data is shared between them.	***
FRONTEX	As FRONTEX does not have access to the data and it does not have a policymaking responsibility the actual risk of function creep is less than in other options. There might be some, limited, interest in FRONTEX to having access to SIS II, VIS and EURODAC, given its operational tasks. Having one organisation	**

	running three or more systems may create the perception that the systems are interconnected and data is shared between them.	
Europol	<p>Europol has access to some categories of SIS II data. Any potential abuse by accessing other categories of data would have to be effectively addressed through technical and organisational measures ensuring the protection of data.</p> <p>As Europol is a police organisation it might be perceived as potentially unlawfully accessing data in the fight against crime.</p>	*

Annex 3
Risk Assessment

1. BASELINE

Table 14: Risk assessment Baseline

Identified Risk	Possibility of Occurrence	Cost/Damage
Financial risk:		
Renewal of the contract with national authorities which are in a <i>de facto</i> monopoly position	High	Pricing above market value
Governance Risk:		
The Commission is not directly implementing the daily management tasks but it is accountable for them. The Commission has to ask national authorities for the relevant information.	Initially high; less over time	Delays in solving issues; inter-institutional difficulties
Legal risk:		
The Baseline solution was explicitly mentioned as being transitional. Changing this to a permanent solution was never the intention of the legislator.	High	
Operational Risk:		
Single point of failure if many systems are run in one facility and the back-up unit is currently not staffed to take over 24/7 service in case of physical attack of the premises where the systems are housed. ⁷⁷	Low	Temporary discontinuity, until CU staff is transferred and the back-up site is operational.
Limited possibility for the Commission to ensure efficiently that the current contracting Member States will build fully new, custom made facilities to provide adequate housing for current and future systems (and BCUs) as well as operational management staff.	Medium	High operational expenditure and maintenance cost. Inadequate facilities, negatively affecting working environment and operational management output.
Different administrative cultures, interests and objectives in the Commission and Member State authorities. Reduced possibility for the Commission to enforce contractual obligations.	High	Delays; higher costs.

⁷⁷ Assumption based on the current situation

2. REGULATORY AGENCY

Table 15: Risk assessment Regulatory Agency

Financial risk:		
Cost and time of setting up the Agency and transition to new location.	High	Loss of key staff; training cost; delays in planning and deployment; discontinuity
High overheads: Insufficient critical mass of operational activity to justify setting up dedicated governance and management structures	High, will eventually decrease	Labour cost; redundancy at administrative level
Delays in setting annual budget and work programme, due to multi-level governance.	High	Delays; inconsistent decision-making.
Governance Risk:		
Complex and non-transparent structure of rules and procedure to accommodate the ' <i>géométrie variable</i> '	High	Delays; inconsistent decision making; reduced supervision
Insufficient influence of the Commission in the Management Board leading to implementation measures being dealt with through comitology, outside the Agency.	High	Loss of effectiveness and consistency
Commission loss of control over budget execution and planning	High	Misalignment with broader policy objectives
Legal risk:		
Technology and/or specific interests driving policy, leading to 'function creep'.	Medium	Litigation; infringements of data protection and civil rights
Level of delegation of executive powers by the Commission;	Medium, depending on extent of delegation	Delays
Upholding data protection rules: A relatively small organisation with little political leverage may find it difficult to withstand pressure from third parties (and also stakeholders) to provide unlawful access to data	Low, depending of Member States and Commission's active and effective engagement	Infringement of data protection rights; threat to the image of the EU as a whole
Operational Risk:		
Relocation: leading to loss of expert staff and continuity risks	High	Loss of key staff; training cost; delays in planning and

		deployment; discontinuity
Lengthy start up time; due to legislative procedures, discussion about location and governance structure; hiring of staff; establishing the organisation.	High	Delays; early write offs or high maintenance cost to keep old hardware running; staff turnover
Single point of failure if many systems are run in one facility. Effective security plan and 24/7 back up unit would avoid this risk.	Medium	Greater contingency of non-24/7 staff in same location

Annex 4
Joint statements of the long-term management of SIS II and VIS
STATEMENT 235/06

Joint statement by the Commission, the Council and the European Parliament on Article 15 relating to operational management of SIS II

"The European Parliament and the Council invite the Commission to present, following an impact assessment containing a substantive analysis of alternatives from the financial, operational and organisational perspective, the necessary legislative proposals entrusting an agency with the long-term operational management of the Central SIS II and parts of the Communication Infrastructure.

