

European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

Work Programme 2013

1. EXECUTIVE SUMMARY.....	4
1.1. Strategic Goals.....	4
1.2. Key operational objectives.....	5
1.2.1. Operational Management of the Systems	5
1.2.2. Integration of new systems users	6
1.2.3. Security and the communication infrastructure	6
1.2.4. Monitoring, reporting and Statistics.....	6
1.2.5. Training.....	7
1.2.6. Cooperation with other Agencies.....	7
1.2.7. Monitoring of research and technology watch.....	7
1.2.8. Communications	7
1.2.9. Financial management, infrastructures, logistics and administration	7
1.2.10. Support to the Management Board and to the Advisory groups.....	8
1.2.11. Outlook for the implementation of these objectives in light of key risks	8
2. GENERAL PART	9
2.1. Introduction	9
2.2. Mission and values of the Agency.....	9
2.3. Vision	10
2.4. Policy context and strategic outlook.....	10
2.5. Strategic goals reflecting the Agency's medium-term vision	12
2.5.1. Strategic Goal 1: Consolidate the Agency's structure and cohesion	13
2.5.2. Strategic Goal 2: Move towards becoming a centre of excellence	15
2.5.3. Strategic Goal 3: Preparations for taking on board additional systems.....	16
2.5.4. Strategic Goal 4: Continuous move to optimise cost-effectiveness	16
2.6. Key operational objectives.....	17
2.6.1. Operational Management of IT Systems and preparations for future IT systems.....	17
2.6.2. Security and the communication infrastructure	22
2.6.3. Monitoring, reporting and statistics	24
2.6.4. Cooperation with other Agencies, projects and actions in the field of freedom, security and justice	24
2.6.5. Training for national authorities on the technical use of the IT systems.....	27
2.6.6. Monitoring of research and technology watch.....	28
2.6.7. Communication.....	29
2.6.8. Financial management, infrastructures, logistics and administrative tasks.....	29
2.6.9. Management Board and Advisory Groups.....	30
2.7. Specific operational objectives and performance indicators	32
2.7.1. Objectives to be steered at Agency level (with direct input from the Executive Director).....	32
2.7.2. Application Management and Maintenance.....	33
2.7.3. General Coordination.....	35
2.7.4. Internal Audit.....	39
2.7.5. Operational matters and Infrastructure	39

2.7.6.	Resources and Administrative Matters	41
2.7.7.	Procurement and Contracts	44
2.7.8.	Security	48

Budget forecast – Draft Budget 2013.....	50
---	-----------

3. SOURCE: DRAFT STATEMENT OF ESTIMATES OF THE REVENUE AND EXPENDITURE IN 2013 OF THE EUROPEAN AGENCY FOR THE OPERATIONAL MANAGEMENT OF LARGE-SCALE IT SYSTEMS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE.....	50
---	-----------

Executive Summary

The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice was established by virtue of Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 (OJ L 286, 01.11.2011, p.1) which entered into force on 21 November 2011. The Regulation provides that the Agency will take up its main responsibilities from 1 December 2012.

The purpose of this Annual Work Programme is to describe the activities to be carried out by the Agency in 2013, translating the strategic goals of the Agency into annual objectives and providing a basis for budgetary planning.

The core task of the Agency will be to ensure the operational management of VIS and EURODAC and to complete the preparations for taking over operations of SIS II. Furthermore, the go-live of SIS II scheduled for March 2013 will be a crucial milestone. The Agency will need to ensure that it is fully prepared to assume the challenging task of managing this critical system from that time onwards.

In the medium-term, the Agency will also develop new large-scale information systems in this policy area, if so provided by relevant legislative instruments.

A number of economic, political and technological developments will have an important impact on the medium-to-long term strategy of the Agency and the way that this is translated into operational goals for 2013. The economic crisis has significantly impacted national budgets and has led to calls for greater accountability and efficiency in all EU policy areas. The Agency will therefore have to clearly demonstrate the benefits of its investments and expenditure and prove that it can systematically deliver value for money. A further factor is the political instability in certain North African countries and the middle-east. The mass influxes of persons from these countries to the EU, in conjunction with new trends in migratory fluxes towards the EU, have highlighted the importance of having effective IT systems in place to manage the external borders and enhance cooperation of relevant authorities. Furthermore, they have also highlighted the political visibility of these systems.

The Agency will also be faced with challenges due to the complexity of the IT systems in this policy area, stemming from the number of stakeholders and the ambitious objectives and requirements of stakeholders.

Strategic Goals

In light of the above, the four strategic goals of the Agency are as follows:

1. Consolidate the Agency's structure and cohesion

To implement the necessary measures to ensure good governance and to strengthen cooperation and team building across the Agency, in order to deliver a seamless service on goals overarching the different units and sites of the Agency.

2. Move towards becoming a centre of excellence

To nurture and enhance the expertise and best practices within the organisation and put in place effective governance, structure, resources, information tools, procedures and methodologies to enable the Agency to move forward towards becoming a centre of

excellence for the management and development of large scale IT systems in the field of freedom, justice and security. A key part of this process will be to ensure alignment of business and ICT goals, by implementing Enterprise Governance of ICT.

3. Preparations for taking on board additional systems

Subject to the adoption of the legal bases for the Registered Traveller Programme and Entry Exit System, it is possible that the Agency may be asked to start developing these systems as from 2015. The Agency should already start planning ahead, strategically, anticipating its specific infrastructure, staffing and organisational requirements, taking account of the financial information in the legislative proposals for these systems.

4. Continuous move to optimise cost-effectiveness

To move towards the proactive search for more cost effective ways of delivering the requisite level of service or technical excellence for the Agency's own internal operations and for the IT systems under its management. This includes examining the scope for achieving cost savings for stakeholders.

Key operational objectives

The basic building blocks, infrastructures and functions of this Agency were put into place in 2012, allowing it to implement its core operational management tasks for the two systems already under its management. From early 2013 onwards, the Agency will start moving into a more pro-active phase.

One of the first steps to take in this direction will be to put in place adequate governance for ensuring alignment of the Agency's business and ICT goals and the creation of value from IT-enabled business developments by implementing recognised standards and business models in this field, namely the Enterprise Governance of ICT model, essential maturity levels of the COBIT framework for IT governance and best practices for IT service management from ITIL. The Agency will also work towards putting in place total quality management, with a view to full implementation of ISO 9001 in the medium term.

Following the recruitment of the first 75 staff members in 2012, as envisaged in the 2012 Agency Establishment Plan and budget, 45 additional staff members will be recruited in 2013.

The key operational objectives of the Agency in 2013 are as follows:

Operational Management of the Systems

The Agency will perform all necessary tasks for operational management of VIS and EURODAC, ensuring continuity of operations 24 hours a day, 7 days per week and make the final preparations for taking over operational management of SIS II. As from March 2013 it will also perform all necessary tasks for operating this system.

With regard to work carried out by contractors in relation to these systems, the Agency will initially only deal with operational supervision. It will take over financial and contractual responsibility as from the time that it is granted financial independence.

- One specific priority for SIS II in 2013 will be to meticulously prepare for taking over operation of this system, in order to ensure that the requisite service level indicators are fully met from the onset.

- The Commission will complete the procedures for concluding the SIS II maintenance contract on behalf of the Agency. The Agency will prepare for taking over operational aspects of this contract (supervision of the preparations for maintenance of the system and of the actual maintenance work as from March 2013).
- Specific objectives for VIS in 2013 will include ensuring that the technical characteristics of VIS will be able to support world-wide roll out. The Agency will also be responsible for supervision and monitoring of work under the contract for maintaining the VIS in working order and will subsequently take over responsibility for work under this contract to upgrade the VIS. Finally, the Agency will also ensure successful testing of VISMAIL 2 by the end of the year.
- With regard to EURODAC, one key priority for the Agency in 2013 will be to ensure the removal of this system from Luxembourg to Strasbourg and Sankt Johann im Pongau at the beginning of the year. This will include operational supervision of the contractors' work in the framework of procurement contracts related to this removal, for example, with respect to any additional IT equipment that may be required. The second main priority will be to start implementing the changes to the system foreseen in the Recast Regulation, subject to the adoption of this instrument.

Integration of new systems users

One priority will be to assist Croatia with its technical preparations for accession to the IT systems managed by the Agency which are now intensifying in light of its preparations for accession to the EU in mid 2013. Other activities in this area will include assistance to Cyprus with its preparations for achieving technical readiness in 2013 for integrating into SIS II and VIS. The actual integration of Cyprus into these systems may only go ahead once the necessary conditions for the application of all parts of the Schengen acquis will be met, as provided for in the Act of Accession of 2003. A number of other Member States will also require assistance with technical matters related to their future integration into SIS II. This applies in particular to the UK and Ireland which will probably integrate into this system from 2014 onwards.

Security and the communication infrastructure

The Agency will put in place and implement security measures and business continuity measures for its own organisation, for the systems that it will manage and for the communications networks for these systems, and carry out any other security tasks foreseen in the establishing Regulation and legal instruments for the IT systems.

Concerning the communication infrastructure for the IT systems under the Agency's management, initially, the Agency will be responsible for supervision, security and coordination of relations between the Member States and the network provider for the communication infrastructure for EURODAC and VIS. This will also be the case for the communication infrastructure for SIS II after the entry into operations of this system in March 2013. The Agency will also ensure that external private-sector network providers will fully respect the security measures and shall have no access to operational data in the IT systems.

Monitoring, reporting and Statistics

The Agency will produce the reporting and statistics on the use of the IT systems under its management and monitor their functioning, as foreseen in the legal bases for these IT systems and reflected in the establishing Regulation. It will report regularly to the European Parliament, the Council and the Commission on the technical functioning of the systems, including the security thereof and will also provide the Commission with information that it requires for the regular evaluation of VIS, EURODAC and SIS II.

Training

The Agency will provide training on the technical use of SIS II, VIS and EURODAC to the National authorities participating in these systems. It will also provide training for SIRENE-staff (SIRENE- Supplementary Information Request at the National Entries) and training for Schengen evaluation team members and lead experts on the technical aspects of SIS II. Further information on the organisation of training on these systems and the steps to be taken to ensure cooperation between the various EU Agencies involved (CEPOL for training of law enforcement authorities on SIS II and SIRENE and CEPOL and FRONTEX for training of Schengen evaluators) is given in point 2.6.5 below.

Cooperation with other Agencies

Cooperation with other Agencies such as CEPOL, EASO, ENISA, EUROJUST, EUROPOL, FRONTEX and FRA will continue in 2013. An action plan will be prepared setting out clear goals and objectives for cooperation with each of these Agencies. Complementarity will be a key priority in many of these relationships. The Agency will also take account of European and international standards, in particular the EU Information Management Strategy and will follow up developments with the European Information Exchange Model.

Monitoring of research and technology watch

The Agency will commence activities for monitoring of research and technology watch in 2013, feeding the results of this into decision-making on technical matters and business objectives. As mentioned above, the putting in place of an appropriate governance framework will ensure that the results of this work are oriented towards meeting the business objectives of the Agency.

Communications

The Agency will organise communications activities on its own initiative in the fields within its tasks, including the establishment of a web site. It will also be involved in the organisation of the SIS II Information campaign in 2013. The Commission also envisages to involve SIRENE experts in the preparation of the SIS II campaign via the SIS VIS Committee SIRENE Formation.

Financial management, infrastructures, logistics and administration

The Agency will consolidate its financial teams and procedures, with a view to obtaining financial independence during the year and taking a more pro-active approach for ensuring value for money across the full spectrum of its activities.

During the initial phase of Agency's operations, before it is granted financial independence, a number of contracts, including the MWO contracts for SIS II and VIS referred to in points 2.6.1.1 and 2.6.1.2 will be concluded by the Commission in the name of the Agency. Once the Agency has been granted financial independence), it will assume responsibility for financial matters related to these contracts.

The Agency will work on the basis of a procurement plan which will be communicated to the Management Board. The Management Board will also be informed of key calls for tenders. Member State experts may be invited on a case-by-case basis to provide technical expertise for the definition of tender documents and procedures.

Key priorities in the area of building management and logistics will be to ensure that work on the permanent premises in Tallinn and works to further upgrade the technical site in Strasbourg in order to meet future requirements remain fully on track.

Further information on the specific operational objectives of this Agency and related indicators, including objectives fixed for essential administrative tasks not referred to above are given in point 2.7 of this work programme.

Support to the Management Board and to the Advisory groups

The Agency's administrative structure will provide continuous support to the Management Board and to the work of the Advisory groups.

