CEDEFOP | European Centre for the Development of Vocational Training

Call for tenders (RFP)	**AO/RES/SAN/SECAUP/026/08**
Type:	Open Procedure
Subject:	**ICT SECURITY SERVICES**
Place of execution	Thessaloniki – Greece
Deadline for submission of offers:	**21/11/2008**
Deadline for obtaining tendering specifications (Infopack)	**07/11/2008**
Submit your offer:	In person at the offices of Cedefop or by postal mail or by courier
Offices:	Europe 123 Pylaia GR-570 01 – Thessaloniki
Postal address:	Cedefop P.O. Box 22427 GR-55 102 – Thessaloniki
To the Attention of:	Procurement Service
Information:	Name of responsible: Mr G. Paraskevaidis Fax : +(30) 2310 490 028 **E-mail:** C4T-services@cedefop.europa.eu

This Page has been intentionally left blank

Thessaloniki, 17/10/2008
RS/PRO/2008/1147

OPEN INVITATION TO TENDER

AO/RES/SAN/SECAUP/026/08

"ICT SECURITY SERVICES"

Dear Sir/Madam,

We thank you for the interest you have shown in this tender.

The purpose of this tender and additional information necessary to present a tender can be found in the attached Tendering Specifications. You should note however the following important points concerning the submission of a tender and its implications.

1. Tenders should be submitted preferably in English, but in any case in one (or in any) of the official languages of the European Union.

2. Tenders may be submitted exclusively in one of the following ways:

   (a) by post to be dispatched not later than 21/11/2008, in which case the evidence shall be constituted by the date of dispatch, the postmark or the date of the deposit slip, to the following address:

   European Centre for the Development of Vocational Training (Cedefop),
   Procurement Service
   Attention of Mr G. Paraskevaidis
   PO Box 22 427
   GR – 55102 Thessaloniki
   Greece

   Important:
   Tenderers shall inform Cedefop by e-mail (c4t-services@cedefop.europa.eu) or fax (+30 2310 490028)
   - ✓ ***that they have submitted an offer in time, and***
   - ✓ ***that they request Cedefop to confirm receipt of the e-mail or fax.***

   Do not attach your offer to the confirmation e-mail or fax.

   or

   (b1) by courier service to be dispatched not later than 21/11/2008, in which case the evidence shall be constituted by the date of dispatch, or the date of the deposit slip,

   or

   (b2) delivered by hand not later than 17h00 on 21/11/2008, in which case a receipt must be obtained as proof of submission, signed and dated by the official in the above mentioned Service who took delivery,

   to the following address:

European Centre for the Development of Vocational Training (Cedefop),
Procurement Service
Attention of Mr G. Paraskevaidis
Europe 123,
GR-57001 Thessaloniki-Pylea
Greece
Tel: +30 2310 490111 / 490 064

Please note that Cedefop is open from 09h00 to 17h00, Monday to Friday. It is closed on Saturday, Sunday and Cedefop holidays.

3. Tenders must be submitted strictly adhering to the following.

Tenders must be submitted in a sealed envelope itself enclosed within a second sealed envelope. If self-adhesive envelopes are used, they must be sealed with adhesive tape and the sender must sign across this tape.

The **outer envelope**, addressed simply to Cedefop (address depending on the means of submission, see point 2 above), should only bear additionally **the name and address** of the sender.

The **inner envelope**, addressed to the Procurement Service as indicated under point 2 above, must bear a self-adhesive label with the indication **"Open Invitation to tender – Not to be opened by the internal mail service"** and all the necessary information, as shown below:

OPEN INVITATION TO TENDER

CEDEFOP No: AO/RES/SAN/SECAUP/026/08

'ICT SECURITY SERVICES'

Name of tenderer:

NOT TO BE OPENED BY THE INTERNAL MAIL SERVICE

The inner envelope must also contain three sealed envelopes, namely, Envelope A – "Supporting Documents", Envelope B – "Technical Proposal" and Envelope C – "Financial Proposal". The content of each of these three envelopes is described in point 6 of the attached tendering specifications.

4. Tenderers must ensure that their tenders are signed by an authorised representative and that tenders are legible so that there can be no doubt as to words and figures.

5. Submission of a tender implies acceptance of all the terms and conditions set out in this invitation to tender, in the specifications and in the draft contract and, where appropriate, waiver of the tenderer's own general or specific terms and conditions. It is binding on the tenderer to whom the contract is awarded for the duration of the contract.

6. The opening of tenders will take place at Cedefop on 01.12.2008, 11h00 (local time). Each tenderer may be represented at the opening of tenders by one person. The name of the person attending the opening must be notified in writing by fax

(Fax No +30 2310 490 028) or by e-mail (C4T-services@cedefop.europa.eu) at least two working days prior to the opening session.

7. Contacts between the contracting authority (Cedefop) and tenderers are prohibited throughout the procedure save in exceptional circumstances and under the following conditions only:

   Before the final date for submission of tenders:

   - At the request of the tenderer, the Cedefop Procurement Service may provide additional information solely for the purpose of clarifying the tendering documents. Any request for additional information must be made in writing by fax (fax No +30 2310 490 028) or by e-mail (C4T-services@cedefop.europa.eu).

   Requests for additional information/clarification should be received by 13/11/2008. No such requests will be processed after that date.

   - The contracting authority may, on its own initiative, inform interested parties of any error, inaccuracy, omission or any other clerical error in the text of the call for tender.

   Any additional information, including that referred to above, will be published on Cedefop's website. Please ensure that you visit regularly the site for updates.

   After the opening of tenders:

   - If clarification is required or if obvious clerical errors in the tender need to be corrected, the contracting authority may contact the tenderer provided the terms of the tender are not modified as a result.

8. All costs incurred in preparing and submitting tenders are borne by the tenderers and cannot be reimbursed.

9. Up to the point of signature, the contracting authority may either abandon the procurement or cancel the award procedure, without the candidates or tenderers being entitled to claim any compensation. This decision must be substantiated and the tenderers notified.

10. This invitation to tender is in no way binding on Cedefop. Cedefop's contractual obligation commences only upon signature of the contract with the successful tenderer.

