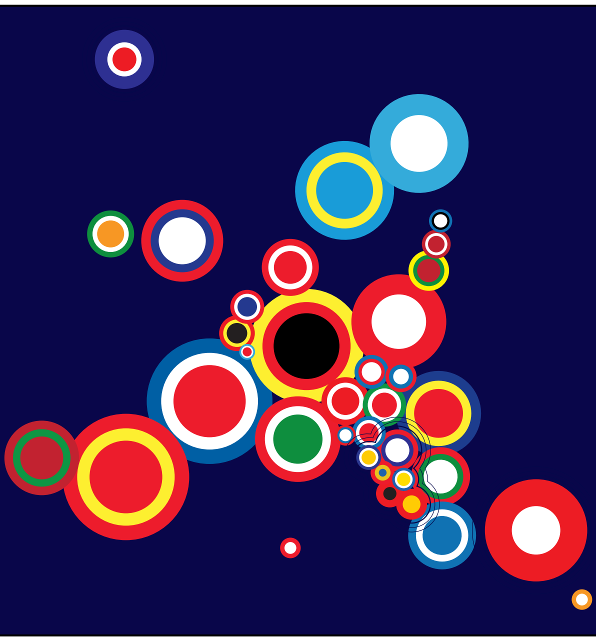
INSTRUMENT FOR PRE-ACCESSION ASSISTANCE (IPA II) 2014-2020

THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA

Implementation of business continuity and disaster recovery system – phase 2



Action Summary

The overall objective of the action is infrastructure development and procedures necessary for complying with criteria for accession to Schengen Area. The expected results are establishment of fully functional Business Continuity and Disaster recovery data centre which will enable business continuity of the ICT systems that support business functions of the Ministry of Interior, development of Disaster recovery process, policies and procedures and training of staff for usage and maintenance of the system.

Action Identification	
Programme Title	Annual Action programme for the former Yugoslav Republic of Macedonia for 2014
Action Title	Implementation of business continuity and disaster recovery system - phase 2
Action Reference	IPA/2014/037-701
Sector Information	
IPA II Sector(s)	**Rule of Law and Fundamental Rights - sub sector Home affairs**
DAC Sector	22040 Information and communication technology (ICT)
Budget	
Total cost (VAT excluded)[1]	EUR 7,000,000
EU contribution	EUR 5,950,000
Management and Implementation	
Method of implementation	Indirect management with the beneficiary country
Indirect management: **Responsible Unit or National Authority/Implementing Agency**	The Central Financing and Contracting Department (CFCD) will be the Contracting Authority and will be responsible for all administrative and procedural aspects of the tendering process, contracting matters and financial management including payment of action activities. The Head of CFCD will act as the Programme Authorising Officer (PAO) of the action. Ms. Radica Koceva (PAO) Central Financing and Contracting Department Ministry of Finance Tel: +389-2-3231 219 Fax: +389-2- 3106 612 e-mail: radica.koceva@finance.gov.mk
Implementation responsibilities	Ministry of Interior Mr. Sasko Kocev, Head of Section for IPA implementation and Senior Programme Officer) E-mail: sasko_kocev@moi.gov.mk
Location	
Zone benefiting from the action	The former Yugoslav Republic of Macedonia
Specific implementation area(s)	Nation-wide activities
Timeline	
Deadline for conclusion of the Financing Agreement	2015 (n+1)
Contracting deadline	d+3
End of operational implementation period	d+6

[1] The total action cost should be net of VAT and/or of other taxes. Should this not be the case, clearly indicate the amount of VAT and the reasons why it is considered eligible.

1. RATIONALE

The Ministry of Interior (MOI) together with other relevant authorities is in charge for managing the flow of persons and goods over state border including border control (border checks and border surveillance). The MOI has developed its own information system for border control. The system keeps data in accordance with the Law on border control related to persons to whom thorough check was performed (Article 64) as well as data with regards to the evidence about security and preventive measures taken against a foreigner in accordance with the Law on Foreigners (Article 143). In addition, the system is directly or indirectly connected to other information systems of the MOI which contain data kept in accordance with article 69 from the Law on police, related to persons for whom there are grounds for suspicion that they are perpetrators of criminal acts or misdemeanours, persons and objects being subject of a warrant, as well as persons to whom the entry to the country is prohibited, and data about registration of vehicles in accordance with the Law on vehicles (Article 73).