The Commission commits itself to presenting, within two years of the entry into force of this Regulation, the necessary legislative proposals to entrust an agency with the long-term operational management of the Central SIS II and parts of the Communication Infrastructure. These proposals shall include the modifications required to adapt the legal instruments on the establishment, operation and use of the second generation Schengen Information System (SIS II).

The European Parliament and the Council commit themselves to dealing with these proposals as quickly as possible and to have them adopted in time to allow the agency to take up fully its activities before the end of a five-year period following the entry into force of this Regulation."

Joint statement by the European Parliament, the Council and the Commission on Article 26 relating to operational management of VIS

"The European Parliament and the Council invite the Commission to present, following an impact assessment that provides a substantive analysis of alternatives from a financial, operational and organisational perspective, the necessary legislative proposals entrusting an agency with the long term operational management of the VIS. The impact assessment could form part of the impact assessment which the Commission undertook to carry out with regard to the SIS II.

The Commission commits itself to presenting, within two years of the entry into force of this Regulation, the necessary legislative proposals to entrust an agency with the long-term operational management of the VIS. Such proposals shall include the modifications required to adapt the Regulation concerning the VIS and the exchange of data between Member States on short stay visas.

The European Parliament and the Council commit themselves to dealing with these proposals as quickly as possible and to have them adopted in time to allow the agency to take up fully its activities before the end of a five-year period following the entry into force of this Regulation."

Annex 5
Description of the SIS, SIS II, VIS and EURODAC

1. SIS AND SIS II

The Schengen Information System (SIS) is an IT system that allows the competent authorities in the Member States to obtain information regarding certain categories of persons and objects. It is thus a vital factor in the smooth running of the area of freedom, security, and justice. It contributes strongly to the implementation of the provisions on the free movement of persons (Title IV of the EC Treaty) and to judicial cooperation in criminal matters and police cooperation (Title VI of the EU Treaty). The Schengen Convention⁷⁸ constitutes the legal basis for the first generation of SIS.

A second generation SIS (SIS II) is currently being developed in order to accommodate the new Member States⁷⁹ and to include new functionalities. The Council entrusted the Commission with the development of SIS II by adopting in parallel a Regulation⁸⁰ and Decision⁸¹ on 6 December 2001.

Council Regulation No. 871/2004⁸² and Council Decision No. 2005/211/JHA⁸³ introduced some new functions to SIS in the fight against terrorism.

Once the development phase of SIS II comes to an end, the operational phase starts. The following three legal instruments will govern SIS II during the operational phase of the project:

- (1) Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II);⁸⁴
- (2) Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II);⁸⁵
- (3) Regulation (EC) No. 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the second-generation

⁷⁸ OJ L239, 22.09.2000.

⁷⁹ The original SIS had already been upgraded to 'SIS 1+' to enable linking the Nordic countries to SIS. In the meantime, the successful deployment of the SISone4all initiative has fulfilled the need to integrate the Member States that joined the EU in 2004 into the SIS.

⁸⁰ Council Regulation (EC) No. 2424/2001 on the development of the second-generation Schengen information system (SIS II), OJ L 328 of 13.12.2001.

⁸¹ Council Decision 2001/866/JHA of on the development of the second-generation Schengen information system (SIS II), OJ L 328 of 13.12.2001

⁸² Council Regulation (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System including in the fight against terrorism, OJ L 162 of 30.04.2004

⁸³ Council Decision (EC) No 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System including in the fight against terrorism, OJ L 68 of 15/3.2005

⁸⁴ OJ L381 of 28.12.2006.

⁸⁵ OJ L 205 of 7.8.2007.

Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates⁸⁶

These legal instruments provide that purpose of SIS II shall be to ensure a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of Title IV of Part Three of the Treaty relating to the movement of persons in their territories, using information communicated via this system.

SIS II shall be composed of:

(a) a central system ("Central SIS II") composed of:

- a technical support function ("CS-SIS") containing a database, the "SIS II database";
- a uniform national interface ("NI-SIS");

(b) a national system (the "N.SIS II") in each of the Member States, consisting of the national data systems which communicate with Central SIS II. An N.SIS II may contain a data file (a "national copy"), containing a complete or partial copy of the SIS II database;

(c) a communication infrastructure between CS-SIS and NI-SIS (the "Communication Infrastructure") that provides an encrypted virtual network dedicated to SIS II data and the exchange of data between SIRENE Bureaux.

The operational Central Unit (CS-SIS) shall be located in Strasbourg (France), and the Business Continuity Unit (back-up site) in St Johann im Pongau, near Salzburg (Austria). Once SIS II goes live, the Commission may entrust France and Austria with the operational management tasks for a transitional period before the long-term management solution is established. According to recital 9 of the SIS II legal instruments, this "transitional period should last for no more than five years from the date from which this Regulation (and Decision) applies".

The following alerts shall be entered in SIS II:

- alerts in respect of third-country nationals for the purpose of refusing entry and stay,
- alerts in respect of persons wanted for arrest for surrender and extradition purposes,
- alerts on missing persons,
- alerts on persons sought to assist with a judicial procedure,
- alerts on persons and objects for discreet checks or specific checks,
- alerts on objects for seizure or use as evidence in criminal proceedings.

The SIS II legal instruments provide that access to data entered in SIS II and the right to search such data directly or in a copy of SIS II data shall be reserved exclusively to the authorities responsible for:

(a) border control, in accordance with Regulation (EC) No 562/2006 of the European Parliament and the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code);

(b) other police and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities.

⁸⁶ OJ L 381 of 28.12.2006.

However, the right to access data entered in SIS II and the right to search such data directly may also be exercised by national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge, in the performance of their tasks, as provided for in national legislation, and by their coordinating authorities.

In addition, the right to access data entered in SIS II and the data concerning documents relating to persons entered in accordance with Article 38(2)(d) and (e) of Decision 2007/533/JHA and the right to search such data directly may be exercised by the authorities responsible for issuing visas, the central authorities responsible for examining visa applications and the authorities responsible for issuing residence permits and for the administration of legislation relating to third-country nationals in the context of the application of the Community acquis relating to the movement of persons. Access to data by these authorities shall be governed by the law of each Member State.

Europol and the national members of Eurojust and their assistants shall, within their mandate, have the right to access and search certain categories of data entered in SIS II (see Art. 41 and 42 of Decision 2007/533/JHA).

2. VIS

The Visa Information System (VIS) is a system for the exchange of visa data between Member States. Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS)⁸⁷ provides the legal basis for the development of the system⁸⁸. The VIS Regulation⁸⁹ defines the purposes, the functionalities and the responsibilities for the VIS and sets up the conditions and procedures for the exchange of data between Member States on applications for short-stay visas and on the related decisions.

VIS shall have the purpose of improving the implementation of the common visa policy, consular cooperation and consultation between central visa authorities by facilitating the exchange of data between Member States on applications and on the decisions relating thereto, in order to:

- facilitate the visa application procedure;
- prevent visa shopping;
- facilitate the fight against fraud;
- facilitate checks at external border crossing points and within the territory of the Member States;
- assist in the identification of any person who may not, or may no longer fulfil the conditions for entry to, stay or residence on the territory of the Member States;

⁸⁷ Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213 of 15/06/2004

⁸⁸ OJ L 213 of 15.6.2004, p. 5.

⁸⁹ Regulation of the European Parliament and of the Council (EC) No 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

- facilitate the application of the Dublin Regulation⁹⁰;
- contribute to the prevention of threats to the internal security of any of the Member States.