    Up to the point of signature, the contracting authority may either abandon the procurement or cancel the award procedure, without the candidates or tenderers being entitled to claim any compensation. This decision must be substantiated and the candidates or tenderers notified.

11. Tenderers are informed that for the purposes of safeguarding the financial interest of the Communities, their personal data may be transferred to internal audit services, to the European Court of Auditors, to the Financial Irregularities Panel and/or to the European Anti-Fraud Office (OLAF).

    Data of economic operators which are in one of the situations referred to in Articles 93, 94, 96(1)(b) and 96(2)(a) of the Financial Regulation may be included in a central database and communicated to the designated persons of the Commission, other institutions, agencies, authorities and bodies mentioned in Article 95(1) and (2) of the Financial Regulation. This refers as well to the persons with powers of representation, decision making or control over the said

economic operators. Any party entered into the database has the right to be informed of the data concerning it, upon request to Cedefop's Head of Finance and Procurement.

12. Evaluating your tender, and your possible subsequent replies to questions, in accordance with the specifications of the invitation to tender will involve the recording and processing of personal data (such as your name, address and CV). Such required personal data will be processed by Cedefop's Finance & Procurement Service solely for that purpose and pursuant to Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of data by the Community institutions and bodies and on the free movement of such data. You are entitled to obtain access to your personal data on request and to rectify any such data that is inaccurate or incomplete. If you have any queries concerning the processing of your personal data, you may address them to the Head of Finance & Procurement Service. You have the right of recourse at any time to the European Data Protection Supervisor for matters relating to the processing of your personal data.

13. All tenderers will be informed in writing of the results of this tender procedure.

Yours sincerely,

G. Paraskevaidis

Head of Finance and Procurement

Attached: Tendering Specifications

VADE MECUM

In responding to this open call for tender please make sure that you have:

– examined all the documents used for this call for tender and any other information available in writing for the purpose of responding;

– examined all further information relevant to the risks, contingencies, and other circumstances having an effect on your tender.

Specifically:

– Do not forget to SIGN your tender by a legally authorised person.

– Be on time with the submission.

– Be concise in your responses.

– Lay your information out so that it is easily accessible to the Evaluation Committee.

– Do not assume the Evaluation Committee knows your company.

– Answer the questions that have been asked and not the ones you would like to answer.

– Ensure your tender is a complying one on all aspects.

– Substantiate the company claims made in the tender. Be accurate in your statements.

– Demonstrate value for money in your tender.

– In drafting your financial offer read carefully §3.3.1 and §5.2, and Annex C**.**

Glossary of terms

The ***Centre*** or ***Cedefop*** is the European Centre for the Development of Vocational Education and Training.

The term ***Contractor*** means the successful **tenderer** with whom a future contract shall be, in principle, established.

Mandatory**:** failure to respond to a mandatory question may imply the rejection of the tender.

For a requirement, ***minimum*** and ***at least*** are synonymous.

Must**:** requirements prefixed with a *must* imply an absolute and mandatory obligation of conformance. Failure to observe this may result in exclusion.

Tender, ***offer***, ***proposal*** and ***bid*** are synonymous.

Tenderer means the entity that submits a tender (offer).

Warranty and ***guarantee*** are synonymous.

*'**Value for money**'* means achieving the best outcome for every Euro spent by assessing both the **costs** and **benefits** of each purchase rather than simply focussing the evaluation of offers on the lowest purchase price alone.

OPEN INVITATION TO TENDER

AO/RES/SAN/SECAUP/026/08

'ICT SECURITY SERVICES'

TENDERING SPECIFICATIONS

Table of contents

INTRODUCTION TO CEDEFOP

The European Centre for the Development of Vocational Training (Cedefop) is an agency of the European Union. Created in 1975 with a tripartite Governing Board, it provides services for the European Commission, the European Union Member States and the social partners as well as for the associated countries of Norway and Iceland. The candidate countries are also associated with its activities.

As the European Union's reference centre for vocational education and training, Cedefop provides policymakers, researchers and practitioners with information to promote a clearer understanding of developments and so enable them to take informed decisions on future action. Cedefop assists the European Commission in encouraging, at Community level, the promotion and development of vocational education and training.

The main tasks of Cedefop as defined in its founding Regulation are to:

- compile selected documentation and analysis of data;
- contribute to the development and coordination of research;
- exploit and disseminate useful information;
- encourage and support a concerted approach to vocational training development issues;
- provide a forum for a wide and diverse audience.

Cedefop's medium-term priorities for 2008-10 concentrate on the priorities set out in the Maastricht communiqué, which has been agreed by 32 countries, the European Commission and the European social partners:

a) 'promoting the image and attractiveness of the vocational route for employers and individuals to increase participation in VET;

b) achieving high levels of quality and innovation in VET systems to benefit all learners and make European VET globally competitive;

c) linking VET with the knowledge economy's requirements for a highly skilled workforce and especially, because of the strong impact of demographic change, the upgrading and competence development of older workers;

d) addressing the needs of the low-skilled (about 75 million people aged between 25 and 64 in the EU) and disadvantaged groups so as to achieve social cohesion and increase labour market participation.'

1. OVERVIEW OF THIS TENDER

1.1. Title and concise description of the contract

"ICT SECURITY SERVICES"

a) Services in the ICT Security field aiming at ensuring that Cedefop is permanently updated in this field and is protected as far as confidentiality, integrity and availability of data and information across its overall ICT infrastructure are concerned. Services will cover the whole spectrum of ICT security, namely: configuration, integration, availability, authentication, risk management, non-repudiation, access control, security classifications, security governance and incident management (See detailed set of required services under §2.4, 2.5, 2.6).

b) The type of contract is a Framework Service Contract.

Orders will be placed by means of Order Forms. Order Forms will be issued throughout the validity of the contract. Their number will depend on the needs and the budget situation of Cedefop.

1.2. Place of delivery or performance

The tasks will be completed both in the contractor's premises and in Cedefop's premises, 123 Europe str., Pylea, Thessaloniki.

1.3. Value of the contract

The total volume of the required services described in this call for tenders is not expected to exceed an upper limit of 270.000 Euro over a 4 year period. The sum of Order Forms to be issued during the period (see 1.1.b above) may not however reach that maximum amount; Cedefop will only be bound by the amounts effectively entered in the successive Order Forms.