With the new requirements for EU accession and the introduction of the Schengen Border Code in mind, the main task of the Ministry of Interior is the gradual harmonisation of legislation, standards and practices for border guarding in compliance with EU requirements, and modernisation of the IT infrastructure and in the field of border management. Therefore the MOI will be the principal responsible authority for setting up the Schengen Information System (SIS), and this system will be built on the basis of information stored at the Information Centre of the MOI. Candidate countries have to be ready to integrate into the SIS when it will be possible. The MOI should develop the national information system so that integrity of data and their lawful use is ensured and the system would be ready to join SIS. Development and establishment of national centre of the SIS (N.SIS) is one of the necessary actions to be undertaken in order to fulfil the requirements of Schengen Acquis. In this regard the aforementioned information system for border control will become the bases for development of the future National Schengen information system. Getting ready for using the SIS presumes building-up of such a national structure that enables data input and direct and continuous access of authorised bodies to the data. It entails the establishment of the N.SIS, of the **S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntries *(*SIRENE) office, set-up the transmission network of the MOI for data input and using the data contained in the SIS. It also involves harmonisation of national databases with the Schengen standards and development of necessary software etc.

The MOI does not have a Disaster Recovery Data Centre for the aforementioned information system for border control which would enable back-up of data and the business continuity of the system. That means that in case of unavailability of the system or loss of data due to natural or man-made disaster there would be no continued operation of the system or its rapid recovery with possible catastrophic consequences to the overall functionality of MOI border control, business processes related to the fight against crime, exchange of intelligence data etc. Generally, it means that information system availability and reliability is crucial for all relevant processes in the Sector related to free movement of people, national border control, police authorities, etc. Therefore it is required to provide a backup data centre for complete disaster recovery purposes as well as to develop policies, plans and procedures to support recovery of the system such as developing the contingency planning policy statement, conducting the business impact analysis, identifying preventive controls, creation of contingency strategies, developing an information system contingency plan etc. In order to assess the current situation, a Framework contract for Preparation of Feasibility study for establishment of Business Continuity and Disaster recovery data centre was implemented (April 15, 2013 - October 14, 2013).

Based on the results of document analysis (building plans, network topology etc.) and the off-site visits, experts identified optimal scenarios and potential locations for the Disaster Recovery Data Centre taking into account first of all European Directives and European Norms and industry best practices and financial aspects (establishment of the data centre and the running costs in the long term). Summary of the Feasibility study is presented in Annex 2.

The process of the establishment of Business Continuity and Disaster recovery data centre as a complex process will be implemented in three phases.

The **first phase** would be implemented under IPA 2013 programme. The construction or refurbishment, depending of the available budget, of a building, including preparation of tender for works contract and supervision of works (framework contracts):

- All work related to the preparation of land for investment,
- All work related to adaptation or erection of the building for needs of DC,
- Power supply for the building,
- Cooling system[*]
- Full size server room,
- Security systems (Access Control (AC) Intrusion Detection System (IDS)
- Closed Circuit Television (CCTV) Security Management System (SMS))

The **second phase** (under this action) would include:

- Preparation of tender dossier for supply of equipment
- Purchasing and installation of the equipment
- Development of policies, plans and procedures
- Training of the end users

The **third phase** (under this action) would include:

- Perimeter security
- Additional RACK cabinets in the server room
- Additional InLine units for the needs of cooling of new RACK cabinets,
- Additional chiller to ensure redundancy n+1 in chillers

PROBLEM AND STAKEHOLDER ANALYSIS

The IT infrastructure in the MOI can be described as highly complex. Its complexity stems from following facts:

- There is no unified IT platform (Operating system/application server/database/storage) for Ministry of Interior IT systems, so IT infrastructure is heterogeneous and contains many different hardware and software platforms;
- There is a mix of in-house developed and third-party developed systems;
- There is divided responsibility for operations and maintenance of IT systems between three different sectors;
- Some of the operations and maintenance work on IT systems is conducted by third-parties (contractors).

