Standard Summary Project Fiche for the Transition Facility

1. BASIC INFORMATION

1.1 CRIS Number: 2004/16762.07.05.
Twinning: MT04-IB-OT-07

1.2 Title: Capacity Building Program in Information Security

1.3 Sector: Administrative capacity

1.4 Location: Malta

2. OBJECTIVES

2.1 Overall Objective (s)

To fully and effectively implement EU requirements relating to Information Security in the Public Service of the Government of Malta.

2.2 Project Purpose

To enable Malta Government and Public Service to communicate effectively with the EU and its member states, to enhance security capability in the public service in Malta, and to empower members of the Maltese public service to contribute effectively in matters of security.

2.3 Justification

The project will address Information Security across the Government of Malta and in particular in the Ministries of Justice and Home Affairs, Foreign Affairs and the Office of the Prime Minister. The project will bear upon the capability of the Government in information security in these Ministries and in the Departments within their portfolios.

The adoption of Council Decisions and the implementation of measures arising from these decisions are an integral and necessary portion of the EU accession process.


This request is being submitted for such development of information security skills in CIMU and across the public service and to put in place the tools required, ensuring adherence to the EU security regulations.

The Information Security expertise being sought includes and goes beyond the NPAA requirement of developing Information Systems skills and skills in managerial and organisational effectiveness: it encompasses all security aspects relating to all types of information - on paper, magnetic, optical etc which include risk management prioritisation of security expenditure and procedural measures across the public service.

3. DESCRIPTION
3.1 Background and Justification

The various Maltese Government ministries and entities need to communicate with the EU and the various member states in a manner conforming to the published EU security guidelines. In order for security policy in Malta to be aligned to that of the EU, CIMU in Malta and its Infosec Unit in particular need to communicate with the Brussels Infosec Department on a two-way basis and on a par as true partners. The same applies to the relationship of the Malta Infosec Department and the Infosec Units of other Member States. This project will increase understanding and facilitate implementation of the Council Decision 2001/264/EC and support Information Security measures in the Government of Malta and the public service.

To this end, the Government of Malta, through the CIMU needs to partner effectively with an appropriate Infosec from another Member State. This close initial relationship with a Member State Infosec and the Maltese Infosec will assist CIMU to build the appropriate capacity of its Infosec Unit and to facilitate relationship building with the Infosec teams of other Member States. This multilateral relationship building will be the right context for Malta to implement its Information Security Plans (see at http://www.cimu.gov.mt/).

Further the intention is to create an understanding in the public service of the need for information security and the EU regulations in this arena.

Malta is currently receiving documents only via an accession countries network which shall stop upon accession. Currently efforts are being made to introduce a set of security processes and procedures which will enable communication with the EU over the current established channels. Major effort will still be required thereafter to train all public service and ministerial personnel in EU security, to introduce as yet not practiced best-in-class security in the area of electronic communication at highest security risk levels.

This Skills Transfer program will help CIMU in its brief to enhance and implement ICT strategy, policy and standards drafting, and compliance and regulation activities in the Maltese Public Service. The partnering being requested is in Information Security in the wider sense, so that CIMU will be able to confidently satisfy the Information Security requirements of the EU and those arising from Maltese Legislation (see Annex IV) CIMU will also be enabled to contribute to the information security effort in the EU. Other organizations (SPECIFY) involved in Information systems shall be trained in the EU security requirements arising from the regulations mentioned.

Working with a partner organisation will allow local staff to adapt, tune and modify model documents supplied by the partner organisation to local needs in the light of local experience.

3.2 Linked activities

There were no previous Pre-Accession projects on information security related to information security in general and to 2001/64/EC in particular. However the Public Service has elaborated a strategy and initiated preliminary work to strengthen information security in the Ministries and Departments.

In terms of meeting the EC Security Regulations 2001/264/EC etc, CIMU since January 2003 has started an ambitious program of works.