1.4. Validity of tenders

Tenderers must maintain the validity of their tender for at least 6 months following the deadline of submission of tenders, i.e. until 21/05/2009.

1.5. Duration of the contract

The contract shall enter into force on the date of signature of the last contracting party, shall be valid for a period of one (1) year and may be automatically renewed up to three (3) times, each for an additional period of one (1) year, covering a total acquisition period of four (4) years (1+1+1+1). The Centre reserves the right to terminate the contract at any time by informing in writing the contractor 30 days in advance.

1.6. Main terms of financing and payment

Payments will be made within 30 days of submission of invoices and at the conditions set out in the draft contract.

2. SUBJECT MATTER OF THIS CALL FOR TENDER (TERMS OF REFERENCE)

2.1. Background Information

Cedefop has been constantly enquiring how to maintain a secure ICT environment through permanent monitoring, reviewing of systems, follow-up of technology.

In 2003, Cedefop conducted a review of its ICT systems resulting in an update of security processes and policies.

Given the new developments in Information Security, the existence of mature standards and proven practices, Cedefop decided to leverage its ICT infrastructure and information assets through the deployment of state-of-the-art practices in Information Security with prime goals to:

(1) enhance the reliability

(2) protect the confidentiality

(3) preserve the integrity and availability of information.

2.2. Aims and goals

Bearing in mind that:

i) Information Security is a demanding continuous process that involves people, procedures, time and costs;

ii) Security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, software and hardware functions,

the present call for tenders targets a multi-year provision of services that will help Cedefop attain the following goals:

- **Goal 1:** Update and broaden the existing organisational context for ICT security in Cedefop through the introduction of an information security management framework (ISMS) based on a business risk assessment, following recent developments and using proven practices and standards (e.g. ISO 27001/2). The policies relating to the ISMS shall concern all areas, departments, services, employees and subcontracted personnel with access to Cedefop information systems, as well as external partners.
- **Goal 2:** Establish a sound Information Security Management program optimising the balance between the value of the protected information and the effort & costs of implementing the necessary security controls. The ultimate goal is to leverage as much as necessary the compliance to the

ISO 27001/2 standards (without necessarily aiming at a full blown certification).

- **Goal 3:** Through a regular auditing, reviewing and controlling of systems and processes by independent professionals, maintain a state of maximum information security compliance to applicable standards, defined policies and controls.

- **Goal 4:** Through permanent monitoring and reviewing of the actual ICT infrastructure, identify vulnerabilities and ensure that ICT systems are reliable, security-enabled and intrusion-proof using updated security policies.

- **Goal 5:** Through the provision of permanently updated professional advice and assistance, introduce when required new security tools, methods and technology in an environment of changing business requirements and rapidly evolving security threads.

- **Goal 6:** Through continuous training of staff raise Information Security awareness and clarify responsibilities and conformance towards information security standards.

2.3. Wider objective

Through the above targeted goals, Cedefop's ultimate objective is to implement and maintain a dynamic, preventive, detective and reactive **Information Security** organisation encompassing processes, people, and ICT systems, which:

(1) protects Cedefop Information assets,

(2) corresponds to Cedefop's needs,

(3) supports its regulatory obligations,

(4) is based on appropriate standards, and

(5) reflects best practices.

2.4. Description of services required under this call for tenders

To attain the goals and objectives outlined in the previous sections, Cedefop expects to acquire expert services governed by a multi-year framework agreement allowing the Centre to proceed stepwise. Work shall be contracted in phases (per specific work orders) throughout the duration of the contract. Required services will cover consultancy and expertise in the following topics:

(1) Consultancy, advice and training regarding Information Security management, assessment and security governance

(2) Audit and Control Services (relating to policies, processes and systems)

(3) Security services on ICT Systems (including implementation of ICT security measures and security of IT applications).

2.5. Typical expected tasks and deliverables

2.5.1. The list below contains a non-exhaustive set of what the Centre considers as foreseeable examples of services. Subsets of these services will be the object of specific work orders that will be submitted to the contractor throughout the period of the framework agreement. The services the tenderers should be able to provide include:

2.5.2. Risk assessment and classification establishing Cedefop's information security needs and requirements while defining its scope and boundaries. The Contractor must identify, analyze and evaluate the risks. This will be done by assessing how security failures may impact Cedefop's business and by proposing options for their treatment. The methodological reference framework shall primarily be ISO/IEC 27001 & 27005 not excluding other formal methodologies for risk assessment (e.g. BSI or from the German Bundesamt für Sicherheit in der Informationstechnik).

2.5.3. Based on 2.4, proposal for an Information Security Policy underpinning the implementation of an Information Security Management System tailored to Cedefop's profile (following the **methodology** of ISO 27001/2) with the aim to: manage, operate, monitor, review, update, **maintain** and improve information security in Cedefop.

2.5.4. Initial and periodic audit and control services to monitor, review and assess the status of the Information Security organisation in order to ensure it remains updated and reliable (assess-protect-detect-react). Such audits and controls apply both on policies and processes as well as on ICT systems.

2.5.5. Continuous training and documentation services to all staff of Cedefop (ICT, management, general staff) in the form of seminars, information sessions, workshops, etc.

Documentation services: Policy papers, briefings, presentation, explanatory notes.

2.5.6. ICT systems' security services regarding the current ICT infrastructure i.e.: the ICT Network and communications infrastructure, the central systems, databases, application and web servers, the desktop environment and peripherals (including laptops and PDAs), the Information Systems and processes. Services shall include but will not be limited to: the analysis, diagnostics, reporting, implementation, mitigation and remedial action regarding protocols, certificates, processes, procedures, systems, devices, etc. covering areas such as:

(a) ICT systems' specific security Policy (including a.o.: general policies, access rights, password handling, virus protection, remote access, Intrusion avoidance and detection, Authentication management)

(b) Control mechanisms and procedures to be actively integrated to existing applications in order to address security gaps and improve systems security

(c) Internal auditing and reviewing of systems, risk analysis

(d) Troubleshooting, patching, hardening filtering

(e) Configuration, tuning, optimization

(f) Detection and vulnerability analysis

(g) Active security testing, internal and external penetration testing

(h) Application code reviews and compliance reviews

(i) Security incident investigations, forensics and troubleshooting, contingency management.