With such complex IT infrastructure it is very difficult to establish and implement an efficient and sustainable disaster recovery strategy. There are also operations and disaster recovery-related risks that are a result of the above-mentioned facts.

The diversity of platforms that host different systems poses a big burden on the IT sector and creates additional overhead for employees involved in the support and maintenance of systems. Some of the platforms used in the MoI IT system are based on rather old technologies and despite the fact that vendors still provide full support for them and that there are no problems related to pure functioning of the systems, there are definitive drawbacks in using them – namely a lack of skilled, qualified

[*] Depending on the budget the cooling and security system might be purchased under second or third phase.

workforce, very difficult maintenance, lack of inter-connectivity options with newer technologies, and vendor lock-in.

Furthermore, besides the lack of specialised Disaster Recovery Data Centre, there is no developed Disaster recovery process, policies and procedures which would enable business continuity of the ICT systems that support business functions of the MOI. More precisely the current situation is as follows:

1. There is no information continuity plan in place, just procedure for incident handling;
2. Disaster recovery is not included;
3. There is no training on disaster recovery in place;
4. Critical information technology resources are not identified.

RELEVANCE WITH THE IPA II STRATEGY PAPER AND OTHER KEY REFERENCES

To accomplish the strategic goal of becoming a member of the EU, and in order to meet the obligations deriving from the Stabilisation and Association Agreement (SAA) and the Accession Partnership (AP), the MOI has to undertake a series of complex adjustments which should bring about a comprehensive and successive adoption of EU standards in all areas relevant for border management. The ultimate objective envisaged is full alignment with the Schengen acquis and its accurate implementation. The main documents and the core strategic framework of the MOI for its further alignment towards the Schengen acquis are the Schengen Action Plan, National Strategy on development of the established system for integrated border management and the derived Action Plan. The Action Plan determines the following strategic goals: upgrading the legal framework in line with the European standards, strengthening the capacities and enhancement of the inter-agency cooperation between the organizational structures, ministries and institutions competent in the system for insert full name (IBM), building and reconstruction of insert full name (BCP)s, upgrading the IT support and of the established systems and projects, development of the cross-border and international co-operation

The Strategic Plan of the MoI pins down the following key objectives: Prevention and detection of organized crime and corruption; Strengthening the trust of all communities in the Police, Completing the Police Reform process, Improving the public security and Improving the efficiency in the fight against terrorism and protection of the national security. Furthermore under the chapter "IT system upgrading", the Strategic plan envisages "**Implementation of business continuity and disaster recovery system".**

The Indicative Strategy Paper 2014-2020, under the Sector Rule of Law and Fundamental Rights, clearly indicates that the human and material capacity of the border police should be further strengthened in accordance with the Schengen *acquis*. It also underlines that improved surveillance and detection capacity of the border police regarding all forms of cross-border crime as well as setting up a base for the future Schengen information system" is needed.

With regards to the fight against organised crime, NPAA stipulates that: *On a medium term basis the strengthening of the law enforcement bodies is envisaged.*

SECTOR APPROACH ASSESSMENT

Although this is a stand-alone action, it is anticipated that during the preparation of the tender dossier for civil works (phase 1) involvement of other governmental institutions (Customs, Public prosecution office, Ministry of information society and administration etc) as users of the centre will be taken into consideration.

LESSONS LEARNED AND LINK TO PREVIOUS FINANCIAL ASSISTANCE

Although impact realised through the previous assistance overall is satisfactory, a number of challenges remain.

Project implementation is often hampered by either insufficient staff and resources allocated to (newly established) institutions or insufficient operational funds available in the government budget to allow for appropriate implementation of the mandate of the concerned department, or by late approval of relevant legislation etc.

Clear co-operation and communication will be established with the all involved stakeholder agencies. Experience / Lessons learnt from during previous projects indicate that specific attention should be given to this aspect.

