File No.: 5.27.06.31

STATISTICAL SERVICE
1444 NICOSIA

STRICTLY CONFIDENTIAL

SURVEY ON ICT USAGE AND E-COMMERCE IN ENTERPRISES OF THE FINANCIAL SECTOR 2010

FOR OFFICIAL USE ONLY	
S/N	
Legal Status	
Enterprise Size	
NACE	

GENERAL INFORMATION:

1. The aim of the survey is to collect data on ICT usage, Internet usage and electronic commerce in enterprises. These data are necessary for the implementation of policy programmes of both the Government and the Private Sector.

2. All requested information must be supplied by the IT manager of the enterprise. Regarding the enterprise's background information (Module X), these should be provided by the General Manager or by any other person responsible.

3. An authorised employee of the Statistical Service will contact the IT manager of the enterprise by phone in order to arrange a visit for the completion of the questionnaire.

4. Definitions of the terms used in the questionnaire can be found in the glossary attached.

5. The reference period for the data is **January 2010**, unless the question refers to other specific period.

6. The collection of data is carried out in accordance with the Statistics Law 15(I)/2000. The Statistical Service is bound by the Statistics Law to treat all information obtained as **STRICTLY CONFIDENTIAL**. Your responses will be used solely for statistical purposes.

G. Chr. Georgiou
Director
Statistical Service

7 January, 2010

Module A: Use of computers and computer networks

A1.	**Did your enterprise use computers, in January 2010?**	**Yes** □	**No** □ → Go to X1
A2.	**Please answer (a) or (b)** a) **How many persons employed used computers at least once a week, in January 2010?** If you can't provide this value, b) **Please indicate an estimate of the percentage of the number of persons employed who used computers at least once a week, in January 2010.**	□□□□ □□□ %	
A3.	**Was your enterprise using an internal network[(1)] (e.g. LAN - Local Area Network) connecting at least 2 computers, in January 2010?**	**Yes** □	**No** □ → Go to A5
A4.	**Did your enterprise use wireless access[(2)] within its internal computer network (e.g. wireless LAN), in January 2010?**	**Yes** □	**No** □
A5.	**Did your enterprise have in use an internal home page[(3)] (Intranet), in January 2010?**	**Yes** □	**No** □
A6.	**In January 2010, did your enterprise have an extranet[(4)] (a website or an extension of the Intranet with access restricted to business partners)?**	**Yes** □	**No** □
A7.	**Did your enterprise have in use, in January 2010, third party free or open source operating systems[(5)], such as Linux?** (i.e. with its source code available, no copyright cost, and the possibility to modify and/or (re)distribute it)	**Yes** □	**No** □

Module B: Access and use of the Internet[(6)]

(Scope: enterprises with Computers)

B1.	**Did your enterprise have access to the Internet, in January 2010?**	**Yes** □	**No** □ → Go to C1
B2.	**Please answer (a) or (b)** a) **How many persons employed used computers with access to the World Wide Web at least once a week, in January 2010?** If you can't provide this value, b) **Please indicate an estimate of the percentage of the number of persons employed who used computers with access to the World Wide Web at least once a week, during January 2010.**	□□□□ □□□ %	

B3. Did your enterprise have the following types of external connection to the Internet, in January 2010?

	Yes	No
a) Traditional Modem[7] (dial-up access over normal telephone line) or ISDN[8] connection	□	□
b) DSL[9] (xDSL[10], ADSL, SDSL etc) connection	□	□
c) Other fixed internet connection (e.g. cable, leased line (e.g. E1 or E3 at level 1 and ATM at level 2), Frame Relay, Metro-Ethernet, PLC - Powerline communication, etc.), fixed wireless connections)	□	□
d) Mobile broadband connection (via 3G modem or 3G handset) using e.g. UMTS, CDMA2000 1xEVDO, HSDPA	□	□
e) Other mobile connection using e.g. analogue mobile phone, GSM, GPRS, EDGE	□	□

B4. Did your enterprise use the Internet for the following purposes, in January 2010?

(as <u>consumer</u> of Internet services)

	Yes	No
a) Banking and financial services	□	□
b) Training and education	□	□

	Yes	No
B5. Did your enterprise use the Internet for interaction with public authorities, during 2009?	□	□ → Go to B7

B6. Did your enterprise use the Internet to interact with public authorities in the following ways, during 2009?

	Yes	No
a) For obtaining information	□	□
b) For obtaining forms, e.g. tax forms	□	□
c) For returning filled in forms, e.g. Filling tax forms online	□	□
If yes to c) c1) To which services? ………………………………..……………………………….…………..		
d) For treating an administrative procedure (e.g. declaration, registration, authorisation request) completely electronically without the need for additional paper work (including payment if required)	□	□
If yes to d) d1) To which services? ………………………………..……………………………….…………..		
e) For submitting a proposal in a public electronic tender system (e-procurement) (in the system itself and not by e-mail[11])	□	□
If yes to e) e1) To which services? ………………………………..……………………………….…………..		