2.5.7. Advice regarding the introduction and use of security software(/hardware) tools and methodologies involved. Possibly assist in installation and configuration of related new tools.

2.5.8. Opportunity studies, and advice regarding the adoption of new technologies/solutions in the field of Information Security, risk management and associated business continuity issues, identity management.

2.6. Profiles Description

The tasks and services described above should be provided to the Centre by the establishment of order forms that will describe in detail each one of the services to be received from the contractor through the duration of the contract.

The contractor will provide these services by allocating to the specific tasks **person-days** using the following four (4) types of consultants:

2.6.1. Senior Security Expert and Project Manager

The Senior Security Expert and Project Manager shall be the person who will be in charge of the Project on the side of the contractor. This person should:

- have a University degree in Information systems, computer science or computer engineering or a relevant field
- have a professional experience of at least **5 years** in the field of ICT Security
- demonstrate through his CV a leading role in drafting security policy guidelines and expertise in best security practices both at a theoretical as well at hands-on level
- demonstrate through his CV a project management role in relevant projects of similar size and scope.

2.6.2. Junior Security Expert

The Junior Security Expert shall be the person who will report to the Senior Security Expert and provide him with assistance in this project. This person should:

- have a University degree in Information Systems, computer science or computer engineering or a relevant field **and** professional experience of at least **3 years** in the field of ICT Security
- demonstrate through his CV an important role in drafting security policy guidelines and expertise in best security practices both at a theoretical as well as hands-on level
- demonstrate through his CV knowledge of security techniques, tools, and methods in similar projects of similar size and scope.

2.6.3. Security Trainer

The Security Trainer shall be the person who will report to the Senior Security Expert and provide him with assistance in this project as regards relevant training needs. This person should:

– have at least **3 years** of training experience in the field; this experience should include training to technical as well as non-technical audience

– be able to propose the curriculum for the training session in co-operation with the ICT staff

– prepare the documentation, notes, hand outs, etc.

– demonstrate through his CV knowledge of security techniques, tools, and methods in similar projects of similar size and scope.

2.6.4. Technical Staff

The technical staff shall be the person who will report to the senior Security Expert and provide him with assistance in this project. This person should:

– have a degree in computer science (not necessarily a university degree) or computer engineering of a relevant field **and** professional experience of at least **2 years** in the field of ICT, **or** (if no formal qualification available) a professional experience of **5 years**

– demonstrate through his CV participation in ICT projects and having knowledge and experience of the platforms for drafting security policy guidelines as well as expertise in security best practices both at a theoretical as well as hands-on level

– demonstrate through his CV knowledge of security techniques, tools, and methods in similar projects of similar size and scope.

2.7. Specific conditions

2.7.1. Confidentiality

A tenderer who submits an offer must maintain confidentiality in respect of any document made available to him by Cedefop regarding any information to which he may have access as a result of the tender. Any document submitted by tenderers will become the property of Cedefop and will be considered confidential.

2.7.2. Non disclosure

Services to be undertaken through this contract will rely on and take into account:

(a) A non-disclosure confidentiality agreement between the contractor and the Centre

(b) Recent developments in ICT Security

(c) ISO 27001/2 standards

(d) Recent practices in Security Compliance Audits.

2.7.3. Specific Cedefop context

While undertaking this assignment, the successful tenderer is required to take into account organization-specific characteristics. **Documentation on the following topics** shall be provided to tenderers upon their request to the e-mail c4t-services@cedefop.europa.eu, indicating explicitly in the body of the message the request to receive the following documents:

(a) the already existing documentation, information, and policy at the Centre in this area,

(b) the existing infrastructure (may be found below),

(c) the ICT organigram,

(d) the related projects according to the priorities of the Centre.

2.7.4. Concise description of the ICT infrastructure at Cedefop

2.7.4.1. Position in the organisation: See the organisational chart on Cedefop's web site http://www.cedefop.europa.eu/index.asp?section=2&sub=2

2.7.4.2. Human Resources in the ICT

Cedefop's ICT department currently comprises of 10 experienced individuals, involved in project coordination, software, web and database development, technical administration and support (systems, network, security, firewall, web servers, Livelink, etc.)

All Cedefop's websites, services, information systems, applications, the Livelink document management system, servers, databases and technical equipment are hosted internally and being managed, supported and developed by the ICT department. Some development and support is outsourced; outsourcing is managed and controlled by the ICT department.

2.7.4.3. Network and telecom profile

(1) The internal network (LAN) is based on a switched Gigabit Ethernet backbone using Cisco technology and VLAN architecture. Current Internet bandwidth: 20 Mbps over the Gigabit backbone of *GRNET*. Backup Internet connection through wireless link with OTEnet (1 Mbps).

(2) Connection with the TESTA-II network of the European Commission (connects to the EC Intranet and other online services such as CIRCA). Connection via an encrypted VPN to Cedefop's Brussels office.

(3) Security: firewall / IDS (Checkpoint FW-1), e-mail security and anti-virus systems (F-secure).

(4) Siemens Hipath 4000 HDMS Telephone Center, with Siemens Xpressions unified messaging for voicemail and e-fax.

2.7.4.4. Systems

(1) The main operating system infrastructure is built on a Microsoft Windows 2003 Active Directory network controlled by 3 domain controllers (Single Forrest – Two sites, one in Thessaloniki and one in Brussels).

(2) The business critical services are supported by three pairs of clustered systems connected using Fibre Channel Switches to two SAN Subsystems (Compaq MA-8000 and Hewlett Packard EVA-4000), as follows:

(a) File and Print services are controlled by a two-node clustered system (active-passive) based on Windows 2003 Advanced Server (two Hewlett Packard Blades BL30 connected to the EVA-4000 Storage).

(b) Internal e-mail services are based on a two-node active-passive Windows 2003 Advanced Server – Exchange 2003 cluster (two Compaq DL380G2 connected to the MA-8000 Storage) and an external front-end Exchange Webmail server (OWA). Migration to Hewlett Packard Blade servers and the EVA-4000 storage is on-going.