Various CIMU policies, CIMU standards and CIMU directive documents are published or being prepared to achieve this aim. A security Strategic plan originally written in 2001 is being revised and shall be implemented in a phased manner. User awareness training shall be part of the general effort to increase security in the public service. Published documentation is available at http://www.cimu.gov.mt/.

The underlying concept for the Infosec Policy framework is MSA ISO/IEC 17799:2001, issued by the Malta Standards Authority based on internationally accepted norms. This framework policy needs to be refined and understood and translated to operational procedures and working processes for the requirements of EU security and information security in general to be met. Supporting Maltese legislation already exists (Annex V).
The scope of application of the Information Security Framework is the Maltese Public Service and the target population of the CIMU policies, standards and directives on Information Security (not to be confused with EU Directives) will be all public officers involved with ICT (ICT is the term used in Malta to describe Information and Communication Technology.) service provider agents, third parties and outsourcing organisations on contract to the public service.

An Information Security Framework (ISF) that is based on International and local standards and legislation has been adopted and implementation of a program of work is in progress to achieve this aim. This ISF for the Public Service contains the following domains, which in turn meet the requirements set in the previously referred to EC regulations:

- Security organisation.
- Asset classification and control.
- Personnel security.
- Physical and environment security.
- Communication and operations management.
- Access control.
- Systems development and maintenance.
- Business continuity management.
- Compliance.

The implementation strategy is a major initiative. It is therefore divided in two major phases, namely:

- Corporate (Horizontal) implementation.
- Specific (Vertical) implementation.

The concept has been designed to close three successive, incremental objectives in information security that the Government of Malta has set for itself, namely:

(i) A Minimum Level of security
(ii) An Adequate Level of security
(iii) A Full Compliance Level

The aim of the Corporate (Horizontal) implementation phase is to introduce a minimum level of Information Security across the whole Public Service and its Agents. This addresses matters of policy, user awareness and security matters common to all areas, such as security organisation.

The aim of the Specific (Vertical) implementation phase is to bring specific groups, Public Service entities and the Agent to a level of Information Security commensurate with their requirements.

With the complex requirements of a public service, the implementation phase is expected to carry over well after accession date. The project shall require heavy resource commitment at CIMU and departmental level in order to ensure that EU security regulations are observed and state of the art security is achieved.
A need is thus perceived for partnership with a member state with experience in introducing and rolling out such programs in public service to satisfy 2001/264/EC and MSA/ISO/IEC17799:part1 (2000) criteria. This project shall address the need for skill transfer and experienced assistance.

3.3 Results:

1. Trained information security officials in all public service ministries, agencies and entities. About 100 officials across public service shall be intensively trained in issues related to information security.

2. Security-aware service providers to the public service in Malta. Such service providers are expected to be several, foremost the agency for IT services to the public service but also as public sector in-house ITC service teams and private sector entities providing services on contract and being used by the Government.

3. The generation of an EU-security compliant national set of public service policy, standard and directive documentation

4. Success in security compliance audits

5. Security operational processes which enable meeting and maintaining a high degree of conformity to the EU requirements

6. Operational routine security tasks (risk assessment, vulnerability assessment, intrusion detection, audit analysis)

3.4 Activities

3.4.1 Institution Building Component: Twinning for 24 months

CIMU is requesting the help of a partner Security group (security office/saa/nsa/infosec) from a Member State. This project will be implemented through a full Twinning with an EU Member State for a period of 24 months. An established and mature Infosec from a Member State will partner with CIMU in a significant skills transfer program. This project is expected to deliver the following:

3.4.1.1- A Resident Twinning Advisor to work closely with and advise CIMU on issues pertaining to the strengthening of administrative capacity in the area of information security, gauge the situation, brief trainers and ensure that content of courses and method of instruction are well tuned to the requirements and the situation pertaining. A provision of EUR 300,000 is being made to cover the costs of the Resident Twinning Advisor.

3.4.1.2- Study visits (see activities below) by key public service officials (up to 10 persons) to the partner organisation for a max of 10 working days per visit.