Even though country accession to the Schengen area is at the moment a long term goal, experience from previous EU enlargements shows that some activities should start at a very early stage, notably the updated Catalogue of recommendations for the correct application of the Schengen acquis and best practices gives recommendations related to security such as:

- there should be a separate back-up system, with regular checks of the switch between the back-up and operational system;
- there must be emergency plans and escalation procedures to be used for remedying incidents that may potentially interrupt the operation of the system and make the Schengen IT systems fully or partly inaccessible;
- backup data must be subject to the required physical protection and kept in separate geographical locations;
- each Schengen State must establish and implement suitable emergency planning measures;
- the emergency plans have to be based on a risk assessment of the threats that may lead to inability to access the system and the impact of the threats on the other Schengen States.

Another important lesson learned during the implementation of the other projects to support the MoI is that it is essential that a strong technical assistance team prepares the supply tender dossier and assists the Ministry of Interior to follow-up on project implementation. The same could be said for the need to ensure project sustainability and budgetary funds for maintenance of the previously achieved results.

2. INTERVENTION LOGIC

LOGICAL FRAMEWORK MATRIX

OVERALL OBJECTIVE	**OBJECTIVELY VERIFIABLE INDICATORS (OVI)**	**SOURCES OF VERIFICATION**	
To establish a base for the future Schengen system.	The country has developed a base for the future Schengen system	EU Progress Report	
SPECIFIC OBJECTIVE	**OBJECTIVELY VERIFIABLE INDICATORS (OVI)**	**SOURCES OF VERIFICATION**	**ASSUMPTIONS**
To implement business continuity and disaster recovery system.	The business continuity and disaster recovery system is fully functional.	EU Progress Report Reports from the system testing	EU integration remains a country priority Political commitment
RESULTS	**OBJECTIVELY VERIFIABLE INDICATORS (OVI)**	**SOURCES OF VERIFICATION**	**ASSUMPTIONS**
1. Detailed report on the current situation and need assessment report related to the establishment of Business Continuity and Disaster recovery data centre, prepared **2.** ICT infrastructure of Business Continuity and Disaster recovery data centre including upgrade of existing ICT infrastructure of Primary Data Centre, implemented **3.** Disaster recovery process, policies and procedures prepared **4.** Trained personal of MoI	• The Business Continuity and Disaster recovery data centre is functional • Disaster recovery process, policies and procedures are tested and adopted • Number of employees trained	Monthly and quarterly reports Report on Provisiona acceptance signing Timetables for staff training, Official reports from the competent services Official report from the Human Resources Section within the Ministry of Interior and received certificates from the trainings	EU integration remains a country priority Professional and political commitment
ACTIVITIES	**MEANS**	**OVERALL COST**	**ASSUMPTIONS**
Activities to achieve Result 1: • Analysis of all relevant information related to the establishment of Business Continuity and Disaster recovery data centre • Preparation of need assessment report **Activities to achieve Result 2**	Two procurement procedures (supply and service)	7.000.000 EUR	1. National budget resources available; 2. Presence of qualified personnel;

• Preparation of the Tender dossier for supply of equipment and services • Procurement of the ICT infrastructure and services for primary and secondary locations • Installation and configuration of software and hardware for Business Continuity and Disaster recovery functions. **Activities to achieve Result 3:** • Developing the contingency planning policy statement. • Conducting the business impact analysis (BIA). • Identifying preventive controls. • Creation of contingency strategies. • Developing an information system contingency plan. • Ensuring plan testing, training, and exercises. • Ensuring plan maintenance. **Activities to achieve Result 4:** • Preparation of Curricula for the usage and maintenance of the system • Training the MoI personal for operation, use and maintenance of the ICT infrastructure for BC&DR.			3. Sufficient financing of the activities from the state budget

ADDITIONAL DESCRIPTION

The following components are envisaged:

Component 1: Survey, conceptual design and estimation of quantities
Component 2: Preparation of Technical Specifications and full Supply Tender Dossier
Component 3: Supply Tender launch and evaluation
Component 4: Implementation of the supply contract
Component 5: Monitoring and supervising of the installation process
Component 6: Preparation of policies, plans and procedures

The following activities are expected to be implemented:

- Conducting survey taking into consideration existing ITC infrastructure of the Beneficiary and third parties;
- Preparation of technical Specifications for the equipment and related installation services for the Business Continuity and Disaster recovery data centre for primary and secondary locations based upon the conceptual design (Conceptual project) including cost estimation for equipment quantities, associated installation and commissioning services, the terms for any guarantee and after-sales maintenance for the Operation, Administration & Maintenance (OAM) of the system;
- Preparation of Tender Dossier for supply contract for the Business Continuity and Disaster recovery data centre for primary and secondary locations including provision of technical support to the Contracting Authority throughout the clarification and evaluation phases of the tender as needed;
- Implementation of Supply contract;
- Provision of technical and procedural advice throughout the implementation (supervision of the installation process) of the supply contract, including stages of the detailed survey and design, delivery, installation and commissioning;
- Assisting the Contracting Authority with Provisional Acceptance procedures for the supply contract;
- Preparation of training needs assessment for training for system management and maintenance, and specific training for final users to be performed under the supply contract and conducting of trainings;
- Developing contingency planning policy statement. A formal policy provides the authority and guidance necessary to develop an effective contingency plan;
- Conducting the business impact analysis (BIA). The BIA helps identify and prioritize information systems and components critical to supporting the organization’s mission/business processes. A template for developing the BIA is provided to assist the user;
- Identifying preventive controls. Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs;
- Creation of contingency strategies. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption;
- Developing an information system contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system’s security impact level and recovery requirements;
- Ensuring plan testing, training, and exercises. Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness;
- Ensuring plan maintenance. The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.

Plans to be considered as applicable for MoI contingency planning are as follows:

1. Business Continuity Plan (BCP)
2. Continuity of Operations (COOP) Plan
3. Crisis Communications Plan
4. Critical Infrastructure Protection (CIP) Plan
5. Cyber Incident Response Plan
6. Disaster Recovery Plan (DRP)
7. Information System Contingency Plan (ISCP)

Assumptions:

- Professional and political commitment;
- National budget resources available;
- Presence of qualified personnel;
- Necessary time limits are respected pursuant to the EU legal regulative
- Continuous courses and trainings are provided for the personnel
- The system functions properly and is regularly maintained and used by the users

Preconditions:

- Appointment of counterpart personnel by the beneficiary before the launch of the tender process;
- Allocation of working space and facilities by the beneficiary for technical assistance before the launch of the tender process;
- Participation by the beneficiary in the tender process as per EU regulations;
- Organisation, selection and appointment of members of working groups, steering and coordination committees, seminars by the beneficiary as per work plan;
- Necessary legislation in force;
- Appointment and availability of the relevant staff of the beneficiaries to participate in implementing activities (especially training activities) as per the work plan;
- The beneficiary ensures appropriate and timely handling of all legal and regulatory arrangements necessary to enable implementation of the works and supplies (e.g. land and property ownership, building permits, import arrangements, etc.)

Risks:

- Better links between actions/projects belonging to the same sector should be ensured (at both design and implementation levels). External coordination with other international donors has to be also ensured;
- Communication between project management, contractor and beneficiaries: it is sometimes unsatisfactory and results in partners not having a clear understanding of the objectives/content of the project as well as the nature/level of the commitment expected from them;
- Absorption capacity is often over-estimated; partners are often unable or unwilling to provide the necessary human and material resources. The availability and permanence of adequate resources is an issue that should be addressed up-front before implementation of some action’s components.
- The above mentioned risks will be mitigated with appropriate measures and appropriate actions such as: establishing good communication channels between all involved stakeholders in the implementation of the action, risk assessment of the contracts to be undertaken prior to the start of implementation and corrective measures during individual projects implementation, regular meetings initiated by relevant stakeholder to be organised, regular monitoring to be conducted and, last but not the least, the MOI to establish an employment policy.

3. IMPLEMENTATION ARRANGEMENTS

The project will be implemented under Indirect Management mode. The Central Financing and Contracting Department (CFCD) will be the Contracting Authority and will be responsible for all administrative and procedural aspects of the tendering process, contracting matters and financial management including payment of project activities. The SPO in the Ministry of Interior will act according to the signed Operational Agreements.

ROLES AND RESPONSIBILITIES

The **Contracting Authority** is responsible for launching the tender, organising the evaluation, preparing and signing the contract and making the payments under the contract. The Contracting Authority will, after review and endorsement by the Steering Committee, formally approve reports (inception, quarterly, interim, final and provisional acceptance) submitted by the Consultant for contractual management purposes, and give guidance where appropriate.