(c) Document Management, Workgroup and Intranet Services based on the Opentext Livelink Software Platform are hosted in a two-node active-active Windows 2000 Advanced Server cluster (two Compaq DL380G3 connected to the MA-8000 Storage). Extranet access is supported via an external Livelink front-end. Migration to Hewlett Packard Blade servers and the EVA-4000 storage is on-going.

(3) Large scalable storage capacity with several hundreds of GB exists in a few tens of hard disks residing in the SAN. Backup is done with Brightstore Arcserve software, using one HP MSL6060 tape library with four SDLT drives, directly connected to the SANs.

(4) There are also several standalone File, Print, Web, database and document servers, running MS-Windows OSs (Windows 2000 and Windows NT) and some Linux servers (DNS, network and systems monitoring, logging, mailing lists, apache).

2.7.4.5. Email

(1) Internal Email services run on a clustered system based on Windows 2003 Advanced Server and Microsoft Exchange Server Enterprise 2003. This system is using the same SAN as the File and Print Services. Exchange's Outlook Web Access (OWA) is hosted on a dedicated server, on the DMZ.

(2) Front end Internet e-mail security gateway is hosted on two Compaq DL380G3 Windows 2000 servers, running Clearswift's MIMEsweeper, and screening from spam and virus threats.

2.7.4.6. Web infrastructure

(1) Web application environment and expertise: mainly Microsoft IIS flavours 3 (Intranet) and 4 (all the others), ASP technology, LDAP, SQL, Database access, XML, VBScript, Microsoft SQL Server, Sybase. In May 2008, it was decided to move to Microsoft .NET technology.

(2) Web log analysis, statistics and analytics is done with WebTrends Marketing Lab 2 (v8.5). The primary search engine for Cedefop's websites is the licensed Google Custom Search, Business Edition.

(3) The official Cedefop corporate informational web site (www.cedefop.europa.eu) is running on Windows 2000 and IIS 5.0.

(4) Cedefop's interactive large core business site (ETV - www.trainingvillage.gr), with 50,000 registered users, is based on ASP scripting, designed on the LDAP front-end of Microsoft's Site Server 3 with an SQL server 7.0 as a backend, maintained in-house, running on two Compaq DL350 servers.

(5) The Europass website (Europass CV, Language Passport, Mobility, Diploma/Certificate Supplement - http://europass.cedefop.europa.eu) is

based on JSP/Jakarta/Tomcat/Apache web technologies and MS-SQL DB Server and is running on two Compaq DL380 servers.

(6) The web based IS "OLIVE" (http://studyvisits.cedefop.europa.eu) is used for managing a decentralised network of study visits exchanges. It is running on Windows 2003 / IIS 6 / ASP / Sybase 15 on the "New-Idefix" server of Cedefop's Study Visits department.

(7) Cedefop's Library hosts a web site (libserver.cedefop.europa.eu) on an Apache server, running on the Aleph system and on the IBM AIX/RS6000.

(8) Extranet functionalities (http://extranet.cedefop.europa.eu) are implemented on Livelink (see below).

(9) A web proxy server ("squid") with 50GB cache is playing the role of a Web gateway to Cedefop's Brussels office computers.

(10) The "UniWeb" project (in-progress) aims to consolidate all web sites of Cedefop into a single portal using OpenText RedDot and Microsoft .NET.

2.7.4.7. Internal Database / Information Systems and Applications

(1) Cedefop's custom-made Financial, Budgetary, Accounting and Human Resources ERP system ("Fibus"), built on Power Builder 8 and Sybase ASE 12.5, is hosted on a dedicated Compaq ML530 running Windows 2000 OS.

(2) The Library system (Aleph v.14.2.9) of Cedefop is hosted on an IBM RS6000 server running AIX and Oracle 8.17.

(3) Opentext Livelink is being used as a Document Management, Groupware, Workflow and Intranet/Extranet Integrated Information System. Cedefop's Intranet is based on Livelink. A dedicated Livelink administrator is managing and developing the system.

(4) "Myfibus" is a web-based personalised employee information system based on Microsoft ASP.

(5) The plans of the Centre are to start using the ERP program of the European Commission (ABAC, i.e. SAP-adaptation) which should go into production in 2009-20010.

2.7.4.8. Desktop environment

The desktop environment includes approximately 160 PCs, running Windows XP Professional, Office 2003 and ca 30 printers and multifunction machines.

2.7.4.9. Audio-visual systems

Advanced videoconferencing infrastructure and know-how exists.

3. SPECIFIC INFORMATION CONCERNING PARTICIPATION TO THIS TENDER

Tenderers must meet the exclusion and selection criteria and have the legal position to allow them to participate in this tendering procedure.

3.1. Exclusion Criteria

Participation to this tender is only open to tenderers who are in a position to subscribe in full to the declaration on exclusion criteria and absence of conflict of interest in Annex A. Therefore all tenderers, all consortium members (if any) and all subcontractors (if any) shall provide the self-declaration found in Annex A duly signed and dated.

In case of recommendation for contract award the tenderer may be requested to provide the following documentation:

- as satisfactory evidence that the tenderer is not in one of the situations described in points a), b) or e) of the declaration, production of a recent extract from the judicial record or, failing that, a recent equivalent document issued by a judicial or administrative authority in the country of origin or provenance showing that those requirements are satisfied.

- as satisfactory evidence that the tenderer is not in the situation described in point d) of the declaration, a recent certificate issued by the competent authority of the State concerned. Where no such certificate is issued in the country concerned, it may be replaced by a sworn or, failing that, a solemn statement made by the interested party before a judicial or administrative authority, a notary or a qualified professional body in his country of origin or provenance.

Cedefop reserves the right to check the situations described in points c) and f) of the declaration.

3.2. Selection Criteria

The tenderer must submit evidence of their economic, financial, technical and professional capacity to perform the contract.

3.2.1. Economic and financial capacity of tenderers

The tenderer must be in a stable financial position and have the economic and financial capacity to perform the contract.