3.4.1.3 - Missions by a pool of short-term experts to Malta to facilitate the activities below. The average duration of each activity will be 15 man-days. Training will be delivered to about 100 officials starting from key ministries which are perceived to require the highest security but rolling out across and down.

The above activities will deliver the following:

- Planning exercise to map out the areas of activity
• Awareness / study visit for high level public service officials of selected ministries and CIMU to the corresponding Ministries of the designated Partner; the visit is to focus on information security arrangements in the core of the designated Partnering Government.

• Overview presentation of information Security Technology and Processes of the designated Partner.

• Overview presentation of Software Security Technology of the designated Partner. (applications, web applications, e-government services)

• To draw up and supply extensive annotated bibliography of information security resources

• To draw up a comprehensive list of high quality Information Security training resources

• To refine risk management and system accreditation methodology to local needs.

• To exercise the adapted risk management methodology on selected areas of the Public Service, e.g. in relation to a secure communication channel.

• Assist in information security audits of key ICT government areas.

• Missions by partner organisation experts to their Maltese counterparts for information exchange locally and understanding of local constraints to implementation of methods to comply with EU security regulations

• Study visits by Maltese key personnel at partner organisation for awareness training in the various areas of security.

• Study visits by local staff at the partner organizations of one or many member states to familiarize local personnel with the use of documentary and legislative publications which comply with EU security regulations

• Training and familiarization of local staff in the partner organization’s home country and area of secure operations in practice e.g.:
  - User awareness training
  - In the public service, the public sector as private sector.¹
  - Methods and Materials discussions on topics such as
  - Standard system configuration
  - Control mechanisms and auditing processes
  - Compliance management and auditing
  - Interfacing with law enforcement of all kinds
  - Legislative aspects

• Expertise exchange between local Infosec, as well as of operational teams of the local service agency for the Maltese Government, in the implementation of secure processes and tools for intergovernment as well as law enforcement and regulatory agency use

• Missions to train local public service personnel involved in security-sensitive selection of methods and products which meet EU and international (e.g. Common Criteria ISO/IEC 15408 EAL levels) requirements for various classes of security

• To assist CIMU in establishing a study visit for CIMU and Agency personnel to various member states InfoSec authorities.

¹ Public sector consists of utilities such as water, power, telecomms, as well as “parastatal” organizations such as the national air carrier. They are not under the same legal standing as the public service.
• To organise on behalf of CIMU a study visit of appropriate duration and local experts to regulatory or special interest groups such as a National Association of Insurers, to a National Association of Electronic Engineers, to a National Computer Society, and to an academic centre active on Software Reliability research

• The Partner to carry out a full scale / in depth InfoSec presentation to the Ministries identified for Horizontal implementation.

• The Partner to assist CIMU and other Malta Government entities involved to prepare technical presentations and user guides on key EU InfoSec matters.

• Awareness training by partner organization staff to Maltese key personnel in CIMU, the ministries and government agencies CIMU at present has an envisaged complement of 30, 14 Ministries, Cabinet Office and potentially House of Representatives are the likely targets of the exercise.

• A cascading train-the-trainer exercise.

• Training in auditing security to operational and compliance management staff.

• Risk assessment of information assets
• Risk assessment methodologies
• Selection of the tools for asset risk assessment
• Selection of the tools for ensuring that assets are protected proportionately to their risk category

• Selection of tools for
  ▪ Risk assessment of assets
  ▪ Vulnerability analysis
  ▪ Audit analysis
  ▪ Intrusion detection

• Specific training and advice on prioritization of the project work involved in security remediation work and in building a national security architecture.

• Specific activity to integrate Maltese activity in Infosec with EU activities such as e-Europe, as well as the current successful initiatives in combating cybercrime and facilitating forensics across borders.

• Assist CIMU in public security awareness presentations and publications, policy definition and maintenance processes on aspects of security.

The Study visits by Maltese staff abroad shall alternate with visits by the experts to Malta.