The Contracting Authority is also responsible for the monitoring the implementation of the contract which shall be carried out by way of appropriate meetings, on-the-spot checks, assessment of reports and verification of financial documentation.

The **Beneficiary** will be represented by the Senior Programme Officer (SPO) within the MOI who will be responsible for monitoring the implementation of the action and a action Co-ordinator from the IT Department responsible for the technical implementation of the action. The Beneficiary will designate one or more representative(s) to be the permanent focus point for co-operation, including management of communications and resource allocation, and to monitor the action implementation. The Beneficiary will establish a **Working Group** comprising of representatives from the administrative, technical and operational branches of the MOI. This Working Group would function as a forum for consultation, exchange of ideas and formulation of questions/recommendations for consideration by the Steering Committee.

During the inception phase and for the purpose of this action, the Beneficiary will establish and chair a **Steering Committee**, which will include at least one representative of the main sub-Beneficiary services. The Contracting Authority, the EU Delegation and a representative of the Consultant’s Expert Team shall be invited to participate with Observer status.

Other bodies, agencies or institutions may be proposed by the Beneficiary as committee members. The final composition of the Steering Committee has to be agreed with the Contracting Authority.

The Consultant will serve as the Secretariat to the Steering Committee. The Steering Committee will have quarterly meetings to oversee the implementation of the planning and implementation process of the project as a whole. Extraordinary meetings shall take place whenever necessary in response to specific requirements.

IMPLEMENTATION METHOD(S) AND TYPE(S) OF FINANCING

The Action would be implemented with two procurement procedures (supply and service), with an overall amount of EUR 7 million, where the IPA amount is EUR 5,950,000.00 and the co-financing is EUR 1,050,000.

4. PERFORMANCE MEASUREMENT

METHODOLOGY FOR MONITORING (AND EVALUATION)

A Steering Committee will be established to oversee the implementation process of the action activities. The Steering Committee will be chaired by the MOI and will include at least one representative of the primarily involved beneficiary services. The Delegation of the European Union, and the Secretariat for European affairs shall be invited to participate with an observer status. The Steering Committee shall meet not less than once per every three months.

The core action team – consisting of the team leader and other expertise will be placed within the Ministry of Interior. The team leader will be responsible for the overall management, representation (co-ordination with the EU and other international bodies) as well as reporting. The co-ordination of activity development in the different components of the activity is significantly important. The team leader is responsible for an appropriate management of resources. During the inception phase of the action, a detailed deployment plan will be developed under the coordination of a Steering Committee, in which each co-operating national institution will be represented to ensure appropriate inclusion.

The role and main functions of the Steering Committee will be:

1. Assess the action progress and monitor all activities of the action, as agreed in the contract;
2. Assess the performance of the Consultant, review and endorse the Consultant's Inception Report and other Reports, and make recommendations as appropriate to the Contracting Authority which will formally approve these reports;
3. Jointly discuss any critical points or bottlenecks for further project implementation and propose and discuss remedial actions to be taken in order to tackle problems.

The contracting authority in coordination with the Senior Programme Officer will monitor the implementation of the action through the project reports, minutes from the Steering Committee meetings, quality check of the produced documents (Assessment report, Tender dossier etc.), on the spot visits, reports from the Provisional acceptance procedure, etc.

The overall implementation of the action in line with the sector will be monitored by the relevant Sector Monitoring Committees.

INDICATOR MEASUREMENT

Indicator	Description	Baseline (2010)	Last (year)	Milestone 2017	Target 2020	Source of information
CSP indicator(s) – if applicable	*n/a*					
Action output indicator 1	*The provisional acceptance for the installed equipment is signed on time in accordance with the agreed timeframe*	*The MOI does not have a Disaster Recovery Data Centre which would enable back-up of data and the business continuity of the system*	*0*	*0*	*100%*	*Project Report* *Progress Report*
Action output indicator 2	*100% of the processes defined in the procedures for Disaster recovery and buisunes continuity are functional at the secondary location.*	*There is no developed Disaster recovery process, policies and procedures which would enable business continuity of the ICT systems that support business functions of the MOI*		*80%*	*100%*	*Monitoring Report* *Project Report* *Progress Report*
Action output indicator 3	*Number of employees trained*	*There is no training neither trianed personal on disaster recovery in place*		*40%*	*60%*	*Monitoring Report* *Project Report* *Progress Report*