Proof of economic and financial capacity may in particular be furnished by **one or more** of the following documents:

(1) balance sheets or extracts from balance sheets for at least the last two years for which accounts have been closed (where publication of the balance sheet is required under the company law of the country in which the economic operator is established the published version must be included; otherwise such documents must be certified by the company's chartered accountant);

(2) a statement of annual overall turnover and annual turnover concerning services covered by this call for tenders of at least 300,000 € during each of the last three financial years, which will be verified with the information provided in Annex B.

3.2.2. Technical and professional capacity of tenderers

Tenderers are required to prove that they have sufficient technical and professional capacity to perform all services as required in this call for tenders. Evidence of the technical and professional capacity may be furnished on the basis of the following documents:

(1) Company profile and internal processes demonstrating the professional and technical capacity to perform services similar to those described in this call for tenders.

(2) List of projects/contracts performed within the last three years, similar to the services described in the present call for tenders. To this end tenderers shall use the **Questionnaire in Annex B.**

(3) Proof of ISO/IEC 27001(2005) certification acquired since at least 2 years for the company. Furthermore, evidence that the **Senior Security Expert** that will be proposed is certified Information Security Management Systems Lead Auditor (for ISO/IEC 27001:2005) and has been involved **at a minimum** of 5 lead audits, which can be factually demonstrated by his CV.

(4) As per section § 2.6, the tenderer shall provide profiles of staff to be entrusted with implementation of the contract who must have the corresponding minimum years of experience in Information Security fields. Evidence of this capacity must be provided in relevant certificates and Curriculum Vitae that also demonstrate very good knowledge of the English language.

3.3. Legal Position

Tenderers are requested to complete the Legal entity form found in Annex D and to provide the documents requested in the form. Tenderers must ensure to include the name and function of the individual(s) entitled to sign on behalf of the organisation in the case of contract award.

4. ADDITIONAL INFORMATION CONCERNING PARTICIPATION TO THIS TENDER

4.1. Participation of consortia

Groupings of suppliers (or consortia), irrespective of their legal form, may submit a tender on condition that it complies with the rules of competition. Such groupings (or consortia) must specify the company or person heading the project and must also submit a copy of the document authorising this company or person to submit a tender.

In addition, each member of the consortium must provide the required evidence for the exclusion and selection criteria. Concerning the selection criteria 'technical and professional capacity', the evidence provided by each member of the consortium will be checked to ensure that the consortium as a whole fulfils the criteria.

If awarded, the contract will be signed by the company or the person heading the project who will be vis-à-vis Cedefop, the only contracting party responsible for the performance of this contract. Tenders from consortia of firms or group of service providers, contractors or suppliers, must specify the role, qualifications and experience of each member or group.

4.2. Subcontracting/Subcontractors

Any subcontracting/subcontractor must be approved by Cedefop, either by accepting the bidder's tender, or, if proposed by the Contractor after contract signature, in writing by an exchange of letters. The subcontracting/subcontractor will be accepted only if it is judged necessary and does not lead to distortion of competition. If awarded, the contract will be signed by the Tenderer, who will be vis-à-vis Cedefop, the only contracting party responsible for the performance of this contract.

The tenderer must indicate clearly, which parts of the work will be sub-contracted, and additionally specify the identity of those subcontractors only undertaking more than 10% of the work by value.

In addition, each subcontractor must provide the required evidence for the exclusion and selection criteria. Concerning the selection criteria 'technical and professional capacity', the evidence provided by the subcontractor(s) will be checked to ensure that the tenderer with the subcontractor(s) as a whole fulfil the criteria.

Where no sub-contracting is indicated, the work will be assumed to be carried out directly by the bidder.

5. AWARD OF THE CONTRACT

Only the tenders meeting the requirements of the exclusion and selection criteria will be evaluated in terms of quality and price. The evaluation of

the technical and financial offer will be carried out by the competent Evaluation Committee, appointed by Cedefop's Director. After the Evaluation Committee has made a proposal, the Centre shall inform tenderers accordingly and invite the tenderer whose offer places first to sign the proposed contract with the Centre.

The contract shall be awarded to the tenderer submitting the tender that offers the best-value-for-money (best quality-price ratio). A quality-price ratio will be calculated for each tender by dividing the total points for quality by the price.

5.1. Technical evaluation

The assessment of the technical quality will be based on the ability of the tenderers to meet the purpose of the contract as described in sections 2.4 and 2.5. The following technical award criteria will be applied to this tendering procedure, based on the technical proposal requested in 5.1.1:

	Award Criterion	Points
1	Quality of the overall presentation of the technical proposal (5.1.1) and general understanding of the services to be carried out: their context, nature, scope and the results to be achieved, taking into account the tendering specifications mentioned in points 2.4, 2.5, and the Aims & Goals (2.2).	40
2	Detailed description of the methodology suggested for carrying out the work and meeting the tendering specifications: proposals and technical solutions including tools, project communication, risk assessment procedure.	25
3	Allocation of resources: project management, work/time planning and scheduling, reporting and quality of the proposed team.	30
4	Modalities for Secure and Easy communication with Cedefop.	5
	TOTAL	100

Tenders scoring **less than 65** (out of a maximum of 100) points against the technical criteria, will not be considered acceptable and will therefore not have their financial proposal evaluated.

5.1.1. Means of proof: Preliminary technical proposal

The assessment of the technical quality will be based on the ability of the tenderer to meet the purpose of the contract as described in the tendering specifications.

To this end, the tenderer must submit **a preliminary technical proposal** where he should outline all matters laid down in the specifications (points 2.4 and 2.5) and should include:

– methodological information

– description of technical solutions

– work planning and scheduling (taking into account that Cedefop's goals and aims (2.2) in establishing a sound Information Security infrastructure will necessarily follow a piecemeal approach).

The level of detail will be very important and it will be assessed during the evaluation of the tender.

The preliminary technical proposal must demonstrate that the Tenderer and his proposed team have the necessary knowledge of Software and Hardware tools, mechanisms, utilities and processes contributing to the ICT security management and change management for the successful implementation of the contract. (Award criterion 1)

It should also prove that the Tenderer is capable of meeting the tendering specifications, by providing to a minimum all the information related to the scope of this project, namely:

– methodology,

– timeline,

– monitoring,

– reporting, and

– management of the project.