- The Management Board will continue to ensure that the Agency performs on the tasks laid down for it under the establishing Regulation in the most cost effective way, taking account of medium-term strategic goals. In addition to the approval of standard documents in the annual budgetary and planning lifecycle, specific matters to be decided on by the Management Board in 2013 will include matters related to the preparations for the permanent premises in Tallinn and the implementation of works on the technical site in Strasbourg. It will also have to endorse decisions related to the removal of EUODAC (see also point 1.2.9 concerning measures to inform the Management board on matters related to procurement).
- The priorities for the Advisory Groups in 2013 will include ensuring the ability of VIS to meet the technical requirements of future world-wide roll-out, follow-up of the entry into operations of SIS II, the growth in use of this system, technical matters relating to the relocation of EUODAC from Luxembourg to Strasbourg and Sankt Johann im Pongau and the adaptation of EUODAC to take account of the future Recast Regulation. A further priority for all of the groups will be the technical preparations for the accession of new Member States, in particular Croatia to these IT systems, the integration of countries such as the UK and Ireland into SIS II and preparations for ensuring technical readiness of Cyprus to join SIS II and VIS.

Outlook for the implementation of these objectives in light of key risks

The objectives fixed for this Agency are challenging and expectations from stakeholders are very ambitious. In the course of 2013, the Agency is expected to rapidly move ahead from its basic mission of operating the IT systems, towards becoming a centre of excellence dealing with highly specialised systems in a complex technical and stakeholder environment. As is the case in any complex business environment, there are risks associated with the Agency's operations. A number of critical risks have been identified in the area of financial resources, availability of premises and the transition towards financial independence. Action plans are in place for addressing all of these risks. The Agency will closely monitor the implementation of these action plans and any future developments in risk exposure. Top priority will be put on consolidating the teams and putting in place governance procedures necessary to enable the Agency to carry out all of its functions whilst effectively managing the risks associated with its operations. In light of the above, the Agency's management is confident that it will meet the expectations of stakeholders in delivering on its goals and objectives.

General Part

Introduction

The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice was established by virtue of Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 (OJ L 286, 01.11.2011, p.1) which entered into force on 21 November 2011. The Regulation provides that the Agency will take up its main responsibilities from 1 December 2012.

The Annual Work Programme of the Agency for the following year is to be adopted by the Management Board by 30 September each year, according to the specific terms of Article 12 of the establishing Regulation, after receiving the opinion of the Commission. The adopted work programme will then be transmitted to the European Parliament, the Council and the Commission by the Management Board and published. In accordance with the establishing Regulation, the annual work programme shall be produced in all official languages of the institutions of the Union.

The objective of the Annual Work Programme is to describe and to agree on the activities to be carried out by the Agency in the year in question, in order to implement the tasks referred to in Chapter II of the above-mentioned Regulation. Its purpose is to translate the strategic goals of the Agency into annual objectives and provide a basis for budgetary planning.

This Work Programme and the implementation thereof is therefore closely linked to the preparation and implementation of the Agency's Draft Budget for 2013, justifying the allocation of means to specific titles, chapters and articles.

As mentioned above, this new Agency was established at the end of 2011. The basic building blocks, infrastructures and functions of this Agency were put in place in 2012, allowing it to deliver on its core tasks for the operational management of VIS and EURODAC and for preparing to take over the operation of SIS II as from March 2013.

The present Work Programme describes the tasks of the Agency in 2013, with a view to:

- Continuous delivery of the core services for managing and operating the IT systems under its responsibility
- Completion of the final steps in building and consolidating the organisation
- Moving forward into a more pro-active phase, taking account of the strategic context and goals described in 2.5 below.

Mission and values of the Agency

The Agency's core mission is to ensure the continuous, uninterrupted operation of European large scale IT systems in the area of freedom, security and justice.

In the medium term, it will also develop new large-scale information systems in this policy area, if so provided by relevant legislative instruments.

The systems managed by, the Agency will make an important contribution to the maintenance of security and free movement between internal Schengen borders and towards the Schengen Area.

All activities of the Agency are steered by technological and economic intelligence.

The Agency ensures that its activities are carried out ensuring sound financial management.

The Agency is a trustworthy operational management body, fully respected by Member States and other stakeholders in the systems under its management.

The Agency's personnel and their high level of expertise and professionalism are a cornerstone of its effectiveness and trustworthiness. The Agency will maintain policies within its organization to ensure that it is a competitive employer and that the skills of its personnel are fully valorized.

In all of its activities, the Agency ensures full compliance with legal requirements, including, in particular, the security and data protection provisions applicable to the systems under its management.

Vision

A centre of excellence for the development and operational management of large scale IT systems in the area of freedom, security and justice, delivering cost effective services of the highest level, guaranteeing continuity of operations and providing a strategic vision of the technologies, solutions and applications needed to meet stakeholders' future expectations.

Policy context and strategic outlook

The establishment of this Agency was already foreseen in the legislative instruments for the Second Generation Schengen Information System (SIS II) adopted in 2006-2007 and the VIS Regulation adopted in 2008. In Joint Statements of the three institutions on the long-term management of these systems, the European Parliament and the Council invited the Commission to rapidly present the necessary proposals and committed themselves to having them adopted in time to allow the Agency to take up fully its activities by 2012. These political commitments have been respected.

The creation of the Agency is situated in the political context of the Stockholm programme and the action plan implementing this programme, which set the framework for the EU's response to major challenges in this policy area and outline a number of key developments in border management and security over the forthcoming period.

Furthermore, the Internal Security Strategy (ISS) adopted in February 2010 identifies "Strengthening security through border management" as one of 5 strategic objectives where the EU could bring real added value over the next four years.

A number of economic, political and technological developments will have an important impact on the medium-to long term strategy of the Agency and the way that this is translated into operational goals for 2013.

The ongoing economic crisis has already led to significant budget cuts at Member State level and has called for greater accountability and efficiency across all policy areas. This situation is most likely to continue well into the medium-term, with serious constraints and increased scrutiny on new investments in information technologies, at both European Union and Member State level. A key challenge will therefore be to demonstrate to stakeholders and society at large the benefits of investments and expenditure made by the Agency, to produce clear evidence of its added-value, cost-effectiveness, sound financial management and the potential for it to achieve cost savings for Member States by applying new technologies and introducing more efficient processes for the systems under its management. This will translate, for example, into a move towards starting small and expanding incrementally insofar as investments in and development of new systems are concerned.

A number of political and societal phenomena will also continue to impact on the environment of the IT systems managed by the Agency. Political developments in neighbouring third countries over the last year, in particular the instability in certain North African countries and the Middle East, led to mass influxes of persons at the southern borders of the EU and, more generally, new trends and challenges in the migratory flows towards the Union. These developments have significantly increased the visibility of external border management questions, highlighting the importance of having effective systems for controlling the borders, maintaining security, effectively managing asylum applications and implementing visa-issuing processes.

The systems managed by the Agency will therefore be clearly visible and under close scrutiny.

The Agency will assist Croatia with its technical preparations for joining the IT systems managed by the Agency which are now intensifying in light of its preparations for accession to the EU in mid 2013. The Agency will also assist Cyprus with its preparations for achieving technical readiness in 2013 for integrating into SIS II and VIS. The actual integration of Cyprus into these systems may only go ahead once the necessary conditions for the application of all parts of the Schengen acquis will be met, as provided for in the Act of Accession of 2003.. A number of other Member States will also require assistance with technical matters related to their future integration into SIS II. This applies in particular to the UK and Ireland which will probably integrate into this system from 2014 onwards.

The complex framework of the IT systems managed by the Agency, both in terms of the number of stakeholders and the variable geometry¹ whereby certain Member States will not be able to vote in the Management Board of the Agency as regards certain systems, also require effective governance structures to be put in place. The Agency must rapidly consolidate its organisation and teams and demonstrate its ability to deliver on the needs of stakeholders, whilst taking full account of EU interests and priorities. As already mentioned above, there will be high expectations for the Agency in terms of value-added.

The scale and complexity of IT systems in this policy area also pose huge technical challenges. Furthermore, their stakeholders expect state of the art solutions in terms of functionalities, response time and continuity of operations. The pace of technological change in the IT sector is both a challenge and an opportunity. The Agency will embrace this pro-actively by putting in place adequate governance procedures, structures and processes to enable it to effectively apply innovative technologies to support business and user needs and increase the efficiency of its own administrative procedures. A few examples of areas to examine would be biometrics and technological advances that will increase the performance, reliability and flexibility of systems.

As described in further detail in point 2.6.1.4 below, the Agency is also likely to be entrusted with the development and management of new IT systems, in particular, the Registered Traveller Programme and an Entry Exit system, for which legislative proposals are due to be presented in 2012. Other systems beyond the area of border management, such as tools for

¹ The legal frameworks of SIS II, VIS and EURODAC are characterized by variable geometry, a term used to denote the fact that certain Member States either do not participate at all in one or several of the systems, or only participate partially. For example, Ireland and the United Kingdom participate in EURODAC but are only involved in SIS II for ex third pillar aspects, not for free movement aspects. These two Member States do not participate in VIS. Denmark on the other hand is involved in SIS II and VIS ex first pillar instruments under international law and in Eurodac under an international agreement. A number of non-EU countries, namely Iceland, Norway, Switzerland and Liechtenstein are associated with the implementation, application and development of the Schengen acquis and therefore participate both in SIS II and VIS. They are also associated with the implementation of Eurodac related measures and participate in Eurodac.

data exchange for combating cross-border crime could also eventually be taken up by the Agency in the medium-term.

In looking forward to the future, it is also important to bear in mind the legacy of the past. There is often a negative image of IT projects managed by the public sector at both national and international level, due to a number of highly visible cases of delays and cost over-runs that have occurred in the recent past. The Agency must build on the experiences and lessons learned in other major IT projects and ensure tight governance, rigorous planning, and close monitoring of implementation of the projects under its responsibility in conjunction with efficient procurement procedures.

One challenge often encountered in such projects is to achieve the right balance between flexibility and budgetary and time constraints. In a policy area such as freedom, justice and security, stakeholders in large IT systems expect a high degree of flexibility on the requirements and technical solutions chosen for ongoing projects, in order to take account of both constantly evolving policy demands as well as latest technological developments, security standards and increasing safeguards for data protection. This is particularly the case when highly visible events occur, such as terrorist attacks or mass migration influxes, which often result in the rapid introduction of new policy measures to combat such phenomena (inter alia by facilitating cooperation and information exchange among responsible authorities). A key challenge for the Agency will be to demonstrate the requisite level of flexibility for developing and adapting the systems under its responsibility, whilst remaining cost effective and minimizing the impact on timing.

Stakeholders already have a number of clearly identified expectations for future enhancements to the IT systems that are managed by the Agency. One key task of the Agency in 2013 will be to ensure timely implementation of a significant capacity increase to the Visa Information System.

Data protection and data security will also be at the core of the Agency's priorities. The Agency will be required to ensure strict respect of all the data protection and security provisions applicable to the IT systems that it manages and will also be subject to regular audits in these specific areas.

By the start of 2013 the Agency is expected to have mastered the basic functions related to the operational management of VIS and EURODAC, ensuring that they operate continuously 24/7. As from the start of 2013, it will complete the final preparations for taking over operational management of SIS II and move forward towards becoming a fully fledged centre of excellence.

Strategic goals reflecting the Agency's medium-term vision

The main strategic goals for the Agency for 2013 and beyond described below reflect the policy context and outlook described in the previous chapter.

Strategic Goal 1: Consolidate the Agency's structure and cohesion

To implement the necessary measures to ensure good governance and to strengthen cooperation and team building, in order to deliver a seamless service on goals overarching the different units and sites of the Agency.
--

The main tasks in this area will be the recruitment of additional human resources, the consolidation of internal procedures, with a view to achieving an efficient and well-functioning administrative structure and team building activities. Work under Strategic Goal 2 to ensure

alignment of business and technological goals will also make an important contribution to the achievement of this goal.

As envisaged in the 2013 Agency Establishment Plan and budget, 45 staff members are due to be recruited in 2013, in addition to the 75 staff members to be recruited by the end of 2012.

These staff members will be recruited from the following recruitment paths:

1. Reserve list constituted in response to the *Open Call for expression of interest for Management, Security, IT-specialists and IT Support and Assistance* published on 23 November 2011,
2. Pool of applications received in response to a notice sent to laureates under existing EPSO reserve lists
3. Reserve list constituted in response to the *Open Call for expression of interest technical personnel with experience in the management of central units of Schengen and Dublin related IT systems (SIS 1, VIS and EURODAC)* published on 30 April 2012.
4. Reserve lists constituted in response to the publication of vacancy notices, in order to fill the positions of Data Protection Officer, Security Officer and Accounting Officer, published on 10 May 2012.

The procedure via the *Open Call for expression of interest* was finalized during the summer of 2012 and resulted in the establishment of reserve lists, which were approved by the Appointing Authority during July and early August 2012.

It is expected that by the end of 2012, the Agency will have achieved its target of recruiting the 75 staff members foreseen for 2012 in the Agency Establishment Plan and budget².

In early 2013, the Agency will concentrate on hiring the remaining 45 staff members, as envisaged by the Establishment Plan and budget. At that moment, the Agency staff will include Human Resources Officers and Assistants (recruited in the second semester of 2012). Therefore, the management of the recruitment process will be carried out directly by the Agency staff.