5. CROSS-CUTTING ISSUES

ENVIRONMENT AND CLIMATE CHANGE (AND IF RELEVANT DISASTER RESILIENCE)

The European Community has a longstanding commitment to address environmental concerns in its assistance programmes. The support to institutions will include a specific component to assist the beneficiary to implement an 'internal environment assessment' to identify areas where it could improve its internal performance vis-à-vis environmental aspects. Beneficiaries shall ensure that during the implementation shall take into consideration national and EU policies related to environmental management and they would be included in all materials/project outputs that may occur.

ENGAGEMENT WITH CIVIL SOCIETY (AND IF RELEVANT OTHER NON-STATE STAKEHOLDERS)

n/a

EQUAL OPPORTUNITIES AND GENDER MAINSTREAMING

The MOI is committed to equal gender treatment throughout its human resource management. The present action however, is not expected to have an additional impact on gender treatment.

MINORITIES AND VULNERABLE GROUPS

The MOI is committed to an equal treatment of minorities throughout its human resource management. The present action however, is not expected to have an additional impact on the treatment of minorities and vulnerable groups.

6. SUSTAINABILITY

After the implementation period of the action MOI would continue maintaining the achieved results. Trained technical staff from the MOI would have the capacity to manage the IT and telecommunication system, to deal with any failure and to train end users. Every year the MOI budget foresees sufficient financial means for maintenance of the IT system and telecommunication network.

7. COMMUNICATION AND VISIBILITY

EU-funded projects should achieve a high and consistent level of visibility. A sufficient level of awareness can only be achieved through coherent branding of all EU projects. The role of contractors and implementing authorities in raising public awareness is thereby crucial. The Consultant shall comply with the provisions of the attached document 'Communications guidelines: visual and written identity for contractors and implementing partners', which is also set out at http://ec.europa.eu/europeaid/work/visibility/index_en.htm. The EU Delegation will use reasonable efforts to assist the Consultant in complying with this obligation, but without incurring expenditure by the EU Delegation. Therefore, the cost of visibility activities has to be included in the incidental budget.

The following indicative set of communication and visibility activities may be covered by the budget for incidental expenditure:

- Press releases on specific project activities
- Organisation of press conferences, when necessary
- All visibility items and activities must receive prior approval by the Contracting Authority
- The equipment delivered will be marked in compliance with the EU visibility manual .

LIST OF ANNEXES (to be shared between Beneficiary Countries and the EC/EU Delegation only)

Indicative list of documents to be annexed to the Action Document:

1. **Executive Summary of the Feasibility Study**

ANNEX 1 - EXECUTIVE SUMMARY OF THE FEASIBILITY STUDY

Bearing in mind security considerations (man-made hazards, natural disasters), applicable standards and industry best practices, the experts identified five possible scenarios for both data-centre establishment and hardware/software deployment, which results in the financial considerations ranging from 1 400 000 to 9 000 000 € for the Data-centre and 4 000 000 € for hardware, software and communication.

Scenarios S1 to S4 are recommended due to the fact that the proper construction of the building is addressed as well as perimeter security with the required stand-off distance. S1 and S4 are designed to handle both the Disaster Recovery activities and anti-terrorism protection. S1 and S4 have the same level of protection and security; however S1 is capable of handling 120 Standard RACKs (1000x800) and S4 handling 300 RACKs.

It is important to mention that none of the Scenarios is designed for protection against foreign military intervention with the use of the military grade rockets/bombs or ground forces however locations S1 and S4, if adequately staffed with armed personnel, are designed to withstand a high profi**le terrorist attack** or limited military intervention with the use of grenades or hand rocket propelled grenades. The Beneficiary may consider adding additional security measurements for perimeter protection including double anti-ram K12 gates for checkpoints or X-ray machines at the entries.