The preliminary technical proposal should describe also the company’s business continuity planning, procedures and the means provided to the staff for seamless service delivery under all possible situations (except those under force majeure conditions) and provide a risk assessment analysis. (Award criterion 2)

At the same time it should indicate the proposed human resources and time allocated respectively. Backup/replacement arrangements should also be proposed. The preliminary technical proposal shall also give a clear indication on the required number of person-days to be dedicated by the staff of the Centre to these tasks in their liaising with the project and the contractor. (Award criterion 3)

The preliminary technical proposal shall finally include the number of resources in person-days of the internal Cedefop ICTF staff that will be needed for this project to be successfully completed. This information will be used for planning purposes.

NB: All the information and means of proof provided are binding and commit the contractor throughout the duration of the contract.

5.2. Financial evaluation

Only tenders scoring 65 points or more (of a maximum of 100 points) against the technical award criteria will have their financial proposal evaluated.

The financial evaluation will be performed based on the prices submitted by the tenderer in the financial grid of **Annex C** "Financial Offer Form".

In order to allow for a comparison of the offers, tenderers are requested to submit prices for the pre-defined scenario reflecting the volume estimates of the Centre for the various requested services. The scenario is presented for evaluation purposes only, and percentages may vary during the actual execution of the contract to reflect the development of the business needs.

NB: Cedefop's estimates are indicative and do not constitute any kind of legal obligation for the Centre.

Information concerning prices:

- The prices quoted must be fixed and not revisable for the first two years of the contract. From the third year of the contract prices may be revised as specified in the draft contract.

- Prices must be quoted in euro and include all expenses.

- Under Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Communities, Cedefop is exempt from all charges, taxes and dues, including value added tax (VAT). Such charges may not therefore be included in the calculation of the price quoted. The VAT amount must be indicated separately.

- It is envisaged that independently of the number of work orders issued each year there shall be an estimated number of up to 8 (maximum) meetings taking place between the tenderer and Cedefop. These meetings shall take place at Cedefop's premises. There is on average one meeting every 6 weeks. Person-day prices should include expenses for those meetings as they shall not be reimbursed by Cedefop. If during implementation of the contract further meetings take place at the request of the Contractor, those will not be eligible for reimbursement; if such further meetings take place at the initiative of Cedefop, costs will be reimbursed to the Contractor on the basis of the applicable rules (see annex VIII to the draft framework contract attached as Annex H to these Tendering Specifications).

6. INFORMATION ON PRESENTATION AND CONTENT OF TENDER

It is extremely important that tenderers present their tender in the correct format and provide all documents necessary to enable the evaluation committee to assess their tender. Tenderers should fully respect the instructions indicated **under points 2 and 3** of this open invitation to tender.

In addition, below you will find details of the required documentation.

6.1. Envelope A - Supporting documents

One original and one copy of:

(5) the checklist found in Annex F

(6) the exclusion criteria declaration as requested in point 3.1 and standard template found in Annex A

(7) the selection criteria documents as requested in point 3.2

(8) the legal entity form found as requested in point 3.3 and found in Annex D

(9) a statement containing the name and position of the individual(s) entitled to sign the contract as requested in point 3.3

(10) the financial identification form as found in Annex E

6.2. Envelope B – Preliminary Technical proposal

One original signed unbound version and four bound copies of:

(1) the technical proposal providing all information requested in point 5.1.1 including information relevant to subcontracting (if applicable) as requested in point 4.2

6.3. Envelope C – Financial proposal

One original signed unbound version and four bound copies of:

(1) the financial proposal (the table in Annex C duly completed).

Annex List

It is MANDATORY that all forms and questionnaires below are dully filled-in and submitted:

(1) Annex A **Declaration on exclusion criteria Form** (mandatory)

(2) Annex B **Selection Criteria Form** (mandatory)

(3) Annex C **Financial Offer Form** (mandatory)

(4) Annex D **Legal Entity Form** (mandatory)

(5) Annex E **Financial Identification Form** (mandatory)

(6) Annex F **Checklist**

(7) Annex G **Contract Notice**

(8) Annex H **Draft Framework Contract**

ANNEX A – DECLARATION ON EXCLUSION CRITERIA

Declaration of honour with respect to

the Exclusion Criteria and absence of conflict of interest

The undersigned.....*[name of the signatory of this form, to be completed]*:

- in his/her own name..... *(if the economic operator is a natural person or in case of own declaration of a director or person with powers of representation, decision making or control over the economic operator)*
  or

- representing..... *(if the economic operator is a legal person)*

official name in full *(only for legal person)*:.....

official legal form *(only for legal person)*:.....

official address in full: .....

VAT registration number: .....

declares that the company or organisation that he/she represents / he/she:

a) is not bankrupt or being wound up, is not having its affairs administered by the courts, has not entered into an arrangement with creditors, has not suspended business activities, is not the subject of proceedings concerning those matters, and is not in any analogous situation arising from a similar procedure provided for in national legislation or regulations;

b) has not been convicted of an offence concerning professional conduct by a judgement which has the force of *res judicata*;

c) has not been guilty of grave professional misconduct proven by any means which the contracting authorities can justify;

d) has fulfilled all its obligations relating to the payment of social security contributions and the payment of taxes in accordance with the legal provisions of the country in which it is established, with those of the country of the contracting authority and those of the country where the contract is to be carried out;

e) has not been the subject of a judgement which has the force of *res judicata* for fraud, corruption, involvement in a criminal organisation, money laundering or any other illegal activity detrimental to the Communities' financial interests;

f) is not the subject of administrative penalty for being guilty of misrepresentation in supplying the information required by the contracting authority as a condition of participation in the procurement procedure or failing to supply an information, or being declared to be in serious breach of its obligation under contract covered by the budget.