There is also an urgent additional requirement for Agency Staff to ensure management of encryption keys. According to Article 7 of the Agency Regulation (tasks related to the communication infrastructure), an external private-sector network provider "*shall be bound by the security measures referred to in paragraph 4 and shall have no access to SIS II, VIS or EURODAC operational data, or to the SIS II-related SIRENE exchange, by any means*". This Article also provides that the management of the encryption keys shall remain within the competence of the Agency and shall not be outsourced to any external private-sector entity. Cryptographic equipment shall therefore remain under the full operational management of the Agency. Subject to the formal approval of additional budget and staff allocations for these tasks in the framework of a revised multi-annual staff policy plan and the preliminary draft budget for 2014, recruitment of additional staff for operating cryptographic equipment for the

² Recruitment of staff on the reserve list for the open call for expressions of interest referred to above was launched immediately after the approval of the reserve lists. As of 29 August 2012, 50 offers of employment had been made. The first staff member recruited by the Agency started working in July 2012 in the premises of DG Home Affairs.

In addition, the recruitment procedure to hire a limited number of technical personnel with experience in the management of central units of Schengen and Dublin related IT systems (SIS 1, VIS and EURODAC) is expected to be completed by the end of September 2012. Offers of employment will be made immediately afterwards.

Finally, reserve lists for the positions of Data Protection Officer, Security Officer and Accounting Officer are expected to be available by the end of 2012.

network and for the management, testing and evolutions for management of encryption keys should be foreseen as of 2014. It is currently estimated that approximately 30 posts could be required for these tasks).

Taking account of the total number of items of cryptographic equipment and the number of sites for the SIS II, VIS and EURODAC projects, it is estimated that 21 operators are required to deliver 24/7 encryption key operation for these projects. The other staff would be required for active management, testing and evolution of the solutions provided.

Today, SIS II includes roughly 150 items of cryptographic equipment over 50 sites, VIS 180 cryptographic equipment over 60 sites and Eurodac 60 cryptographic equipment over 30 sites. In addition, in order to ensure the critical availability of the cryptographic equipment, a complete and redundant set of cryptographic management platforms has to be deployed in the 2 operational sites of the Agency. This requires a permanent presence on a 24*7 basis of 2 cryptographic operators on the main site and 1 backup on the backup site, which means 21 operators. (It is generally assumed that a permanent presence of 1 staff 24*7 requires 7 Full Time Equivalent taking into account holidays, illness, on-duty, permanence and recuperation time.)

These operators are in charge of continuous monitoring and incident management. In addition to the operator staff, a cryptographic solution requires active management, testing and evolutions. Due to the critical nature of the services relying on the cryptographic equipment, a multidisciplinary team of experts has to deal with product management, integration with network and applications, change and release management, maintenance and support. This requires an additional team of 5 to 10 staff, depending on the complexity of the cryptographic equipment.

With the exception of the above-mentioned resources, subject to approval, no additional recruitment is foreseen for the period 2014-2015 for tasks linked to the operational management of VIS, SIS II or EURODAC.

Depending on the results of an impact assessment and subject to the adoption of legal bases for the Registered Traveller Programme and Entry Exit systems, it is possible that the Agency may require human resources from 2015 onwards for developing the Registered Traveller Programme and Entry Exit systems. In the course of 2013, the Agency should start to examine scenarios for future resource requirements for the development of these two systems.

Training of the Agency's staff will also be a key priority. This will include induction training for new staff members and further training as necessary, according to tailor-made training plans for each staff member. Technical staff will undergo an assessment of their skills and requirements. This will be, followed by specific training on technical matters related to the IT systems and their business environment. There will also be specific training for management, including training on the business objectives of the systems. Last but not least, there will be a strong emphasis on team building activities, with a view to consolidating teams, focusing in particular on teams extending across different sites. Objectives have been fixed to ensure that a sufficient number of financial specialists are fully trained as soon as possible.

The Agency will also continuously strive to ensure that its administrative processes evolve in line with changes to EU procedures and regulations and newly emerging good practices.

Strategic Goal 2: Move towards becoming a centre of excellence

To nurture and enhance the expertise and best practices within the organisation and put in place effective governance, structure, resources, information tools, procedures and methodologies to enable the Agency to move forward towards becoming a centre of excellence for the management and development of large scale IT systems in the field of freedom, justice and security. This will also entail ensuring effective

networking with other agencies, bodies and authorities operating in related fields and, in particular, with those established in the area of freedom, security and justice.

In 2013, the initial building blocks of the centre of excellence will be put into place. The Agency will start off by putting in place adequate governance for ensuring alignment of business and ICT goals and the creation of value from IT-enabled business developments. This will be achieved via an action plan defined in 2012 for implementing Enterprise Governance of ICT³ which will also entail implementing essential maturity levels of the COBIT⁴ framework for IT governance in 2013. The Agency will progressively build on this work in subsequent years. The Agency will also implement best practices in IT service management from ITIL⁵, in particular with respect to the operation of the IT systems.

A further important activity in this area will be to work towards putting in place total quality management, with a view to full implementation of ISO 9001 in the medium term.

This work will also entail consolidating the Agency's structures, human resources and information management processes for technology watch and structured monitoring of new and forthcoming technological and economic developments (see point 2.6.6). The Agency will also participate in networking and expertise-sharing activities for these purposes.

In parallel, the Agency will also apply appropriate methodologies with a view to implementing new technologies in a cost-effective way for its own operations and for the systems under its management, cooperating closely with stakeholders. The optimization of knowledge management systems will also be important for allowing effective exchange and use of information already available within the Agency. The results of technology watch and research monitoring will feed into other decision-making processes and preparatory work of the Agency, including requirements, specifications and tender procedures. Given the nature of the systems managed by the IT Agency and the lead time for implementing changes, largely due to budgetary and procurement formalities, the most important impact on end users is likely to occur in the medium term and, in particular, for the first generation of systems to be developed by the Agency.

Strategic Goal 3: Preparations for taking on board additional systems

To plan ahead strategically for the systems that the Agency is likely to be required to develop and manage in the medium term, with a view to defining the human resource, budgetary and infrastructure requirements.

The Agency may also be made responsible for the preparation, development and operational management of other large-scale information systems in the area of freedom, security and

³ A management concept and international standard which seeks to define and embed processes and structures throughout the organization, in order to enable both business and IT people to execute their responsibilities, while maximizing the value created from their IT-enabled investments.

⁴ Control objectives for information and related technology (COBIT) is a framework created by ISACA in order to support governance of IT by defining and aligning business goals with IT goals and IT processes. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT defines 34 generic processes to manage IT, together with their respective process inputs and outputs, key process activities, objectives, performance measures and an elementary maturity model.

⁵ ITIL is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (ITILv3 / ITIL 2011 edition), it consists of five core publications, each of which covers an ITSM lifecycle stage. ITILv3 underpins ISO/IEC 20000, the International Service Management Standard for IT service management, although differences between the two frameworks do exist.

justice, if so provided by relevant legislative instruments, in accordance with the provisions of Article 1(3) of the establishing Regulation.

The Agency will look ahead, in order to anticipate the general implications of the additional IT systems that it may be required to develop and manage in the medium term and be in a position to ensure prompt delivery of input to decision-making at Commission level (notably on the Agency's personnel, budgetary and infrastructure requirements). The Agency will also ensure that there is enough flexibility in its internal organisation to take the initial implementation steps as soon as possible after the relevant legal bases are adopted.

Immediate priorities in this area, mainly related to Entry Exit and Registered Traveller Programme are addressed in further detail in point 2.6.1.4.

Strategic Goal 4: Continuous move to optimise cost-effectiveness

To move towards the proactive search for more cost effective ways of delivering the requisite level of service or technical excellence, both with respect to the Agency's own internal operations and the setting up and management of new IT systems. This goal also includes examining the scope for achieving cost savings for stakeholders.

The main priorities under this goal will be:

- To put in place an effective interface between technology watch activities (under Goal 2) and procurement procedures and to review performance in this area, with a view to continuous improvement.
- To attain a high level of expertise within the organisation on procurement matters in 2013 and to progressively reinforce this expertise bringing it up to the highest level (by training, information exchange and dissemination of information summarizing the basic rules and procedures). Adequate advisory services on financial matters will also be put in place within the Agency.
- Internal communication will also include actions to ensure that the priority of achieving technical and organisational excellence in the most cost effective way is firmly embedded in the organisational culture.

Operational goals for financial management are covered in point 2.6.8 and actions PC1 et seq. in point 2.7.

Key operational objectives

This point describes the main operational objectives of the Agency in 2013. The specific operational objectives in point 2.7 go into further detail, providing a clear link to outputs/results and covering a number of administrative tasks not covered below.

Performance indicators for most of these specific objectives, in particular those not related to the management of the systems, the communication infrastructure or security are given directly in point 2.7. This applies in particular for administrative and coordination tasks.

Comprehensive agreements on the service level that the Agency will guarantee to the Member States for management of the systems, the communication infrastructure and security will be approved by the Management Board as soon as possible in 2013. These will include detailed indicators, with a view to guaranteeing a service level across the board

equivalent to or surpassing the arrangements in place with other operators prior to take-over of these activities by the Agency⁶.

The indicators contained in this document and those to be developed at a later stage will focus on key criteria such as timeliness, quality of service, stakeholder satisfaction and achievement of the objective (supply of deliverable).

Stakeholders require confidence and a reasonable expectation of deliverables and services to be provided by the Agency. Priorities have therefore been fixed taking account of input from stakeholders. This draft work programme was discussed by the Management Board in its meetings of March and June 2012 and the opinions of the Board have been taken into account in the fixing of priorities in this programme. The portfolio of deliverables and services outlined in the present work programme balances stakeholders' needs, the outcome of the risk analysis exercise and the need to respect fundamental requirements laid down in the establishing Regulation for the Agency and the legal bases for the systems that it will operate.

The objective of integrating new system users such as Croatia, Cyprus, Ireland and the UK is covered for each individual system in point 2.6.1.

Operational Management of IT Systems and preparations for future IT systems

SIS II

To carry out all necessary activities to ensure continuity of operations of SIS II from the time it enters into operations in March 2013. This will include supervision of the work of the selected contractor for the maintenance contract and starting technology watch activities related to this project.

By the end of 2012, the SIS II Transition Plan, which aims to enable the transfer of knowledge from the main development contractor (HPS) to CSIS⁷ which will take over SIS II temporarily pending the putting in place of the relevant Agency teams, is due to have been implemented and the main development contractor will have handed over SIS II to CSIS.

In the period up to March 2013, the Agency will take over the full operations of SIS II, including the follow up of the final migration preparations, shadowing the CSIS staff responsible for implementing these deliverables.

As from March 2013 when SIS II is due to enter into operations, the Agency will become responsible for the operational management of Central SIS II, taking over the tasks conferred on the Management Authority by Regulation (EC) No 1987/2006 and Decision 2007/533/JHA. The Agency will be responsible for all the tasks necessary to keep Central SIS II functioning 24 hours a day, 7 days a week in accordance with the above-mentioned regulations, in particular the maintenance work and technical developments necessary for the smooth running of the system.

The Agency will implement and apply the Service Support and Delivery processes to ensure that the IT Service Management is aligned with these critical and high availability operations. In particular, the Agency will be responsible for the following tasks in this area:

⁶ With respect to VIS and EURODAC, the communication infrastructure and security, the Agency will have to maintain the level of service that was in force prior to its take-over of the systems. It will also guarantee an equivalent service level for SIS II.

⁷ The Central Site for the SIS II system, managed by the French authorities in the transitory phase pending the take-over of the SIS II project by the Agency

- SIS II Service Support Processes (incident management, problem management, configuration management, change management and release management)
- SIS II Service Delivery Processes (Availability Management, Continuity Management, Service Level Management, Capacity Management).

Assistance will also be provided to Croatia with its technical preparations for accession to SIS II which are now intensifying in light of its preparations for accession to the EU in mid 2013. The Agency will also provide assistance to Cyprus with its preparations for achieving technical readiness in 2013 for integrating into SIS II. The actual integration of Cyprus into SIS II may only go ahead once the necessary conditions for the application of all parts of the Schengen acquis will be met, as provided for in the Act of Accession of 2003. A number of other Member States will also require assistance with technical matters related to their future integration into SIS II, in particular the UK and Ireland which will probably integrate into this system from 2014 onwards.

The contract for the call for tenders published in 2012 for the maintenance of the SIS II after Final System Acceptance is due to be signed by the Commission on behalf of the Agency at the end of July 2013. The Agency will prepare for taking over operational aspects of this contract (supervision of the preparations for maintenance of the system and of the actual maintenance work as from March 2013).

One priority area to examine, with a view to making future technological enhancements to SIS II, will be biometrics. Initially photographs and fingerprints will only be used to confirm the identity of a person who has been located as the result of an alphanumeric search made in SIS II. The SIS II legal instruments also specify that, as soon as this becomes technically possible, fingerprints may also be used to identify such a person on the basis of his/her biometric identifier⁸. The Commission is required by the legal bases to present a report on this matter. The Agency is prepared to contribute to this report if required.