Mission experts required:

- Process and procedure) in security accreditation of systems for various risk levels
- Risk assessment(s)
- Evaluation of cryptographic solutions and systems for e.g. EU or NATO use,
- A higher user awareness training for public service
- Deployment of special tools for automatic security monitoring of high risk systems (intrusion detection, vulnerability analysis, handling of alerts about system and software vulnerabilities).
- Secure internal network set-up for intra-government handling of EUCI and national classified information electronically (voice/fax/data/VTC)

This work package will also produce a Project History Document that will document Lessons Learnt and any shortfalls for action in subsequent Information Security projects of the Malta Infosec.
3.4.2 Investment Component

The Inspection Handbook used by the security office of the General Security Council of the EU as well as standards related to the provision of security such as ISO17799/BS7799 require the implementation of state of the art toolkits for the policing of the security of the communications and information systems under review.

The selection and configuration of such tools is intended to be the objective of the project, such tools not being “commercial off the shelf” products. The vulnerability scanning system (“server”) in question is often a special system designed to be able to run “attacks” in a stealthy manner without disrupting production, with special security requirements to its set-up and design.

The same applies to the intrusion detection systems, where specific hardware is usually used rather than a generic hardware with special software.

Encryption devices for secure communication with the systems and between different entities geographically separated are perceived to be required.

This component will comprise a supply tender for the **purchase of the tools** required for risk assessment of assets, vulnerability analysis, audit analysis and intrusion detection. The following procurement is foreseen:

<table>
<thead>
<tr>
<th>Item</th>
<th>Estimated Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licence for Vulnerability Scan toolkit</td>
<td>€16,000</td>
</tr>
<tr>
<td>Vulnerability scanner  server</td>
<td>€2,000</td>
</tr>
<tr>
<td>3 Network Intrusion systems with Software and database server back-up</td>
<td>€100,000</td>
</tr>
<tr>
<td>4 Encryption Devices</td>
<td>€77,000</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>€195,000</strong></td>
</tr>
</tbody>
</table>

The security toolkit aspect is mainly a set of software and hardware instruments to be used to audit and monitor the affected systems to ensure compliance to security regulations. An external needs assessment report will be attached to the fiche in due course. The owner of this equipment will be the Central Information Management Unit as proxy for the Maltese public service.

3.5 Lessons Learned

CIMU has to date received no EU or other assistance, for example of a bilateral nature, in the implementation and introduction of information security measures in practice. The recent history of Malta as well as the trusting and friendly nature of the Maltese in general requires a massive thrust which creates difficulty even for established member states with a history of such counterespionage information security measures. Malta and CIMU are being faced with needing to implement a large number of systems used by various Council and Commission bodies to enable secure handling of documentation which is classified. The information security processes and the user awareness at national level thus needs to be increased in order to ensure that no EU classified information is compromised by accident or due to malicious insider or outsider attack.

4. INSTITUTIONAL FRAMEWORK

Besides the general approach, it is envisaged that selected ministries shall be the focus of this program:

- **Office of the Prime Minister** responsible for, among others, the Public Service, Planning and Priorities Coordination, Department of Information, Central Information Management Unit, the Management Efficiency Unit, and the Armed Forces.
• **Ministry for Justice and Home Affairs** responsible for, among others, the Attorney General’s Office, the Courts of Justice, Local Government, the Police, Immigration, Airport Security, Prisons, Citizenship and Expatriate Affairs, Lands, Government Property and Estates, Notary to Government, Public Registry and Land Registry

• **Ministry for Foreign Affairs and Investment Promotion** responsible for relations with the European Union, Commonwealth and other bi- and multi-lateral relations with other countries (see section 3.3 above). This detail should be under Institutional Framework in Section 4.

The following is an introduction on the Central Information Management Unit and on the Information Security Department within CIMU, a division of the Office of the Prime minister within which the security function for Malta resides.