In addition, the undersigned declares on their honour that:

g) they have no conflict of interest in connection with the contract; a conflict of interest could arise in particular as a result of economic interests, political or national affinities, family or emotional ties or any other relevant connection or shared interest;

h) they will inform the contracting authority, without delay, of any situation considered a conflict of interest or which could give rise to a conflict of interest;

i) they have not made and will not make any offer of any type whatsoever from which an advantage can be derived under the contract;

j) they have not granted and will not grant, have not sought and will not seek, have not attempted and will not attempt to obtain, and have not accepted and will not accept any advantage, financial or in kind, to or from any party whatsoever, constituting an illegal practice or involving corruption, either directly or indirectly, as an incentive or reward relating to award of the contract;

k) that the information provided to Cedefop within the context of this invitation to tender is accurate, sincere and complete;

l) that in case of award of contract of a value greater than 133,000 Euro, they shall provide the evidence that they are not in any of the situations described in points a), b), d) and e) above. Specifically:

For situations described in (a), (b) and (e), production of a recent extract from the judicial record is required or, failing that, a recent equivalent document issued by a judicial or administrative authority in the country of origin or provenance showing that those requirements are satisfied. Where the Tenderer is a legal person and the national legislation of the country in which the Tenderer is established does not allow the provision of such documents for legal persons, the documents should be provided for natural persons, such as the company directors or any person with powers of representation, decision making or control in relation to the Tenderer.

For the situation described in point (d) above, recent certificates or letters issued by the competent authorities of the State concerned are required. These documents must provide evidence covering all taxes and social security contributions for which the Tenderer is liable, including for example, VAT, income tax (natural persons only), company tax (legal persons only) and social security contributions.

For any of the situations (a), (b), (d) or (e), where any document described in the two paragraphs above is not issued in the country concerned, it may be replaced by a sworn or, failing that, a solemn statement made by the interested party before a judicial or administrative authority, a notary or a qualified professional body in his country of origin or provenance.

By signing this form, the undersigned acknowledges that they have been acquainted with the administrative and financial penalties described under Article 134b in conjunction with Article 133a of the Commission Regulation (EC, Euratom) No 2342/2002 of 23/12/2002 laying down detailed rules for the implementation of Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities, which may be applied by analogy by Cedefop if any of the declarations or information provided prove to be false.

Full name Date Signature

ANNEX B – SELECTION CRITERIA FORM

No.	*Question*	*Answer (if space not sufficient please adapt the table)*		
1.	Since when is your company consulting private enterprises and public administration on ICT security services?			
2.	How many similar projects in size and scope has your company realised? With what turnover for the years below?	Number	Turnover in Euro (with similar projects)	Percentage of overall company turnover
	2005			
	2006			
	2007			
3.	Please indicate reference projects similar to the tasks described in Sec. 2. Please add name of the entity, type (public/private), address and year(s).			
4.	Please describe number and profile of the employees having carried out the reference projects as indicated under point 3 above.			

ANNEX C – FINANCIAL OFFER FORM

The following grid should be used to draw up a financial proposal **for a one year period (scenario).** In this scenario it is estimated that services will cover a total of 60 man-days per year.

The completed financial proposal shall be used as reference throughout the envisaged four year contract execution period, as the contract will be signed for an initial 1-year period and may be renewed up to three times under the same conditions. **Proposed fees shall be all-inclusive**. No extra costs, including the cost for planned meetings and any extra meetings held at the request of the Contractor, will be reimbursed by Cedefop (see 5.2, 4th indent).

Item		Value (Price in €)
1.	**SSE_E =** Price for External[1] person-day for Senior Security Expert & Project Manager	
2.	**SSE_I =** Price for Internal[2] person-day for Senior Security Expert & Project Manager	
3.	**JSE_E** = Price for External[1] person-day for Junior Security Expert	
4.	**JSE_I** = Price for Internal[2] person-day for Junior Security Expert	
5.	**TS_E =** Price for External[1] person-day for Technical Staff	
6.	**TS_I =** Price for Internal[2] person-day for Technical Staff	
7.	**ST_I** = Price for Internal[2] person-day for Security Trainer	
8.	**Total Financial Offer =** (5% x SSE_E + 10% x SSE_I + 20% x JSE_E + 20% x JSE_I + 20% x TS_E + 20% x TS_I + 5% x ST_I) x 60	

The total Financial Offer should result from correctly multiplying entered values taken from rows 1-7 by the indicative scenario's corresponding time allocations.

[1] External = Work done on the premises of the contractor (does not require travel and accommodation expenses)

[2] Internal = Work done at Cedefop's premises (it may require travel and accommodation expenses which should be included in the price offered)

ANNEX D – LEGAL ENTITY FORM

(to be downloaded, depending on the nationality and legal status of the tenderer, from the following website)

http://europa.eu.int/comm/budget/execution/legal_entities_en.htm

ANNEX E - FINANCIAL IDENTIFICATION FORM

(to be downloaded, depending on the nationality of the tenderer, from the following website)

http://europa.eu.int/comm/budget/execution/ftiers_en.htm

PLEASE NOTE:

Please indicate the BIC (Bank Identification Code) in the REMARKS box of the downloaded form.

ANNEX F – CHECK LIST OF MANDATORY DOCUMENTS

The checklist must be used to ensure that you have provided all the documentation for this tender and in the correct way. This checklist should be included as part of your offer.

Please Tick ✓ the boxes provided

Mandatory documents to be included as part of the tender	**Reference paragraph**	**Included**		**If the document is not included, please provide an explanation for the reason**
Envelope **'A'** must contain one original and one copy of:		**Yes**	**No**	
- this checklist		☐	☐	
- exclusion criteria declaration (If applicable, including those of consortia)		☐	☐	
- selection criteria documents (If applicable, including those of consortia and relevant subcontractors)		☐	☐	
- legal entity form		☐	☐	
- name and position of the individual(s) entitled to sign contract		☐	☐	
- financial identification form		☐	☐	
Envelope **'B'** must contain one original and four copies of:				
- the Technical proposal		☐	☐	
Envelope **'C'** must contain				
one original and four copies of:				
- the Financial proposal				

You should also ensure that:

☐	Your offer is formulated in one of the official languages of the European Union.
☐	Both the technical and financial proposals of the offer are signed by you or your authorised agent.
☐	Your offer is perfectly legible in order to rule out any ambiguity.
☐	Your offer is submitted in accordance with the envelope system as detailed in the invitation to tender point 3.
☐	The outer envelope bears the information mentioned in the invitation to tender point 3.

ANNEX G – CONTRACT NOTICE

ANNEX H – DRAFT FRAMEWORK CONTRACT