See also specific operational objective AM1 in point 2.7.2. Reporting obligations for SIS II are covered in point 2.6.3, technology watch activities are covered in point 2.6.6 and training of NS.SIS and SIRENE staff is covered in 2.6.5 and specific objectives GC9 and 10.

VIS

The Agency will be responsible for operational management of the VIS, ensuring continuity of operations. It will also be responsible for ensuring that the technical characteristics of VIS will be able to support world-wide roll out. The Agency will also supervise and monitor the maintenance work under the contract for maintaining the VIS in working order and will also take over responsibility for work under this contract to upgrade the VIS. The Agency will also ensure successful testing of VISMAIL 2 by the end of the year.

The Agency will be responsible for operational management of the VIS. This will include all the tasks necessary to keep the VIS functioning 24 hours a day, seven days a week in accordance with the VIS Regulation. A key component of these activities will be the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of operational quality, in particular as regards the time required for interrogation of the central database by consular posts, which should be as short as possible.

⁸ Article 22 b) and c) of the SIS II Regulation and Decision. Before this functionality is implemented in SIS II, the Commission shall present a report on the availability and readiness of the required technology on which the European Parliament shall be consulted.

The Agency will implement and apply the Service Support and Delivery processes to ensure that the IT Service Management is aligned with these critical and high availability operations. In particular, the Agency will be responsible for the following tasks in this specific area:

- VIS Service Support Processes (incident management, problem management, configuration management, change management and release management)⁹
- VIS Service Delivery Processes (Availability Management, Continuity Management, Service Level Management and Capacity Management)

By the end of 2012, roll-out of VIS to the first 3 Regions (North Africa, Middle East and the Gulf will have been completed. Roll-out to other geographical regions is due to take place in 2013, possibly extending into 2014. The Commission will be responsible for political aspects of this roll-out. The main responsibility of the Agency will be to ensure that the technical characteristics of VIS will be able to support this world-wide roll out. As part of this process, the VIS Advisory Group will be requested to provide an opinion on this matter.

With respect to financial management, the Agency will continue to supervise and monitor the maintenance work under the contract for maintaining the VIS in working order concluded by the Commission in the name of the Agency. It will also then take over responsibility for work under this contract to upgrade the VIS. The main objectives of this upgrade will be, firstly to update the system in response to Member States requests, notably with respect to increased capacity¹⁰, fulfilling the legal obligation under Article 26 of the VIS Regulation (operational management) to ensure that the best available technology is used for the system. The second objective of this upgrade will be to introduce modifications related to the implementation of the new Visa Code adopted on 5 May 2010¹¹. Work to enhance the capacity of VIS will be prioritised, in order to complete the roll out of the VIS and ensure a stable level of operation and support to Member States. The Agency will take over contractual matters relating to this contract once it has been granted financial independence.

At the start of 2013, an upgraded version of the VIS Mail Relay (the Central server) for the next phase (VIS Mail Phase 2) is due to be ready for testing. The Application Test Plan for Phase 2 developed by an external contractor of the Commission will also have been completed. In parallel, Member States are due to have completed work on their national applications for this deliverable.

The Agency will coordinate any remaining activities related to the development of VIS Mail Phase 2, as well as the VIS Mail Phase 2 tests with the Member States. These are scheduled to take place between January and July 2013. The Agency will follow up and validate the results of these tests. After the successful completion of all tests, between August 2013 and October 2013, the Agency will ensure the integration, preparation and the move to the production environment (following a Decision according to Article 46 of the VIS Regulation). According to the schedule, VIS Mail Phase 2 is due to be ready by the end of October 2013, which should coincide with the finalisation of the roll-out of the VIS in all regions¹². Subsequently there will be work for the integration of new Member States likely to

⁹ The configuration management database shall be maintained and kept up-to-date, as well as the Trouble Shooting Guide, the Knowledge Database and an exhaustive list of Frequently Asked Questions for the users

¹⁰ Expected capacity requirements for final roll-out are significantly higher than those anticipated in the original feasibility study carried out in 2002.

¹¹ It was decided at the time to press ahead with VIS development on the basis of the specifications that were valid at that time, in order to avoid further delay to the project.

¹² There is no legal provision on the exact duration of the VIS Regional Rollout, as this depends on the Member States and the speed at which they deploy the system. It must therefore be understood that the Decision

join the Schengen Area in the near future (for example, Croatia and preparations for ensuring technical readiness of Cyprus).

The Agency should also consider putting in place a Business Continuity Plan that takes due account of the end to end functioning of national systems as well as the central system, considering end to end Business continuity strategies, best practices and testing for the volunteering Member States.

See also specific operational objective AM2 (point 2.7.2). Monitoring, reporting and statistics activities are described in point 2.6.3 and technology watch is covered in point 2.6.6.

EURODAC

To operate the EURODAC central database on behalf of the Member States in conformity with the provisions of the EURODAC Regulations, to ensure the removal of the system from Luxembourg to Strasbourg and Sankt Johann im Pongau and to start implementing the changes to the system foreseen in the Recast Regulation, subject to the adoption of this instrument. A further priority will also be to assist Croatia with its technical preparations for accession to EURODAC. The Agency will also ensure operational supervision of any work carried out by contractors for the above-mentioned tasks, particularly in relation to additional development work and relocation of the system.

The Agency will be responsible for the operation of the EURODAC central database on behalf of the Member States, in conformity with the provisions of the EURODAC Regulations¹³.

Negotiations on a proposed recast of the EURODAC Regulation are in progress and it will hopefully be adopted as from the end of 2012. Changes foreseen by the current text include the marking of records (instead of blocking) and changes to time limits for Member States to submit an asylum request. It is possible that other functionalities may be retained in the finally adopted version.

The Agency will implement the changes foreseen in the Recast Regulation making sure that the technical changes will make optimal use of new technologies and processes. A prior assessment study is necessary, in order to clearly identify the technical (hardware, software, professional services) and financial impact of these changes on the current systems (CU - BCU - TEST). The implementation of these changes will most likely start in 2013, depending on the outcome of the assessment study and the procurement procedure.

The Agency in 2013 will also ensure the removal of this system from Luxembourg to Strasbourg and Sankt Johann im Pongau. This will include operational supervision of contractors' work related to this removal, notably with respect to any additional IT equipment that may be required. The related procurement procedures will be concluded by the Commission on behalf of the Agency. Once the Agency has been granted financial independence it will take over responsibility for financial and contractual aspects.

Croatia is due to join EURODAC in 2013. The Agency will play an important role in providing assistance to Croatia in all phases of its technical preparations.

Most of the current contracts for EURODAC with the Commission expire at the end of 2012 and need to be extended / renewed. Procedures for extension, renewal and transfer to the

according to Art. 46 will only be taken when the regional rollout is almost finished and not necessarily at exactly 22 months after the go-live of VIS.

¹³ Regulations (EC) No 2725/2000 and (EC) No 407/2002.

Agency of these contracts will be completed by the Commission on behalf of the Agency in 2012. In the preparation and negotiation of these procedures and contracts, top priority will be given to cost effectiveness.

Other EURODAC-related tasks of the Agency are covered in points 2.6.2 Security and communication infrastructure, 2.6.3 Monitoring, reporting and statistics and 2.6.6 (monitoring of research and technology watch). The key EURODAC-related technology watch priority for 2013 will be to ensure that any technical changes needed to meet the provisions of the Recast instrument, will make optimal use of new technologies and processes.

See also specific operational objective AM3 in 2.7.2.

Possible development and operational management of other systems

If the legal bases for the Registered Traveller Programme and Entry Exit System are adopted in 2014, the Agency could be asked to start developing these systems as from 2015. It would therefore be advisable for the Agency to estimate its possible infrastructure, staffing and organisational requirements, taking account of the financial fiches of the legislative proposals for these systems, with a view to being able to start preparations as soon as possible, in the event that the legal instruments should be adopted.

As announced in the Smart Borders Communication of 25 October 2011¹⁴, the Commission intends to present proposals in 2012 for two legislative instruments laying down the legal framework for these systems. These proposals would include provisions entrusting the development and operational management of a Registered Traveller Programme and an Entry Exit system to the Agency. According to the current planning, it is envisaged that the negotiations with the Council and Parliament for the adoption of these regulations could be completed by the end of 2014. If these these legal bases are adopted, and if adoption takes place within this estimated time frame, it is envisaged that the Agency would start work on these systems as from 2015.

In parallel, it is possible that an amendment to the Agency Regulation may be adopted, with a view to transferring responsibility from the Commission to the Agency of certain responsibilities for the communication infrastructure and security with respect to existing systems and putting in place the framework for resources needed by the Agency for the development of the new systems.

Given that the Agency's Establishment plan would also need to be modified, in the event that the legal bases for the Registered Traveller and Entry Exit systems are adopted (with a view to providing the Agency with the additional human resources needed for the development of these systems, it would be advisable to tentatively plan ahead for this in 2013.

Work would only commence on the development of these new systems if and when the European Parliament and Council have adopted the respective legal bases, setting out clearly the specifications. However, the Agency should already start planning ahead tentatively with a view to defining more specific requirements in terms of infrastructure, staffing and organisation, taking account of the information included in the financial fiches of the legislative proposals for these systems.

See also specific operational objective AM4 in point 2.7.2.

¹⁴ COM(2011)680

Security and the communication infrastructure

Security

The Agency will put in place and implement security measures and business continuity measures for its own organisation, for the systems that it will manage and for the communication networks for these systems, and carry out any other security tasks foreseen in the establishing Regulation and legal instruments for the IT systems.

In 2013, the Agency will complete work on the business continuity and disaster recovery plan for the Agency and finalize preparations for taking over security aspects of SIS II.

It will also ensure the full implementation and compliance with the various security measures and security plans for the Agency itself¹⁵, the systems¹⁶ that it will manage (covering matters such as organisation of security, technical measures including measures to ensure protection of records, business continuity, access control, accountability - ensuring that every access to and all exchanges of personal data are recorded at central level, cooperation with EDPS and follow-up of EDPS audits), the communication networks for these systems¹⁷ (including procedures and security provisions for business continuity, management of contractors and management of encryption keys), and data protection measures as regards security for the exchange of supplementary information through the SIS II communication infrastructure.

Furthermore, the Agency will carry out any additional security tasks assigned to it under the legal instruments for the systems that it operates such as regular reporting on security matters within the more general framework of reporting on the systems.

See also specific operational objectives on security (in particular MAN3 in point 2.7.1 and SE 2 & SE5 in point 2.7.8).

Communication Infrastructure

Initially, the Agency will be responsible for supervision, security and coordination of relations between the Member States and the network provider for the communication infrastructure for EURODAC, VIS and for SIS II after its entry into operations in March 2013. It will also ensure the full respect of data protection provisions concerning any access to data in the system by external bodies.

It is possible that the Agency's competencies with respect to the communication infrastructure (supervision, security and coordination of relations between the Member States and the network provider for SIS II, VIS and EURODAC) could be extended to allow it to take over other systems and/or to assume responsibility for financial matters in this area, subject to a modification of the relevant legal provisions.

Once the Agency takes over VIS and EURODAC and, as from March 2013 when it will take over SIS II, responsibility for the communication infrastructure for each respective system will be divided between the Agency and the Commission¹⁸. The Agency will be responsible for

¹⁵ The Security Plan, the Disaster Recovery Plan once this is approved, confidentiality and professional secrecy requirements and rules for staff working with data in the systems.

¹⁶ Security measures and security plans for SIS II, VIS and EURODAC.

¹⁷ Security measures and security plans for the communications network for SIS II, VIS and EURODAC prepared by the Agency.

¹⁸ In order to ensure coherence in exercise of their respective responsibilities for the network, the Agency and the Commission shall agree on operational working arrangements between them, to be reflected in a Memorandum of Understanding (Article 7(2) of the Agency Regulation). This is due to be approved in 2012).

supervision, security and coordination of relations between the Member States and the network provider for the communication infrastructure for these three systems.

The Commission will be responsible for all other tasks relating to the communication infrastructure, in particular, the tasks relating to the implementation of the budget, acquisition and renewal and contractual matters¹⁹. The Commission will also retain responsibility for the adoption of the security measures and the security plan for the communication infrastructure for SIS II²⁰.

In accordance with the establishing Regulation, tasks relating to the operational management of the communication infrastructure may be entrusted to external private-sector entities or bodies in accordance with Regulation (EC, EURATOM) No 1605/2002. In such a case, the network provider shall be bound by the security measures laid down in the basic instruments for each system and shall have no access to SIS II, VIS or EURODAC operational data. Without prejudice to existing contracts on the network of SIS II, VIS and EURODAC, the management of the encryption keys shall remain within the competence of the Agency and shall not be outsourced to any external private sector entity. The Agency will ensure that these provisions are respected.