The designated authorities of the Member States may in a specific case and following a reasoned written or electronic request access the data kept in the VIS referred to in Articles 9 to 14 of the VIS Regulation if there are reasonable grounds to consider that consultation of VIS data will substantially contribute to the prevention, detection or investigation of terrorist offences and of other serious criminal offences. Europol may access the VIS within the limits of its mandate and when necessary for the performance of its tasks.

Detailed rules on access for entering, amending, deleting and consulting VIS data as well as on access to biometrics for verification at external border crossing points, for verification within the territory of the Member States, for identification, for determining the responsibility for asylum applications and for examining an asylum application are set out in the VIS Regulation.

The VIS shall be connected to the national systems of the Member States to enable the competent authorities of the Member States to process data on visa applications and on visas issued, refused, annulled, revoked or extended.

The VIS Regulation provides that during a transitional period the Commission shall be responsible for the operational management and thereafter a Management Authority. During this transitional period, which should last for no more than five years from the date of entry into force of the VIS Regulation, the Commission may delegate that task to national public-sector bodies in two different Member States. The Central VIS shall be located in Strasbourg (France) and its back-up system in St Johann im Pongau (Austria).

3. EURODAC

EURODAC is a database that stores and compares the fingerprints of asylum applicants and illegal immigrants apprehended in connection with the irregular crossing of an external border. It was established to allow Member States to determine the State responsible for examining an asylum application according to the Dublin Regulation.

A Council Regulation establishing the system was adopted in 2000,⁹¹ and in 2002 the Council adopted implementing rules thereto.⁹² The system became operational in January 2003. The Commission has proposed to amend the EURODAC Regulation in order to contribute to the building of the second phase of the Common European Asylum System.⁹³

⁹⁰ Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national OJ L 050 , 25/02/2003 P. 0001 – 0010.

⁹¹ Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the establishment of “EURODAC” for the comparison of fingerprints for the effective application of the Dublin Convention (EURODAC Regulation), OJ L316 of 15.12.2000.

⁹² Council Regulation (EC) No. 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No. 2725/2000 concerning the establishment of “EURODAC” for the comparison of fingerprints for the effective application of the Dublin Convention.

⁹³ COM(2008) [...].

The Eurodac Regulation provides for the establishment of a Central Unit managed by the European Commission containing an Automated Fingerprint Identification System (AFIS) which shall receive data and transmit “hit – no hit” replies to the national authorities (to the National Access Point servers) in each Member State.

The central unit's activities are monitored by the EDPS. National authorities are responsible for the overall quality of the data transferred to, recorded or erased from the Central Unit and for the security of the transmission of data between their national authorities and the Central Unit. The EURODAC technical platform is likely to be reviewed in the coming years and is expected to be upgraded.⁹⁴

Data on the following categories of persons are to be found in EURODAC:

Category 1: data on asylum applicants. Fingerprints are stored for 10 years, and are compared against category 1 and category 2. Data should be erased in advance of the 10 years when an individual obtains the nationality of one of the Member States.

Category 2: data on aliens apprehended irregularly crossing an external border. They are kept for storage only (2 years). Category 1 data which are sent later will be compared against these.

Data should be erased in advance of the 2 years if the individual receives a residence permit, leaves the territory of a Member State or obtains the nationality of one of the Member States.

Category 3: data on aliens found to be illegally present in a MS. These data are not stored, only searched against category 1. The transmission of this category is not mandatory for Member States.

The following data is collected for any asylum applicants over 14 years of age:

- fingerprints
- sex of the data subject;
- Member State of origin, place and date of the application for asylum;
- reference number used by the Member State of origin;
- date on which the fingerprints were taken, date on which the data were transmitted to the Central Unit
- operator user ID of the person who transmitted the data.

⁹⁴ 2008 Budget Submission to the European Parliament: Title 18, Area of Freedom, Security and Justice, p. 10.