**Central Information Management Unit: Current Situation**

The CIMU is a unit based within the Office of the Prime Minister (OPM), reporting to the Permanent Secretary, OPM. Cimu currently employs 30 persons and the expected future full complement of staff is 35. The concept for the establishment of CIMU was espoused in the 1999 - 2001 Information Systems Strategic Plan (ISSP) for the Public Service, which Cabinet approved in November 1998. Subsequently, CIMU was established by Government in February 1999 to:

- Provide leadership and vision for ICT in the Public Service.
- Promulgate policies and standards on the use and application of ICT in the Public Service.
- Ensure compliance to such policies and standards as well as carry out value for money reviews on investment made in ICT to date.

CIMU today is organised into five Departments. These are:

- The Information Security.
- The ICT Governance.
- The Strategy and Planning.
- The Knowledge Management and Communications.
- The Compliance and Agent Management.

CIMU operates in close collaboration with the Maltese Government ‘in-house’ ICT Agency and also works through a number of supporting focused teams.

**Information Security Department**

As this section shall be the focal point of this Institutional capacity Building Program, it is described in some detail.

On January 13th, 2003, the Prime Minister designated CIMU as the Infosec Department for Malta. The Head of Infosec has taken on the assignment on 1st October.

The Infosec Department is assigned responsibility for:
Implementing the security requirements as established by EU Council and EU Commission directives and orders.

Ensuring that procured security products used for communication and information systems are certified against acknowledged criteria by an appropriate international evaluation or certified body.

Drawing up the requisite governance framework for ICT security within the Public Service.

Infosec education and training at various levels of personnel within the Infosec itself and within the Government Departments and for updating users on Infosec issues.

Liasing with the National Security Authority on matters relating to personnel vetting in relation to the EU document and information classification system.

The Infosec department will plan in the areas below; classifications and markings, classification management, physical security, general rules on the need-to-know principle, security clearance procedure for GSC officials and other servants, preparation, distribution, transmission, storage and destruction of EU classified material, top secret registries, security measures to be applied at the time of specific meetings held outside the Council premises and involving high sensitivity issues, incident management - breaches of security, data protection - of information handled in information technology and communication systems and release of EU classified information to third States or international organisations.

It is pertinent to note that the Head, Infosec chairs the Public Service ICT Security Team whose mission it is to:

Participate and shape the design of a security strategy for the Public Service.

Steer the implementation of the security strategy across the Public Service.

Review ICT security policies and standards prior to submission to OPM for approval.

Issue best practice, policies, standards to the Public Service.

Perform management reviews and audits of security framework within the Public Service.

Annex VII provides a brief of synthesis of the other departments constituting CIMU and key for it either chairs or participates in.

**ICT Governance Department**

The purpose of this department is to establish the CIMU policy, standards and directives framework within the Maltese public service.

In the determination of the ICT Governance framework it is believed that a resolution of core technological issues is required - whether these relate, for example to authentication and authorisation; PKI, etc. For this purpose, CIMU will undertake proof of concept studies and pilots prior to the submission of recommendations relating to new ICT policies, standards and technologies.

The Department is also responsible for the articulation of the ICT Architecture. Moreover, it is believed that in essence, data and its resulting transformation into information, constitutes the essential element of the ICT environment. Thus, the essence of this function is that of providing a focused and directed approach to establish a meta-data framework that will ensure the attainment of information sharing.

**Strategy and Planning Department**
This department is entrusted with the articulation of the macro ICT vision and strategy and also towards communication and dissemination of the strategic and governing ICT framework across the Public Service.

This function will continue to play the leading role, in conjunction with the Budget Office at the Ministry of Finance, with regards to formulating the recommendations to the Office of the Prime Minister and the Ministry of Finance respectively in relation to the annual ICT Ministry budgets.

A primary assignment is the articulation on an ICT Strategic Plan for the Public Service for the period 2003 - 2005.