The S-TESTA contract with DG DIGIT is due to expire at the end of 2013. With regard to existing activities, it will be possible to have specific contracts running in this framework until September 2014, but with limited change requests²¹. A new framework contract should be available in 2013. Contractual formalities under the new framework contract and the migration of SIS II, VIS and EURODAC to the new network have to be completed by September 2014 at the very latest. The Commission is responsible for contractual matters related to the network. A key priority for the Agency in 2013 will be the preparation and implementation of network migration in its specific areas of competence (supervision, security and management of relations between the Member States and provider of the new network for VIS, SIS II and EURODAC). The new framework contract will also have to be used subsequently for the Entry Exit and RTP networks subject to approval of the relevant legal bases (the legal instruments for these systems would entrust contractual matters for the network to the Agency). At present the Commission is responsible for all contractual aspects related to the networks of SIS II, VIS and EURODAC. In the future, it is possible that changes would be made to the SIS II and VIS legal bases and to the Agency Regulation to entrust the Agency with responsibility for contractual matters for the networks for these systems.

See also specific operational objective OPU2 in point 2.7.5.

Monitoring, reporting and statistics

The Agency will produce the reporting and statistics²² on the use of the IT systems under its management and monitor their functioning, as foreseen in the legal bases for

¹⁹ Article 26 (2) and (3) of the VIS Regulation, Article 15 (2) and (3) of the SIS II Regulation and Decision and Article 5(b) of the Agency Regulation

²⁰ Article 16(1) of the SIS II Regulation

²¹ The sTESTA Framework Contract expires on 28.9.2013 and the last specific contracts can cover services until 28.9.2014, but with limited change requests allowed/possible over the last year.

²² With respect to VIS, the Agency will need statistics in order to carry out the following tasks assigned to it under the VIS Regulation:

- Technical maintenance, article 50 (2): the Agency will require access to the necessary information on processing operations in VIS
- Reporting on the technical functioning of VIS, Article 50 (3)
- Providing the Commission with the information necessary to produce the overall evaluations Article (50 (7))

these IT systems and reflected in the establishing Regulation. It will report regularly to the European Parliament, the Council and the Commission on the technical functioning of the systems, including the security thereof and will also provide the Commission with information that it requires for the regular evaluation of VIS, EURODAC and SIS II.

See also specific operational objectives AS1-5 in point 2.7.6.

Cooperation with other Agencies, projects and actions in the field of freedom, security and justice

Cooperation with Agencies such as CEPOL, EASO, ENISA, EUROJUST, EUROPOL, FRONTEX and FRA will continue in 2013. An action plan will be prepared setting out clear goals and objectives for cooperation with each of these Agencies. Complementarity will be a key priority in many of these relationships.

The Agency will also take account of European and international standards, in particular the EU Information Management Strategy and will follow up developments with the European Information Exchange Model.

Agencies

Cooperation with Agencies such as the European Police College (CEPOL), European Asylum Support Office (EASO), the European Network and Information Security Agency (ENISA), EUROJUST, the European Law Enforcement Agency (EUROPOL), the Fundamental Rights Agency (FRA) and the European Agency for the Management of Operational Cooperation at the External Borders (FRONTEX) will continue in 2013, building on the relations already established in 2012. One priority area will be to negotiate a memorandum of understanding with other European Agencies involved in training matters related to the area of freedom, security and justice.

The Executive Director of the Agency will participate in the annual meetings of the heads of JHA Agencies and a representative of the Agency (desk officer level) will participate in the JHA Agencies Contact Group, with a view to exploring and agreeing on other forms of cooperation. The Agency will prepare an action plan setting out clear objectives for cooperation with each of the other agencies referred to below. Representatives of a number of these Agencies will be invited to give presentations at Management Board meetings.

• CEPOL

One of the tasks of the Agency for operational management of large scale IT systems is to facilitate and ensure training for Member State users concerning the systems that it operates. It is also required to provide training on the technical use of SIS II for SIRENE staff in the Member States and for Schengen evaluation team members and lead experts.

Law enforcement personnel are a key component of the users of the IT systems operated by the Agency. The Agency should coordinate its training for this stakeholder group with CEPOL, with a view to ensuring complementarity. One approach to explore is the development of joint curricula. Further information on this matter is given in point 2.6.5.

Training for Schengen evaluation team members and lead experts will also have to be discussed with FRONTEX with a view to agreement on a memorandum of understanding between the agencies involved in this area.

- **EASO**

The function of this Agency is to strengthen European Union (EU) countries' practical cooperation on asylum, to support EU countries whose asylum and reception systems are under particular pressure and to enhance the implementation of the Common European Asylum System (CEAS). The key cooperation objective, initially, will be to set up a sound working relationship with this Agency, ensuring complementarity.

- **ENISA**

The main task of ENISA is to enhance the capability of the EU, the Member States and the business community to prevent, address and respond to network and information security problems. It serves as a Centre of Expertise, stimulating cooperation between the public and private sectors in this area. Initial objectives for cooperation with this Agency should focus on exchange of information and expertise.

- **EUROJUST and EUROPOL**

Decision 2007/533/JHA (the SIS II Decision) provides for access to SIS II data by specifically authorised staff of EUROPOL and national members of EUROJUST and their assistants. These bodies may only access the specific data that they require for the performance of their tasks. EUROPOL will also obtain access to consult the data in VIS in relation with the application of Decision 2008/633/JHA.

Both of these Agencies may attend the meetings of the Management Board of the Agency as observers when a question concerning the application of the SIS II Decision is on the agenda. EUROPOL may also attend the meetings of the Management Board as observers when a question concerning the application of the VIS Decision is on the agenda.

EUROJUST supports the competent authorities of the Member States to render their investigations and prosecutions more effective when dealing with cross-border crime. In addition to matters related to its own participation in SIS II, the key cooperation objective, initially, will be to set up a sound working relationship with this Agency, ensuring complementarity.

The main mission of EUROPOL is to make Europe safer by assisting the Member States of the European Union in their fight against serious international crime and terrorism. It handles information sent by or to the Member States for the purposes of criminal investigations, intelligence analysis, etc. The Agency for operational management of large scale IT systems in the field of freedom, security and justice, on the other hand, is specialised in operating and developing IT systems or any other form of information exchange platform without touching the data that passes through the systems under its responsibility. In addition to matters relating to the participation of EUROPOL in SIS II and VIS, the Agency could envisage cooperation with a view to providing EUROPOL with IT expertise and a framework for managing platforms for information exchange.

- **FRA**

The IT systems operated by the Agency for operational management of large scale IT systems may generate human rights concerns, ranging from data protection to restrictions on freedom of movement. The Agency will keep FRA informed of its activities, the legal regime applicable to the systems under its management, the responsibilities of the Member States with respect to data processing and the technical constraints inherent in these IT systems.

- **FRONTEX**

One priority area to clarify with FRONTEX (and also with CEPOL) will be the training related to technical use of SIS II provided by the Agency for operational management of large scale IT systems for Schengen evaluators and lead experts. The Agency intends to explore the possibility of concluding a memorandum of understanding with the agencies concerned including FRONTEX on this and other matters. Other suggestions for areas where the Agency could provide support to FRONTEX would be for researching, testing and developing IT systems for assisting FRONTEX in its activities. For more substantial tasks of this nature with resource and budget implications, it would be necessary to adopt legal provisions conferring these tasks to the Agency.

European Information Exchange Model

The establishing Regulation provides that "the Agency should follow European and international standards taking into account the highest professional requirements, in particular the European Union Information Management Strategy" (Recital 22). The EU Information Management Strategy²³ (IMS) provides a methodology to ensure that decisions about the need for managing and exchanging data and decisions about the ways to do so are taken into account in a coherent, professional, efficient and cost-effective way, accountable and comprehensible to citizens and professional users. In this context the Commission will present a Communication on the European Information Exchange Model (EIXM) in December 2012. Taking full account of the IMS, the EIXM aims to achieve better coherence and consolidation in the area of information exchange for law-enforcement cooperation²⁴. The Agency will continue to follow up developments with the EIXM with a view to defining the possibilities for future cooperation once the EIXM policy has been endorsed at political level.

See also specific objective GC2 in point 2.7.3.

Training for national authorities on the technical use of the IT systems

The Agency will provide training on the technical use of SIS II, VIS and EURODAC to the national authorities participating in these systems. It will also provide training for SIRENE-staff (SIRENE- Supplementary Information Request at the National Entries) and training of experts on the technical aspects of SIS II in the framework of the Schengen evaluation.

The Agency will be responsible for providing training on the technical use of SIS II, VIS and EURODAC to the national authorities participating in these systems, as laid down in the founding Regulation and the specific legal bases for the IT systems under its management.

This will also include training for SIRENE-staff (SIRENE- Supplementary Information Request at the National Entries) and training of experts on the technical aspects of SIS II in the framework of the Schengen evaluation.

The Agency's programme of training activities for SIRENE staff in the Member States in 2013, will take account of discussions held in the course of 2012 to clarify the respective roles of the Agency, CEPOL and Member States in this area.

In concrete terms the Agency will sign a memorandum of understanding with CEPOL and agree on the inclusion in CEPOL's training curricula for law enforcement authorities of the relevant SIRENE and SIS II training. The memorandum should also cover division of responsibility between the agencies.

It is envisaged that training of Member States authorities on SIS II will commence once the operational manuals for these systems have been validated. At this stage, subject to the completion of the above-mentioned discussions with CEPOL, it is envisaged that training by the Agency will focus on training visits to the technical site for the national authorities participating in these systems, in order to foster knowledge transfer. Training sessions would be held in small groups with a demonstration of the relevant system and a detailed explanation of the operational manual.

²³ The IMS was adopted by JHA Council on 30.11.2009 (see doc. 16637/09 JAI 873).

²⁴ The first step of EIXM carried out in 2010/2011 consisted of a mapping exercise on the four areas of legislation, communication, information flows and technology.

Similarly, the Agency's programming for training for Schengen evaluation team members and lead experts in technical aspects of SIS II will take account of discussions held in 2012 to clarify the respective roles of the Agency, CEPOL and FRONTEX. A key objective of these discussions will be to examine the roles assigned to each agency for this specific objective in their respective legal bases and to achieve complementarity by ensuring that each Agency offers a different portfolio of training activities, which when combined cover all aspects of the Schengen Evaluation process.

The future Regulation on the establishment of an evaluation and monitoring mechanism to verify the application of the Schengen Acquis, currently in negotiation in the European Parliament and Council, is also likely to have an impact on future programming of training in this area.

With respect to VIS and EURODAC, the Agency will also need to coordinate development of curricula with national authorities and establish a training delivery plan in cooperation with these authorities.

See also specific operational objectives GC 9-11 in point 2.7.3 & cooperation with other EU Agencies (point 2.6.4).

Training for the Agency's staff is covered in point 2.5.1.

Monitoring of research and technology watch

The Agency, in cooperation with the Member States, is required to ensure, that at all times the best available technology, subject to a cost-benefit analysis, is used for all applications under its management, including the IT systems, software for administration and the networks. It will also apply the same principles for its own internal systems. This priority is reflected in strategic goals N° 2 "Moving towards becoming a centre of excellence" and N° 4 "Optimising cost-effectiveness".

The Agency will put in place structures, resources, information tools, procedures and methodologies for technology watch (including monitoring of research) to enable it to take maximum advantage from new technological developments relevant to its activities. This will include the monitoring of research. The putting in place of Enterprise governance of ICT referred to earlier, will ensure that the fruits of this work are geared towards delivering business value. The advisory groups will play a crucial role in this work.

Monitoring of Research

The Agency will monitor the developments in research relevant for the operational management of SIS II, VIS, EURODAC and other large-scale IT systems. Specific priorities will be defined at a later stage, taking account of the opinions of the Advisory Groups.

The Agency will keep the European Parliament, the Council, the Commission and the European Data Protection Supervisor (where data protection issues are concerned) informed of developments at least twice a year.

Technology watch

This work will consist of monitoring new technological breakthroughs, innovative techniques and processes, standards, legislation, security issues and solutions relevant to the operation, management and future development of the IT systems in the field of justice, freedom and security, including impending changes in the operational sectors that these IT systems aim to support. It will also entail following-up developments in new equipment and software, with a view to ensuring efficient procurement. The Advisory Groups will also make an important contribution by providing advice on matters relevant to specific systems and areas that

should be earmarked for pro-active monitoring. The Agency will build up on the contacts already started in 2012, with a view to ensuring effective networking, cooperation and exchange of good practice with other agencies and authorities operating in related fields.

A few examples of areas to examine under both this heading and monitoring of research would be biometrics, including functionalities for biometrics search, technological advances that will increase the performance, reliability and flexibility of systems, such as virtualisation and new trends in higher performance database design and querying, technologies and applications enabling more effective treatment of identity, including fuzzy logic and technologies and applications to facilitate interconnectivity.

See also specific operational objectives MAN1 (Implementation of Enterprise Governance of ICT and other standards, point 2.7.1), GC1 (technology watch, point 2.7.3) and AS6 (Monitoring of research, point 2.7.6).