Scenario S2 provides basic protections in terms of anti-terrorism, however is susceptible to a more sophisticated terrorist attack due to the stand-off distance and lower grade walls with minimal distance between outer walls and Server Room (IT Chamber).

Scenarios S3 and S5 are not recommended however they can serve as a solution only if the Primary Datacenter location is tailored to meet Tier III standards and hardened to withstand terrorist attack.

Scenari o	Description	Location	Stage 1 Datacenter (Tier II, 60 RACKs*)	Stage 1 (hardware and software for primary and secondary locations)	Stage 2 Datacenter (Tier III and 120 RACKs*) + Perimeter Security	Total
S1	New building (Recommended Scenario)	Strumica	€ 5 100 000	€ 4 000 000	€ 1 900 000	€ 11 000 000
S2	Adaptation of a building	Kavadarci	€ 3 100 000	€ 4 000 000	€ 1 900 000	€ 9 000 000
S3	Minimalistic adaptation	Kavadarci	€ 2 000 000	€ 4 000 000	€ 900 000	€ 6 900 000
S4	New building To serve as DRDC (300 RACKs) for the Government of the former Yugoslav Republic of Macedonia	Strumica	€ 9 000 000 (300 RACKs, Tier III)	€ 4 000 000		€ 13 000 000
S5	Very risky	Kavadarci	€ 1 400 000	€ 4 000 000	NO TIER III capabilities	€ 5 400 000

*) Number of RACKs for S2, S3, S5 refer to Standard RACKs (1000x800) S1 and S4 refer to Standard RACKs (1000x600)

Scenario	Protection against natural disasters	Protection against man-made disasters		
	Earthquakes, fires, flooding	Low profile terrorist-attack	High-profile terrorist attack	Foreign military intervention
S1	YES	YES	YES	NO
S2	YES	YES	NO	NO
S3	YES	NO	NO	NO
S4	YES	YES	YES	NO
S5	NO	NO	NO	NO

1.1. Scenario S1 (recommended, optimal)

1. The new building of medium protection level and 600 square meters is erected in Strumica or any other location with available stand-off distance from the anti-ram fence to the outline of the building 100 meters or more and no hills or high rise building in the nearby vicinity
2. Building Management System with Access Control System, Intrusion Detection System and CCTV is installed
3. K12 fence with anti-ram gate and the fully equipped guards post is erected in Phase 2
4. Tier III datacenter facility of the capacity of max. 120 RACKS is established in the building
5. CBR threats not addressed

1.2. Scenario S2 (realistic)

5. The existing building in Kavadarci is adapted
6. Building Management System with Access Control System, Intrusion Detection System and CCTV is installed
7. K12 fence with anti-ram gate is erected in Phase 2
8. Tier III datacenter facility with proper Server Room (IT Chamber) of the capacity of max. 120 RACKS is established in the building, without Power Quality Systems
9. Phase 1 will cover one track for power (1xGen/UPS) and one track for HVAC
10. CBR threats not addressed

1.3. Scenario S3 (minimalistic)

1. Server Room (IT Chamber), single UPS/Generator and minimal necessary electrical equipment and single HVAC system is installed for 60 RACKS maximum
2. No adaptations to the existing building except necessary works for installation of the Server Room (IT Chamber), cabling etc.
3. CBR threats not addressed

1.4. Scenario S4 (to serve as disaster recovery and business continuity solution for the Government of the former Yugoslav Republic of Macedonia)

1. The new building of medium protection level is erected in Strumica or any other location (for example Prilep) with available stand-off distance from the antiram fence to the outline of the building 100 meters or more and no hills or high rise building in the nearby vicinity
2. Building Management System with Access Control System, Intrusion Detection System and CCTV is installed
3. K12 fence with single antiram gate and the fully equipped guards post (single) is erected in Phase 1
4. Tier III datacenter facility of the capacity of max. 300 RACKS is established in the building
5. CBR threats not addressed

1.5. Scenario S5 (risky)

- Single UPS/Generator and necessary electrical equipment (ELC 1, 2, 3, 5, 7) and single HVAC (HVC-1) system is installed for 60 RACKS maximum
- No Server Room (IT Chamber) installed, only concrete walls and ceiling is provided
- Basic adaptations of the building