**Knowledge Management and Communications Department**

This department was created in January 2003 to lead the introduction of KM in the Public Service. It is developing KM concepts in CIMU and the Public Service and formulating strategy for Enterprise Content Management and Electronic Records Management in the Public Service. It is also responsible for the management of two key corporate websites of the Public Service: the Government Portal (www.gov.mt) and the Corporate Intranet. Corporate data management is also within the Department’s mandate and for this reason the Department is the business owner of the Corporate Data Repository.

This department has also been entrusted with the national co-ordination of the European Union’s Interchange of Data between Administrations (IDA) program.

**Compliance and Agent Management Department**

Auditing and core operational activities to ensure conformance to published standards, policies and “CIMU Directives” in the target population of providers of services – the “agent” or third party service providers to the government.

**Supporting Focused Teams**

To achieve this continuous liaison between CIMU, the Agent and the Ministries, teams are set up which meet on a regular basis to provide feedback to the CIMU:

Information Management Officers Forum (IMO Forum) - Chaired by the Head of the Chief Information Management Officer.

Corporate Architecture Team (CAT) - Chaired by the Head of ICT Governance Department

Policies and Standards Team - Chaired by the Head of ICT Governance Unit.

ICT Security Team - chaired by the Chief Information Management Officer

Investment and Planning Team - Chaired by the Head of the Strategy and Planning Department.

### 5. DETAILED BUDGET (EUROS)

<table>
<thead>
<tr>
<th>Transition Facility Support</th>
<th>Investment Support</th>
<th>Institution Building</th>
<th>Total TF (=I+IB)</th>
<th>National Co-financing*</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twinning capacity building project</td>
<td>-</td>
<td>500,000</td>
<td>500,000</td>
<td>-</td>
<td>500,000</td>
</tr>
<tr>
<td>Equipment</td>
<td>146,500</td>
<td>-</td>
<td>146,500</td>
<td>48,500</td>
<td>195,000</td>
</tr>
<tr>
<td>Total</td>
<td>146,500</td>
<td>500,000</td>
<td>646,500</td>
<td>48,500</td>
<td>695,000</td>
</tr>
</tbody>
</table>
The amounts for co-financing indicated in the table correspond to cash co-financing. In addition, in-kind contributions from the Maltese administration for a good implementation of the Twinning may be developed in the covenant.

The cost of air tickets of Maltese officials participating in study visits will be paid for out of the Travel vote of the beneficiary.

The co-financing expenses will be monitored by the beneficiary and the National Authorising Office NAO. For the earmarked co-finance, a clear and verifiable set of costs will be provided. The beneficiary will define which budget lines are the source for co-finance.

The beneficiary together with the NAO commits to sound financial management and control.

For the Investment component, co-financing will be joint.
6. IMPLEMENTATION ARRANGEMENTS

6.1 Implementing Agency

Infosec Authority (within the Office of the Prime Minister)
Central Information Management Unit
Office of the Prime Minister
Gattard House
National Road
Blata l-Bajda

Contact Person:

Dr Albert Caruana
Head
Telephone: (+356) 2122 0634
Fax: (+356) 25992842
E-mail: albert.j.caruana@gov.mt

Project Leader:

Mario Mallia Milanes
Security Consultant
Telephone: (+356) 2122 0634
Fax: (+356) 25992842
E-mail: mario.mallia-milanes@gov.mt

Contracting Authority

Department of Contracts
Notre Dame Ravelin
Floriana CMR 02
Malta

Contact Person:

Mr Dennis Attard, Assistant Director
Tel: +356 21247682
Fax: +356 21247681
Email: dennis.attard@gov.mt

6.2 Twinning

A Twinning arrangement will be sought for the Institution Building component.

Twinning counterpart:

Mario Mallia Milanes
Security Consultant
Telephone: (+356) 2122 0634
Fax: (+356) 25992842
E-mail: mario.mallia-milanes@gov.mt
6.3 Non-Standard Aspects

N/A

6.4 Contracts

One twinning Covenant is envisaged for the implementation of the institution building component. The estimated value is €500,000
A supply tender is envisaged for the procurement of the security toolkit, estimated value €195000.