Communication

The Agency will organise communication activities on its own initiative in the fields within its tasks including the establishment of its own web site. It will also be involved in preparations for the SIS II campaign scheduled for the first quarter of 2013 and the organisation of repeat campaigns where required. The Agency is also required by the legal bases of the IT systems under its responsibility to take care of the publication of certain types of information, including lists of national authorities which have the right to access or use data in the IT systems managed by the Agency and updates to such lists.

See also specific operational objectives GC5-6 in point 2.7.3.

Financial management, infrastructures, logistics and administrative tasks

The Agency will consolidate its financial teams and procedures, with a view to obtaining financial independence during the year. It will also be responsible for ongoing building management and logistics tasks, progressively putting in place in-house arrangements to replace the service level agreements with central Commission services. In parallel, it will make sure that all work related to the future premises in Tallinn and the upgrade of the technical site at Strasbourg remain fully on track. See also point 1.2.9 for further information, including consultation of the Management board on financial matters.

Financial management

The Agency will deal with a wide range of procurement procedures, including procedures for upgrading buildings and facilities, procurement of equipment and furnishings and specialised procurement related to the IT systems under its management. The Agency will consolidate its financial procedures and teams and ensure that staff are fully trained in this area in 2013, with a view to seeking financial independence. It will strive to obtain good value for money in all areas of financial management and regularly review the scope for improving cost effectiveness of its operations.

Further information on detailed operational objectives is given in point 2.7.7.

Administrative and logistical tasks

At present many of the basic administrative and logistical tasks related to the Agency and its personnel are carried out under the terms of the various service level agreements between the Agency and Commission Services and/or EU bodies. From 2013 onwards, the Agency will progressively move towards setting up its own in-house services, or outsourcing services under its own responsibility, for many of the items covered by these initial SLAs. One major

priority for the Agency itself early in 2013 will be its involvement in the procedures for completion of the first wave of recruitment.

Further information on detailed operational objectives is given in AS7 (logistics and building management) and AS 8-9 (human resources) in point 2.7.6.

Preparation and management of premises and sites

The following activities are foreseen in 2013:

- **Headquarters building in Tallinn, Estonia:** The Agency is situated in temporary premises since June 2012. The Agency will supervise the preparatory work related to the permanent premises to be provided by Estonia for the Agency headquarters, ensuring that construction work remains on schedule for meeting the target of having the building available in 2014.
- **Preparations for the technical site in Strasbourg:** priority works necessary for the entry into operations of the Agency (identified in a study carried out by an external contractor in 2012) are due to be implemented by December 2012 at the latest. Further reconversion works may be necessary in the course of 2013. One key priority will be to ensure timely readiness of infrastructures related to SIS II. The Agency will also carry out further analysis of the implications for the site of developing future systems, taking account of the existing study.
- Further reconversion works may also be necessary in the course of 2013.
- **Infrastructure management on the back up site:** Work in 2013 will consist essentially of routine infrastructure management and maintenance.

Detailed operational objectives are given under AS7 (logistics and building management) in point 2.7.6.

Management Board and Advisory Groups

Management Board

In the area of governance, the core objective will be to continue to ensure that the Agency performs the tasks set out in its establishing Regulation in the most cost-effective way, taking account of medium-term strategic goals. As in 2012, the staff of Agency will provide continuous support to the Management Board in carrying out its mandate. This includes ongoing contact with the Board members, organisation of the statutory meetings and preparation of the documents to support its work. The Executive Director shall participate in the meetings of the Management Board without voting rights. The Management Board will meet a minimum of once every six months.

In addition to the approval of standard documents in the annual budgetary and planning lifecycle such as the budget and draft budget (estimates) for 2014, the Annual Activity Report for 2012 and the draft Annual Work Programme for 2014, important matters to be decided on by the Management Board in 2013 will include matters related to the preparations for the permanent premises in Tallinn and implementation of the works on the technical site in Strasbourg. The Management Board will also have to endorse decisions related to the removal of EURODAC.

Advisory Groups

The staff of the Agency will also provide full support to the work of the Advisory Groups. The Executive Director or his/her representative will be entitled to attend all meetings of these groups as observers.

There will initially be three configurations of the Advisory groups (SIS II, VIS and EURODAC). These groups are due to meet every 1-2 months in 2013. The procedures for their cooperation and their operation shall be laid down in the Agency's rules of procedure.

The main role of these groups will be to provide the Management Board with expertise relating to large-scale IT systems and, in particular, in the context of the preparation of the annual work programme and the annual activity report. They will also provide recommendations related to security measures and an opinion on multi-annual work programmes. Members of these groups may also be called upon to assist members of the Management Board. Other tasks of the Advisory Groups could include providing information technology expertise to the Management Board on the systems, preparing technical specifications of a descriptive nature which do not impose normative provisions on the Member States and the Commission, providing input on the draft reports on the technical functioning of the systems, on the training of experts, on the orientation for monitoring of research, on statistics on the systems and on any other matter strictly related to the development or operational management of the systems. The specific priorities will be fixed by each group. In particular, their work will take account of operational priorities for the relevant system.

Priorities for these groups for 2013 include ensuring the ability of VIS to meet the technical requirements of future world-wide roll-out, follow-up of the entry into operations of SIS II, the growth in use of this system, technical matters relating to the relocation of EURODAC from Luxembourg to Strasbourg and Sankt Johann im Pongau and the adaptation of EURODAC to take account of the future Recast Regulation. A further priority for all of the groups will be the technical preparations for the accession of new Member States, in particular Croatia to these IT systems, preparations for ensuring technical readiness of Cyprus to join SIS II and VIS (as mentioned above, the necessary conditions for the application of all parts of the Schengen acquis, as provided for in the Act of Accession of 2003 need to be met in order for Cyprus to actually join the Schengen area) and the integration of countries such as the UK and Ireland into SIS II.

Detailed operational objectives related to administrative support for the Management Board and the advisory groups is given under AS10-11 in point 2.7.6.

Specific operational objectives and performance indicators

Contents:

2.7.1 Objectives to be steered at Agency level (with input from the Executive Director)

2.7.2 Application Management and Maintenance

(Operational management of SIS II, VIS and EURODAC and preparations for new IT systems)

2.7.3 General Coordination

(Technology watch, inter-agency cooperation, data protection, legal advice, internal and external communication, training for agency staff and training for MS, SIRENE operators and Schengen evaluators)

2.7.4 Internal Audit

2.7.5 Operational matters and Infrastructure

(Systems management, network, helpdesk, monitoring the functioning of the systems)

2.7.6 Resources and administrative matters

(Monitoring, reporting, information for the Commission, the EP, EDPS and the MS, statistics, Monitoring of research, logistics and building management, human resources, administrative support to the management board and the advisory groups)

2.7.7 Procurement and Contracts

2.7.8 Security

Objectives to be steered at Agency level (with direct input from the Executive Director)

Goal/ Obj N°	Objective	Outputs & performance indicator	
		Output	Performance indicator
MAN1	<p>1.1 Prepare action plan for implementing Enterprise governance of IT.</p> <p>1.2 The action plan in 1.1 above should also include work to implementing the essential maturity levels of the COBIT framework for IT governance in 2013.</p> <p>1.3 Plan ahead with a view to future implementation of ISO 9001.</p>	<p>1.1-1.1.2 Action plan prepared</p> <p>Start implementing action plan.</p> <p>1.3 Action plan in place with a view to medium-term implementation of this standard</p>	<p>1.1-1.2 Action plan prepared and work on track with action plan.</p> <p>1.3 Action plan prepared.</p>
MAN2	<p>Define, in consultation of the Commission, and approve Service Level Agreements (one for each IT system, one for the the communication</p>	<p>Management Board to approve detailed indicators by end Q1 2013</p>	<p>Timeliness and quality.</p> <p>The indicators must respect at least the same level of service in place for each deliverable, prior to take-over by the Agency</p>

	<p>infrastructure and one for security), laying down the level of service that the Agency will guarantee to the users of the systems (Member States). These will contain detailed performance indicators.</p> <p>These agreements will guarantee a service level across the board equivalent to or surpassing the arrangements in place with other operators prior to take-over of these tasks by the Agency²⁵.</p>		
MAN3	<p>Ensure that an adequate management structure is put in place to allow the Agency to fulfil security requirements.</p>	<p>3.1 Put in place a specific security unit.</p> <p>3.2 Ensure that any significant security issues are escalated to higher levels.</p> <p>3.3 Management Board to ensure timely adoption of key security deliverables required by the legal bases</p> <p>3.4 Management Board to ensure adequate follow-up to audit recommendations and EDPS reports and/or audits.</p>	<p>3.1 Security unit put in place</p> <p>3.2 Procedures communicated to all staff</p> <p>3.3 All deliverables required by legal bases adopted. Timeliness of adoption.</p> <p>3.4 Action plans put in place for all recommendations.</p>

Application Management and Maintenance

	Objective	Outputs & performance indicator	
		Output	Performance indicator
AM1	Operational management of SIS II,	<p>1.1 All necessary tasks to ensure 24/7 functioning of the Central SIS II in accordance with the legal bases for this system. In particular the maintenance & technical developments</p>	<p>1.1-1.2 Specific indicators will be contained in the service level agreements developed under objective MAN2 above.</p> <p>1.3 Achievement of the milestones to be agreed with</p>

²⁵ With respect to VIS, EURODAC, the communication infrastructure and security, the Agency will have to maintain the level of service that was in force prior to its take-over of the systems. It will also guarantee an equivalent service level for SIS II.

		<p>necessary for the smooth running of the system and the monitoring of the technical performance of the system.</p> <p>1.2 The specific objectives and indicators in the SLA should also cover product management objectives (e.g. requirements managements system to capture stakeholder requirements, product roadmap with new versions and releases and ensuring stakeholder satisfaction with the functionality of the SIS II application).</p> <p>1.3 Supervise & monitor work under the contract for maintenance of SIS II after final system acceptance.</p>	<p>MS in the framework of the contract for maintenance of SIS II after final system acceptance.</p>
<p>AM2</p>	<p>Operational management of VIS</p>	<p>2.1 Operational Management</p> <p>All necessary tasks to ensure 24/7 functioning of the Central VIS in accordance with the legal bases for VIS. In particular the maintenance & technical developments necessary for the smooth running of the system. This will also include the the monitoring of the technical performance of the system.</p> <p>2.2 Maintain and keep up-to -date:</p> <ul style="list-style-type: none"> • The configuration management database • The Trouble Shooting Guide • The Knowledge Database • An exhaustive list of FAQs for users. <p>2.3</p> <ul style="list-style-type: none"> • Supervise & monitor maintenance work under the VIS MWO contract. 	<p>2.1-2.2 Specific indicators will be contained in the service level agreements developed under objective MAN2 above.</p> <p>2.3 Achievement of the milestones agreed with MS in the framework of the MWO contract and the extension.</p> <p>2.4 VISMAIL2</p> <p>Successful completion of testing on schedule</p>

		<ul style="list-style-type: none"> Take over responsibility for monitoring work under this contract to upgrade the VIS, <p>2.4 VISMAIL2</p> <ul style="list-style-type: none"> Complete the tests on schedule. <p><i>See Security heading for security deliverables related to this system</i></p>	
AM3	Operational management of EURODAC	<p>All necessary tasks to ensure 24/7 functioning of the Central EURODAC in accordance with the legal bases for this system. In particular the maintenance & technical developments necessary for the smooth running of the system.</p> <p>This will include work for monitoring technical performance of the system.</p>	<p>Specific indicators will be contained in the service level agreements developed under objective MAN2 above.</p> <p><i>See Security sector for security deliverables related to this system.</i></p>
AM4	New IT Systems Estimates and plans related to the possible future take-over of new systems, in particular, Entry Exit and RTP.	<p>Estimates of possible organisational, resource & financial implications of involvement by the Agency in future programming periods in preparation for the possible adoption of legal bases for these future systems (taking account of the financial fiches in the legal proposals).</p>	<p>Indicative plan addressing organisational and resources issues (financial and human resources) related to the possible take over of these systems.</p>

General Coordination

	Objective	Outputs & performance indicator	
		Output	Performance indicator
GC1	Technology watch	Put in place practical systems/teams, for technology watch in accordance with the governance models and methodologies put in place at organisational level and ensure that the results of technology	<ul style="list-style-type: none"> Organisation/Team in place and first concrete proposals/suggestions for technologies that could realistically be used to improve the Agency's operations the systems under its management.