Annex 6
Administrative costs

Preferred option: New Regulatory Agency (Proposals for establishing an Agency for the operational management of the SIS II, VIS and EURODAC and for the development and the management of other large-scale IT systems in application of Title IV of the EC Treaty)						Tariff (€ per hour)		Time (hour)		Price (per action or equip)	Freq (per year)	Nbr of entities	Total of actions	nbr	Total cost	Regulatory origin (%)			
No.	Ass. Art.	Orig. Art.	Type of obligation	Description of required action(s)	Target group	i	e	i	e							Int	EU	Nat	Reg
1			Submission of (recurring) reports	Retrieving relevant information from existing data	Member States	25		45,00		1.125,0	1,00	27		27	30.375		100%		
2			Submission of (recurring) reports	Filling forms and tables	Member States	25		15,00		375,0	1,00	27		27	10.125		100%		
3			Submission of (recurring) reports	Submitting the information (sending it to the designated recipient)	Member States					10,0	1,00	27		27	270		100%		

4			Submission of (recurring) reports	Retrieving relevant information from existing data	Participating third countries (NO,IS,CH,L I)	37		45,00		1.665,0	1,00	5	5	8.325	100%		
5			Submission of (recurring) reports	Filling forms and tables	Participating third countries (NO,IS,CH,L I)	37		15,00		555,0	1,00	5	5	2.775	100%		
6			Submission of (recurring) reports	Submitting the information (sending it to the designated recipient)	Participating third countries (NO,IS,CH, LI)					10,0	1,00	5	5	50	100%		

7			Submission of (recurring) reports	Retrieving relevant information from existing data	EU staff in the Agency	74		90,00		6.660,0	1,00	1	1	6.660	100%		
8			Submission of (recurring) reports	Filling forms and tables	EU staff in the Agency	74		30,00		2.220,0	1,00	1	1	2.220	100%		
9			Submission of (recurring) reports	Submitting the information (sending it to the designated recipient)	EU staff in the Agency	74				10,0	1,00	1	1	10	100%		

10		Cooperation with audits	Inspecting and checking (including assistance to inspection by public authorities)	EU staff in the Agency	74	24,00	1.776,0	1,00	1	1	1.776	100%		
----	--	-------------------------	--	------------------------	----	-------	---------	------	---	---	-------	------	--	--

Total administrative costs (€) **62.586**

The likely administrative burdens for Member States and for the participating third countries (NO, IS, CH, LI) are only assessed for the preferred option, because the burdens are neutral across all options.

Regardless of whether an Agency (options 3,4,5) or the Commission and Member States (options 1,2) are entrusted with the long-term management of the systems,

administrative burdens would be incurred both at the management level as well as at the level of individual Member States or participating third countries.

The systems will need to be run at national level and information on this will need to be provided, regardless of the option chosen for carrying out the central management function.

The long-term management option, as such, does not entail administrative burdens on citizens or enterprises.

The assumption is that there are 220 working days in a year and 8 working hours in a day.

Average employment costs in the EU-27 public administration: Eurostat: Average hourly labour costs, defined as total labour costs divided by the corresponding number of hours worked (€20,35 in 2005).

The 2005 figure has been rounded upwards, based on the assumption of economic growth and pattern over the preceding years and overheads of 10% have been added.

http://epp.eurostat.ec.europa.eu/portal/page?_pageid=1996,39140985&_dad=portal&_schema=PORTAL&screen=detailref&language=en&product=Yearlies_new_population&root=Yearlies_new_population/C/C4/C43/dbb1

Average employment costs in the European Commission in 2007, DG BUDG, note 24/11/2006, Adonis No 11216

Average employment costs in the third/associated countries public administration: Eurostat: Average hourly labour costs, defined as total labour costs divided by the corresponding number of hours worked (€32 in 2005).

The 2005 figure has been rounded upwards, based on the assumption of economic growth and pattern over the preceding years and overheads of 10% have been added.

http://epp.eurostat.ec.europa.eu/portal/page?_pageid=1996,39140985&_dad=portal&_schema=PORTAL&screen=detailref&language=en&product=Yearlies_new_population&root=Yearlies_new_population/C/C4/C43/dbb1