7. IMPLEMENTATION SCHEDULE

7.1 Start of Tendering / Call for Proposals  September 2004/July 2004
7.2 Start of Project activity  December 2004
7.3 Project Completion  December 2006

8. SUSTAINABILITY

The Government is committed to maintain the administrative function of CIMU once EU support has been withdrawn, and the financial resources required will be provided for in the annual budgetary estimates. The maintenance costs for the equipment purchased through this project will be borne on national funds. The Government will also provide sufficient resources in terms of staff as necessary to cover the functioning of the system to be set up through the project.

The project is dependent on the availability of the appropriate human resources, as well as on continuing financial support from the Office of the Prime Minister, that is forthcoming. Currently CIMU Infosec consists of one consultant and one Head with an administrative assistant shared with a larger team. The increased security effort will generate increased numbers of requests for consultation on security matters and an increase in the workload to process and answer reports of incidents, violations, and requests for new services to be accredited. Similar increase in load can be expected to affect the compliance and agent management team. Other teams in CIMU may also need to dedicate more resources e.g. to maintaining related policies and creating novel solutions to manage and present the output related to security. As the activities of CIMU increase, there will be a need for additional recruitment. This additional staff does not need to be in place for the project to commence.

9. CONDITIONALITY AND SEQUENCING

A further evaluation of the necessary budget (under the maximum budget foreseen in the fiche) of the investment component will be issued on the basis of the results of a feasibility study when they are available. The Equipment contract is conditional upon the results of this feasibility study.

I Logframe planning Matrix
II Detailed implementation chart
III Contracting and disbursement schedule by quarter for full duration of programme (including disbursement period)
IV Relevant Maltese legislation
V  List of equipment required
# ANNEX I

## LOGFRAME PLANNING MATRIX FOR Project

### Capacity Building Program in Information Security

<table>
<thead>
<tr>
<th>Overall objective</th>
<th>Objectively verifiable indicators</th>
<th>Sources of Verification</th>
</tr>
</thead>
</table>
| • To fully and effectively implement EU requirements relating to Information Security in the Public Service of the Government of Malta. | • adoption of 2001/264/EC across Public Service (see 2.1, 3.2, 4.0) as evidenced by ad hoc audit interviews of public service officials handling EUCI  
• security awareness and security operational procedures in all Ministries of the Government of Malta (see 5.0) as evidenced by CIMU compliance management audits  
• understanding of security tools as evidenced by reports generated from these tools – The team using these tools will need to reduce the output or have processes to detect and ignore false positives and prioritise other findings for action | • Maltese Policies to be drafted on Information Security  
• Operational security tools for risk assessment, vulnerability assessment, audit analysis and intrusion detection  
• Security compliance audits by Malta  
• Security Compliance audits by EU Infosec |

### Project purpose

To enable Malta Government and Public Service to communicate effectively with the EU and its member states, to enhance security capability in

<table>
<thead>
<tr>
<th>Objectively verifiable indicators</th>
<th>Sources of Verification</th>
<th>Assumptions</th>
</tr>
</thead>
</table>
| • missions by expatriate experts to Malta  
• extensive courses / training / | • deliverables by Maltese professionals – reports  
• reports by Mission experts | • timely adjudication  
• timely kick-off and progress |
the public service in Malta, and to empower members of the Maltese public service to contribute effectively in matters of security.

mentoring to Maltese professionals
- CIMU official auditing capability

• normal EU project monitoring, tracking and control
• introduction of information security auditing as a regular activity

• increasing opportunity to local staff to deploy knowledge/skills in Malta Government and EU related work.