		watch feeds into other Agency processes.	
GC2	Inter-agency cooperation	Prepare Action plan for cooperation with other Agencies, setting out possible themes of cooperation & channels for agreeing on concrete cooperation measures. Work will build on discussions held in 2012. The final goal will be to agree on a clear set of cooperation objectives/deliverables for each network & implement these.	1.1 Action plan drafted 1.2 Work stays on track with action plan
GC3	Put in place the necessary procedures and processes to ensure the highest level of data protection with regard to the Agency's administrative operations and with respect to the information systems under its management and to ensure their full implementation.	3.1. Put in place procedures 3.2. Spot checks on functioning	All necessary procedures in place Draft action plan addressing any weaknesses identified. No serious weaknesses identified in spot checks or in the framework of audits.
GC4	Legal advice: Establish a framework to provide legal advice where necessary for the internal operations of the Agency and to defend its position vis-à-vis the exterior (eg for legal matters related to tender procedures).	4.1. Establish framework and procedures 4.2. Legal advice provided in time for internal decision-making 4.3. Timely legal advice with regard to the Agency's position in any possible litigation	Timeliness and quality of advice
GC5	Internal communication: To promote the mission, values and culture of the Agency to its staff members through the drafting and dissemination of communication tools, internal awareness raising events and other best practices;	5.1. Tailored intranet site for Agency Staff 5.2. Informal internal awareness raising activities and events 5.3. Awareness raising about the priority of achieving technical & organisational excellence as cost-effectively as possible.	5.1 weekly updates 5.2 1 awareness raising activity per month 5.3 twice per year (via intranet and/or internal meetings).
GC6	External communication: To promote the Agency	6.1. Prepare a more detailed external communication strategy	• Timely finalization of strategy and information materials

	<p>and the systems that it operates and to fulfil the communications requirements laid down in the founding Regulation and the legal bases of the IT systems managed by the Agency</p>	<p>by the end of Q2</p> <p>6.2. Finalize planning & preparations with respect to the Agency's contribution to the SIS II information campaign & implement these tasks in time for the start of operations of SIS II (it is also possible that work may start on the planning of future campaigns)</p> <p>6.3. Communicating on the Agency's own initiative in fields within its tasks, including further development of and regular updates to the Agency's web site, and optimization of the site's visibility.</p> <p>6.4. Develop a network of media contacts, build sound relations with these contacts, provide media-friendly, information (clearly defined messages), assess the impact by monitoring & press reviews & organise media training for Agency staff</p> <p>6.5. Possible organisation or involvement in subsequent campaigns for VIS, should these be required</p> <p>6.6 Fulfilment of all publication requirements laid down in the legal bases, in particular:</p> <p>6.7 Publication of the Annual Work Programme for 2014 and the annual activity report for 2012</p> <p>6.8 Annual publication of lists of national authorities authorized to use or search data in the IT systems under its management (SIS II, VIS, EURODAC), as defined in the legal bases for these</p>	<ul style="list-style-type: none"> • Progressive increase in the number of hits on the Agency's web site throughout the year • Satisfaction of users and stakeholders (annual web site survey, survey after each campaign) • Quality and quantity of press coverage on major developments related to the Agency. • Timely fulfilment of publication requirements under the legal bases (annual report for the Agency, lists of national authorities and annual updates thereto and other reporting obligations)
--	--	---	---

		systems.	
GC7	General Training for Agency staff	<p>7.1 General Training</p> <ol style="list-style-type: none"> 1. Welcome pack training (2 sessions in 2013) 2. Administrative Welcome pack training (2 sessions in 2013) 3. Team building events and presentations: <ol style="list-style-type: none"> i) in-house team building seminars ii) lunch time/breakfast presentations with possible VC link between sites, iii) away day <p>Team building activities will take full account of budget constraints, with emphasis on low-budget in-house solutions.</p>	<p>90% of Agency staff attending at least 2 team building events in the year</p> <p>100% of staff in departments extending across both sites to attend at least 2 team building activities in the year.</p>
GC8	Technical Training for Agency Staff.	<p>Technical training for the Agency's own technical staff</p> <p>8.1 Agency IT Welcome Pack Training: 1 week course for new technical recruits with (aspects common to all of the systems).</p> <p>8.2 Specific technical upgrade training²⁶</p> <p>8.3 Business and operational training: training related to the business & operational functions of the specific system that staff will operate/manage²⁷</p>	<p>General:</p> <ul style="list-style-type: none"> - 100% of staff have attended the compulsory courses listed in their training plan. - Trainee satisfaction (=>At least 3 on a scale of 1 to 5)
GC9	Training for national authorities on IT systems managed by the Agency	At least 2 courses on each system in 2013	Trainee satisfaction (=>At least 3 on a scale of 1 to 5

²⁶ For example, on subjects such as Oracle, Weblogic and/or specific hardware), taking account of the specific tasks of personnel & their existing level of knowledge.

²⁷ For example, how visas are processed, the business environment for EURODAC and how to resolve incidents. For VIS and SISII, this training will be delivered based on the material delivered by the main development contractor during the VIS/BMS and SISII Transition plans (mainly operational procedures describing large-scale or daily operational scenarios).

GC10	Training for SIRENE operators	4 Courses in 2013 Precise activities will depend on the outcome of discussions with CEPOL	Trainee satisfaction (=>At least 3 on a scale of 1 to 5
GC 11	Training of Schengen evaluation team members and lead experts	1-2 courses in 2013 depending on requirements of experts Precise activities will depend on the outcome of discussions with FRONTEX and CEPOL	Trainee satisfaction (=>At least 3 on a scale of 1 to 5

Internal Audit

Goal / Obj N°	Objective	Outputs & performance indicator	
		Output	Performance indicator
IA1	To audit the internal control system put in place, in order to assess its effectiveness and, more generally the performance of the units in implementing the Agency's projects, actions and services, with a view to bringing about continuous improvement.	Set up the necessary organisation and define a three year audit plan	Organisation in place and audit plan ready for early Q4.

Operational matters and Infrastructure

Goal/ Obj N°	Objective	Outputs & performance indicator	
		Output	Performance indicator
OPU1	Systems management: (dealing with operating systems, upgrades, oracle and off the shelf products, etc)	1.1 Change management efficiency 1.2 Configuration management efficiency	Specific indicators will be contained in the service level agreements developed under objective MAN2 above.
OPU2	Network: 2.1 Supervise the network	2.1 Ensure adequate	2.1-2 Specific indicators will be contained in the service level

	<p>& coordinate relations between the Member States & the network provider for SIS II, VIS & EURODAC & ensure security of the communication infrastructure for VIS & EURODAC (<i>security of the communication infrastructure for SIS II remains under the Commission's responsibility</i>).</p> <p>2.2 Ensure that the measures & precautions applicable to any network tasks entrusted to external private sector bodies are fully respected.</p>	<p>availability of the sTESTA Network (as defined in the following network indicators for the network for SIS II, VIS and EURODAC)</p> <p>2.1.1 Site availability (availability of the TAP measured by the SLA monitoring device, between the TAP and a defined reference site (CU and BCU)).</p> <p>2.1.2 Throughput availability (to show the % of the bandwidth available compared with the target bandwidth)</p> <p>2.1.3 95 Percentile Network Round Trip Delay (between two sites compared to the target level 95-percentile round trip delay)</p> <p>2.1.4 95 Percentile Network Packet Loss ratio between two sites compared to the target 95-percentile packet loss ratio</p> <p>2.2 Validate the external contractors' operational procedures and their conformity with related provisions in the contracts</p> <p>2.3 Preparation and implementation of network migration for for VIS, SIS II and EURODAC in the areas of competence of the Agency (supervision, security and management of relations between the Member States and the new network provider).</p> <p><i>Additional indicators for this objective may be added to the final service level agreement.</i></p>	<p>agreements developed under objective MAN2 above.</p> <p>2.3 Timeliness of preparations</p>
OPU3	Helpdesk	3.1. Service desk team availability	Specific indicators will be contained in the service level

		3.2. Availability of issue tracking system (Service Level Management Tool) 3.3. Availability of service Catalogue (exhaustive list of all services to be rendered by the Agency to the Member States).	agreements developed under objective MAN2 above.
OPU 4	To monitor the technical functioning of the IT Systems under its management & gather all technical data needed to meet its reporting, statistics and monitoring obligations.	Statistics and information on the functioning of these systems as foreseen in the legal bases. Further information is given in point 4.4.7.	Quality and timeliness of deliverables

Resources and Administrative Matters

	Objective	Outputs & performance indicator	
		Output	Performance indicator
	Research, statistics and reporting		
AS1	Monitoring: 1. Finalize preparations for the monitoring procedures for SIS II 2. Monitoring for SIS II, VIS and EURODAC	1. Finalize procedures by March 2013 2. Implement monitoring	1. Quality and timeliness of procedures 2. Quality and timeliness of monitoring
AS2	Reporting: Adoption of the Annual Activity report for the Agency for 2012 and submission to the EP, the Council, the Commission and the Court of Auditors	15 June 2013	2. Quality and timeliness
AS3	Reporting Fulfilment of all reporting obligations laid down in the establishing Regulation and legal bases for the IT systems under the Agency's management such as : 1. Annual report on the activities of the Central	Draft reports referred to in the legal bases.	All reporting obligations fulfilled according to the defined deadlines or legal obligations.

	<p>Unit of EURODAC</p> <p>2. Report on the technical functioning including the security of VIS two years after it was brought into operation (& every 2 years thereafter) and submit it to the EP, the Council and the Commission</p> <p><i>A similar report will also be required for SIS II, 2 years after entry into operation.</i></p>		
AS4	<p>Information for the Commission, the Parliament, EDPS and the MS</p> <p>1. Provide the Commission with the information necessary to produce the regular evaluation of VIS, EURODAC and SIS II</p> <p>2. Inform the EP and Council of the measures to ensure the security of data use in the VIS²⁸ Once the Agency's own security plans are available.</p>	Provide adequate information as required	Submit reports/information on time
AS5	<p>Statistics</p> <p>1. Finalize the work to ensure that MS have implemented statistics gathering mechanisms, including common counting rules, in order to be able to fulfil reporting obligations from day one of SIS II operations & as from that time publish statistics related to SIS II pursuant to the SIS II basic instruments</p> <p>2. Provide statistics on the IT systems as laid down in the Establishment Regulation and legal bases for the IT systems under the Agency's management</p>	<p>5.1 Put in place effective statistics gathering and reporting procedures for SIS II by March 2013.</p> <p>5.2 Provision of all statistics</p> <ul style="list-style-type: none"> - Statistics on SIS II as from March 2013 - Statistics on VIS as from the beginning of 2013²² - Quarterly statistics, annual statistical compilations on the work of the Central Unit of EURODAC and any other statistics that may be required on EURODAC 	<p>5.1 Timeliness and conformity with legal obligations</p> <p>5.2 Timeliness and quality of statistics.</p>
AS6	Monitoring of research	1. Discussion of action	1-3. Timely implementation of

²⁸ In May 2010, the Commission adopted a Decision on a Security Plan for VIS, implementing the security provisions of the VIS basic instruments. This Decision entered into force when VIS went live and will remain in force until the Agency, which will have its own security plans, takes up its responsibilities.

	<p>1. Set up adequate structures to ensure effective monitoring of research</p> <p>2. Monitor the developments in research relevant for the operational management of SIS II, VIS, EURODAC and other large-scale IT systems.</p> <p>3. Keep the European Parliament, the Council, the Commission and the European Data Protection Supervisor informed on a regular basis of developments related to the monitoring of research.</p>	<p>plans for each sector (system) in the advisory groups in Q1 2013. These will also describe the appropriate media/frequency for reporting obligations under point 3 below.</p> <p>2. Regular monitoring of developments, Communication of information internally and to stakeholders by an appropriate medium.</p> <p>3. Report via the appropriate channels.</p>	<p>action plan.</p>
AS7	<p>Logistics and building management</p> <p>To provide services in the field of building management, facility management and logistics on all Agency sites;</p>	<p>1.1 Ongoing tasks related to infrastructure management of the temporary HQ premises in Tallinn.</p> <p>1.2 Ensure that the work to make available new HQ premises Tallinn remains on schedule</p> <p>1.3 Follow up re-conversion and construction work by the contractor to further upgrade the Strasbourg site</p> <p>1.4 ensure readiness of infrastructures related to SIS II.</p> <p>1.5 Ongoing tasks related to infrastructure management for the St Johann im Pongau site</p> <p>1.6 Uninterrupted routine operation of logistical services;</p>	<p>1.1, 1.5, 1.6: Annual survey. User satisfaction at least 75%.</p> <p>1.2 All works scheduled for 2013 completed on time</p> <p>1.3 Establishment by mid Q2 of a detailed work programme for the years 2014-2017 & work remains on track with this.</p> <p>1.4 Infrastructures for SIS II to be ready before March 2013</p> <p>1.5 & 1.6 (see 1.1)</p>
AS8	<p>HR: To develop the Agency's competency framework (recruitment needs, organisational needs, staff development needs).</p>	<p>Competency framework in place.</p>	<p>Recruitment, selection and staff development processes based on competency framework.</p>
AS9	<p>HR: To recruit and replace</p>	<p>Ensure that work to recruit</p>	<p>Posts filled within 16 weeks</p>

	staff in relation to the establishment plan and ED decisions;	the 120 members of staff is completed as soon as possible in 2013 Replacement of SNEs and Agency staff, according to requirements, timely placement of newly selected staff;	from publication.
AS10	Administrative support to the Management board	Organisation of at least 4 meetings (coordination of logistical arrangements, coordination of agenda and documentation & participation of ED in the meeting).	Quality and timeliness of deliverables (in particular, documents available in advance of meetings, according to the terms of the operational procedures)
AS11	Administrative support to the Advisory Groups	Agency to ensure secretariat.	Quality and timeliness of deliverables

Procurement and Contracts

Goal	Objective	Outputs & performance indicator	
		Output	Performance indicator
PC1	1.1-1.2 Further consolidate and re-enforce financial and procurement procedures, including ex ante controls. 1.3. To provide proficient advice on procurement procedures to other units of the Agency and to potential contractors and suppliers.	1.1 Consolidate procedures & inform relevant staff This includes putting in place structures for the preparation and implementation of tender procedures and for the possible consultation of Member State experts on a case-by-case basis for technical expertise. for evaluation procedures and the definition of technical aspects related to tender documents. 1.2 Coordination of all phases of the contracting procedure & provision of feedback on scope for improvement. 1.3 Provision of advice and in house training.	1.1 Increased number of trained staff. 1.2 increased number of procurement procedures completed in time 1.3 User satisfaction (via annual survey, result >=75%).
PC2	To process all invoices/ requests for reimbursements within the time limits set.	2.1 Timely payments 2.2 Periodical analysis of delays and analysis	2.1. Less than 15% of transactions not paid within the regulatory limits. 2.2 Analysis leads to concrete

		thereof	objectives for improvement
PC3	To maintain and further develop tailored financial information for Agency management.	3.1 monthly budget implementation reports 3.2 monthly overviews of payments	3. Timeliness of monthly reports and overviews and level of user satisfaction (annual survey. User satisfaction >=75%)
PC4	To contribute to the development, streamlining and implementation of the Agency's procurement policies, whilst ensuring full respect of EU legislation and guidelines.	Periodic internal reviews of procedures, taking account of input from users, ex ante and any changes in central procedures (at least once per year, with a view to proposing action plans for making improvements).	Carry out periodic review (before end of 2013) and implement changes in line & on schedule with action plan.
PC5	Fine tuning and validation of the Agency's accounting system, including local financial management systems	5.1 Agency Accounting system is devised and validated. 5.2 Introductions and modifications to the system are made after consultation of authorizing officers and validation by the Accounting officer.	Positive external validation
PC6	To keep and present the accounts in accordance with Title VII of the Financial Regulation	6.1. The accounts comply with the rules, are accurate and comprehensive and present a true and fair view of the Agency's' assets and liabilities, the financial situation and the outturn of the financial year; 6.2. The revenue ledger and general ledger system are maintained and contain updated data; 6.3. The management of the Agency is provided regularly with information on transactions they have entered and validated in the central accounting system ABAC/SAP); 6.4. The treasury management and assets register are regularly reconciled and in case of any discrepancies, relevant parties informed properly thereof; 6.5. Regular monitoring of the regularization of non	6.1-2 Accounts respect all provisions of the Financial Regulation 6.3. Timeliness of reports provided 6.3 & 6.6 Monthly meetings with authorizing officers 6.5. Decreased numbers of discrepancies 6.6 Monthly Meetings with

		<p>budget operations is ensured;</p> <p>6.6. Interface with authorizing officers on accounting matters;</p> <p>6.7. Implementing the accounting rules and methods and the chart of accounts in accordance with the provisions adopted by the European Commission's Accounting Officer;</p>	<p>authorizing officers</p> <p>6.7 No significant negative observations</p>
PC7	To implement all internal control standards within the organisation, to perform periodic reviews and to ensure that staff are informed of these standards and any related procedures.	<p>Put in place an action plan for implementing all standards within the Agency.</p> <p>Standards related to financial management should be implemented as early as possible.</p> <p>With regard to risk analysis, due to the nature of the IT systems under its management, the Agency is expected to rapidly surpass baseline standards in this area.</p> <p>2 reviews per year.</p> <p>Publish summary of standards on the intranet & refer to these in induction training for staff.</p>	<p>Number of fully implemented standards Target: 100% compliance.</p> <p>Should there be, due to exceptional circumstances, a small number of standards which are not fully implemented, clear action plans must be put in place to remedy the situation as soon as possible after the end of the year.</p>
PC8	To implement payments, collect revenue, follow-up to notes, VAT and recovery orders	Rigorous treasury policy implemented.	The funds on bank accounts correspond to the actual needs of the Agency
PC9	To demonstrate the ability to assume full financial independence.	Implementation of the essential elements of objectives 1-4 (1.1-1.3 2.1-2.2, 3.1-3.2, 5, 6, 7 & 8 in 2013.	<p>9.1 All financial staff recruited and 90% of these have received full financial training.</p> <p>9.2 Satisfactory coordination (including ex ante) procedures in place 1.1-1.2 above (quality of processing of test files controlled by COM)</p> <p>9.3 Outcome of an on-site check to ensure either satisfactory performance or ability to ensure satisfactory</p>

			performance for indicators PC1-8.
PC 10	Prepare a procurement plan	Prepare a procurement plan Q4 2012.	Quality and timeliness

Security

Obj N° & Goal (G)	Objective	Outputs & performance indicator	
		Output	Performance indicator
SE1	<p>Security</p> <p>To ensure that the Agency's offices operate in an adequate security environment, respecting the security plan for the Agency (and the disaster recovery plan, once it has been finalized). This will include measures to ensure that staff are fully aware of the basic security rules and procedures related to their activities and that Incidents and Irregularities are reported.</p>	<p>1.1 Advice / updates to other units of the Agency on security</p> <p>1.2 Training for staff on security</p> <p>1.3 Verify the functioning of the security procedures in practice and of the BCP plan once it has been approved.</p> <p>1.4 Put in place action plans to address any issues identified.</p>	<p>1.1 Quality & clarity of information</p> <p>1.2 All staff have participated in security training by the end of 2013</p> <p>1.3 No serious negative findings</p>
SE2.	<p>Ensure that confidentiality and professional secrecy requirements rules for staff working with data in the systems are respected</p>	<p>2.1 Information/training for staff</p> <p>2.2 occasional checks (at least once per year) + put in place action plans to remedy any issues identified.</p>	<p>2.2 No significant negative findings</p> <p>Other specific indicators may be added to the service level agreements developed under objective MAN2 above.</p>
SE3	<p>Complete work on the business continuity and disaster recovery plan for the Agency.</p>	<p>3.1 Finalize plan by March 2013</p>	<p>3.1 Timeliness of implementation</p>
SE4	<p>To ensure that all security aspects are taken into account in the planning and re-structuration of Agency premises</p>	<p>4.1 Check that premises are compliant with security standards.</p> <p>Put in place action plan for any issues identified.</p>	<p>4.1 User satisfaction</p> <p>No significant negative findings</p>
SE5	<p>Ensure that security measures & security plans for SIS II, VIS & EURODAC and for the communications</p>	<p>5.1 information, advice and training for staff on security</p> <p>5.2 Regular reports on compliance with detailed service level definition +</p>	<p>Specific indicators will be contained in the service level agreements developed under objective MAN2 above.</p>

	networks related to these systems are fully implemented.	Annual checks 5.3 Annual check of the functioning of the BCP and revise if necessary	
--	--	---	--

Annex A – Budget

The figures below are based on the Draft Budget for the Agency for 2013 that was prepared by the Commission in its care-taker role and adopted by the Management Board. The total amount of the EU subsidy to be provided to the Agency in 2013 has been adopted by the Commission. Subsequently, it is due to be approved by the Budgetary Authority at the end of 2012, as part of the EU General Budget for 2013.

Budget forecast – Draft Budget 2013

	Commitment appropriations (EUR)	Payment appropriations (EUR)
Title 1	14,962,000	14,787,000
Staff Expenditure		
11 Salaries & allowances	14,262,000	14,262,000
- of which establishment plan posts	13,851,000	13,851,000
- of which external personnel	411,000	411,000
12 Expenditure relating to Staff recruitment	0	0
13 Mission expenses	300,000	225,000
14 Socio-medical infrastructure	0	0
15 Training	400,000	300,000
16 External Services	0	0
17 Receptions and events	0	0
Title 2- Infrastructure and operating expenditure	15,138,000	9,920,000
20 Rental of buildings and associated costs	5,523,000	3,645,000
21 Information and communication technology	0	0
22 Movable property and associated costs	0	0
23 Current administrative expenditure	0	0
24 Postage / Telecommunications	0	0
25 Meeting expenses	715,000	850,000
26 Running costs in connection with operational activities	8,500,000	5,100,000
27 Information and publishing	300,000	225,000
28 studies	100,000	100,000
Title 3 - Operational expenditure	10,900,000	9,730,000
Operational cost (to be specified by chapter)	10,900,000	9,730,000
TOTAL EXPENDITURE	41,000,000	34,437,000

Source: Draft Statement of Estimates of the Revenue and Expenditure in 2013 of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

Annex B – Overview of critical risks and mitigating measures

The Agency has developed an organisational wide, corporate risk management process. This aims to aggregate risks (including the related responses) at organisational level and integrate this process into its annual planning and reporting, in conformity with Internal Control Standard (ICS) N° 6 of the Commission²⁹.

A risk is defined as an uncertain event or set of events that, should it materialize, would have a negative impact on the achievement of objectives set out in the annual Work Programme and the delivery of the medium-term goals of the Agency. The overview only shows critical risks.

A risk is considered as "critical" and reported in the Work Programme and Activity Report if it can:

- jeopardise the realisation of major objectives;
- cause serious damage to the Agency's partners (Commission, Member States, companies, citizens, etc.);
- result in critical intervention at political level (eg Council/Parliament) regarding the Agency's performance;
- result in the infringement of laws and regulations;
- result in material and/or financial loss;
- put the safety of the Agency's staff at risk; or
- in any way seriously damage the Agency's image and reputation ;
- even if not covered by the above categories, a risk should be also considered as critical if multiplication of its likelihood and impact indicators amounts to at least 20 (where risks are evaluated on a 1-5 scale with 5 denoting the highest - critical - level).

²⁹ See also specific objective PC7 in point 0

(1) Overview of critical risks (threats) which could impact on the 2013 Work Programme

Ref. n°	Risk description (cause, event and effect)	Objectives concerned	Response type ³⁰	Actions
01	Risk of a delay in making available the premises of the permanent headquarters in Tallinn, coupled with problems in prolonging the arrangements for staying in the temporary premises	AS7 (impacts on all objectives)	Reduce	<ul style="list-style-type: none"> • Close monitoring of the building contractor's work to ensure that the work to make available new HQ premises Tallinn remains on schedule • Take advantage of specialised advice from OIB (SLA) for advice on any issues that may emerge • Push for a legal solution for prolongation of the arrangements for the temporary premises, should this be required
02	Risk of a delay in making available the premises of the technical site in Strasbourg	AS7	Reduce	<ul style="list-style-type: none"> • Speed-up the process of extension of the existing temporary premises (bungalow) • Send an official letter to the French authorities to fix a clear deadline for the transfer of the existing building to the Commission. Follow this up closely to ensure that the deadline is met.
03	Risk of not securing the budgetary resources in 2013 that will be necessary for ensuring the availability of the 30 extra resources needed to manage the Crypto boxes as of 2014 when the contract with OBS is over.	OPU2 (2.2)	Reduce	<ul style="list-style-type: none"> • Carry out a study with a view to presenting strong argumentation for the need for these extra resources. • Increase requirements towards the new network contractor providing cryptographic equipment to deliver additional support and training to other staff.

³⁰ Threat risk type responses are: Reduce (take actions to minimise the probability or impact; the responsibility for the risk effect(s) and response measure(s) stay with the Agency); Remove (change the scope of the business objective concerned); Transfer (a third party takes responsibility for the risk); Accept (conscious and deliberate decision to accept the risk and, especially, the possible effect(s) on the business objective); Share (the responsibility for the risk effect(s) and risk response measure(s) are shared between the involved parties)

Ref. n°	Risk description (cause, event and effect)	Objectives concerned	Response type ³⁰	Actions
04	<p>Risk of not being able to achieve financial independence in 2013</p> <p><i>Strict conditions have been set for the transfer of financial responsibility to the Agency. These will not be compromised.</i></p> <p><i>Any delay in transferring this responsibility to the Agency will increase the complexity of implementing financial procedures, due to limitations on the resources available in the Commission. This could have wide ranging implications for all operational and logistical activities of the Agency.</i></p>	PC1-9 (impacts on most objectives)	Reduce	<ul style="list-style-type: none"> • Give priority to ensuring that a core number of experienced financial experts are amongst the first staff members to be recruited (see 1 above) • Ensure that this core group of financial staff are fully trained and in place as soon as possible to take care of essential financial procedures, including ex ante and provision of internal feedback. • Network with other Agencies to draw from their experiences and best practice in setting up their financial systems. • Seek advice from the Commission on critical matters • Consider the possibility of exceptional recruitment procedures for financial staff, should insufficient recruits be in place by early 2013