<table>
<thead>
<tr>
<th>Results</th>
<th>Objectively verifiable indicators</th>
<th>Sources of Verification</th>
<th>Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Trained information security officials in all public service ministries, agencies and entities. About 100 officials across public service shall be intensively trained in issues related to information security.</td>
<td>setting up of a fully operational Infosec in Malta for matters of procedural and logical security, processes in place for risk assessment and classification as well as accreditation of sensitive systems</td>
<td>risk assessments of SCIS being carried out, SSRS generation, accreditation panels</td>
</tr>
<tr>
<td>2.</td>
<td>Security-aware service providers to the public service in Malta. Such service providers are expected to be several, foremost the agency for IT services to the public service but also as public sector in-house ITC service teams and private sector entities providing services on contract and being used by the Government.</td>
<td>contribution of CIMU to EU work, committees; projects, EU-NISA (European Network and Information Security Agency), etc</td>
<td>personnel availability</td>
</tr>
</tbody>
</table>
enable meeting and maintaining a high degree of conformity to the EU requirements

6. Operational routine security tasks (risk assessment, vulnerability assessment, intrusion detection, audit analysis)

<table>
<thead>
<tr>
<th>Activities</th>
<th>Means</th>
<th>Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. A Resident Twinning Advisor to work closely with and advise CIMU on issues pertaining to the strengthening of administrative capacity in the area of information security, gauge the situation, brief trainers and ensure that content of courses and method of instruction are well tuned to the requirements and the situation pertaining.</td>
<td>Twinning, Supply Tender</td>
<td>Contributions by Maltese professionals to EU security committees, Success in Project audits by EU</td>
</tr>
<tr>
<td>2. Study visits by key public service officials (up to 10 persons) to the partner organisation for a max of 10 working days per visit.</td>
<td></td>
<td>Purchase of needed security tools financed as part of this project (co-financed by CIMU)</td>
</tr>
<tr>
<td>3. Missions by a pool of short-term experts to Malta to facilitate the activities below. The average duration of each activity will be 15 man-days. Training will be delivered to about 100 officials starting from key ministries which are perceived to require the highest security but rolling out across and down.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Deployment of security toolkit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Title: STRENGTHENING MALTA’S CAPACITY IN THE ISSUANCE OF VISAS

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Components</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

D = Design
C = Contracting
I = Implementation
X = Closure
Title: Capacity Building Program in Information Security

<table>
<thead>
<tr>
<th></th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
</tr>
<tr>
<td>Contracted</td>
<td></td>
<td>500,000</td>
<td></td>
</tr>
<tr>
<td>Disbursed</td>
<td></td>
<td>375,000</td>
<td></td>
</tr>
</tbody>
</table>

All Figures in Euros
ANNEX IV - Relevant Maltese Legislation

There is legislation that is specific to ICT, to Data Protection as well as legislation in other areas but that is related to or may in some ways impact confidentiality, and/or integrity and/or availability of information.

Specific

Computer misuse provisions of the Criminal Code
Data Protection Act 2001
Electronic Commerce Act

General

Constitution of Malta
European Convention Act
Criminal Code
Code of Organisation and Civil Procedure
Data Protection Act
Electronic Commerce Act
Official Secrets Act
Professional Secrecy Act
Income Tax Management Act
Prevention of Money Laundering Act

Copyright Act
Press Act
National Archives Act
Malta Financial Services Centre Act
Malta Resources Authority Act
Malta Communications Authority Act
Security Communications Ordinance
Malta Standards Authority Act
Competition Act
Annex V – List of Equipment Required

(Rough Orders of Magnitude of most likely needed items)

<table>
<thead>
<tr>
<th>Item</th>
<th>Estimated Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licence for Vulnerability Scan toolkit</td>
<td>€16,000</td>
</tr>
<tr>
<td>Vulnerability scanning system (server)</td>
<td>€2,000</td>
</tr>
<tr>
<td>3 Network Intrusion Devices with Software and database server back-up</td>
<td>€100,000</td>
</tr>
<tr>
<td>4 Encryption Devices</td>
<td>€77,000</td>
</tr>
<tr>
<td>TOTAL</td>
<td>€195,000</td>
</tr>
</tbody>
</table>