	Yes	No
B7. Did your enterprise have a Website[12] or Home Page, in January 2010?	□	□ → Go to B9

<u>If yes</u>, give the address of your website:

……

B8.	**Did the Website or Home Page have any of the following facilities, in January 2010?**	**Yes**	**No**
	a) A privacy policy statement, a privacy seal or certification related to website safety	□	□
	b) Product catalogues or price lists	□	□
	c) Possibility for visitors to customise or design the products	□	□
	d) Online ordering, reservation or booking, e.g. shopping cart	□	□
	e) Order tracking available on line	□	□
	f) Personalised content in the website for regular/repeated visitors	□	□
	g) Advertisement of open job positions or online job application	□	□
B9.	**Was your enterprise, in January 2009, using a digital signature[13] in any message[14] sent, i.e. using encryption methods that assure the authenticity and integrity of the message** (uniquely linked to and capable of identifying the signatory and where any subsequent change to the message is detectable)**?**	**Yes** □	**No** □

Module C: Electronic transmission of data[15] between enterprises

(Scope: enterprises with Computers)

Electronic transmission of data suitable for automatic processing means:
- sending and/or receiving of messages (e.g. orders, invoices, payment transactions, product descriptions, transport documents, tax declarations)
- in an agreed or standard format which allows their automatic processing,
e.g. EDI, EDIFACT, ODETTE, TRADACOMS, XML , xCBL, cXML, ebXML
- without the individual message being manually typed.
- via any computer network(s)

C1.	**In January 2010, did your enterprise send or receive electronically such information[16] to or from other enterprises in a format that allowed its automatic processing?**	**Yes** □	**No** □ → Go to D1
C2.	**Did your enterprise send or receive electronically such information for the following purposes?**	**Yes**	**No**
	a) Sending orders to suppliers	□	□
	b) Receiving e-invoices[17]	□	□
	c) Receiving orders from customers	□	□
	d) Sending e-invoices[17]	□	□
	e) Sending or receiving product information (e.g. catalogues, price lists)	□	□
	f) Sending or receiving transport documents (e.g. consignment notes)	□	□

Module D: Automatic share of information within the enterprise

(Scope: enterprises with Computers)

Sharing information electronically and automatically between different functions of the enterprise means any of the following:

- Using one single software application to support the different functions of the enterprise;

- data linking between the software applications that support the different functions of the enterprise;

- using a common database or data warehouse accessed by the software applications that support the different functions of the enterprise;

- within this enterprise, sending or receiving electronically information that can be automatically processed.

D1. In January 2010, when your enterprise received a sales order (either electronically or not), was the relevant information about it shared electronically and automatically with the software used for the following functions?

	Yes	No
a) Your management of inventory levels	□	□
b) Your accounting	□	□
c) Your production or services management	□	□
d) Your distribution management	□	□

D2. In January 2010, when your enterprise sent a purchase order (either electronically or not), was the relevant information about it shared electronically and automatically with the software used for the following functions?

	Yes	No
a) Your management of inventory levels	□	□
b) Your accounting	□	□

	Yes	No
D3. In January 2010, did your enterprise have in use an ERP [18] (enterprise resource planning) software package to share information between different functional areas (e.g. accounting, planning, production, marketing)?	□	□

D4. In January 2010, did your enterprise have in use any software application for managing information about clients (so called- Customer Relationship Management – CRM[19] software) that allows it to:

	Yes	No
a) Capture, store and make available to other business functions the information about its clients?	□	□
b) Make analysis of the information about clients for marketing purposes (setting prices, make sales promotion, choose distribution channels, etc.)?	□	□

	Module E: ICT Security (Scope: enterprises with Computers)		
	ICT security means: Measures, controls and procedures applied on ICT systems in order to ensure integrity, authenticity, availability and confidentiality of data[15] and systems.		
E1.	**In January 2010, did your enterprise have a formally defined ICT security policy with a plan of regular review?**	**Yes** □	**No** □ → Go to X1
E2.	**Were the following risks addressed in the ICT security policy?**	**Yes**	**No**
	a) Destruction or corruption of data[15], due to attack or by unexpected incident	□	□
	b) Disclosure of confidential data [15] due to intrusion[20], pharming[21], phishing[22] attacks or by accident	□	□
	c) Unavailability of ICT services due to attack from outside (e.g. Denial of Service attack[23])	□	□
E3.	**In January 2010, what was the approach of your enterprise to make staff aware of their obligations in ICT security related issues?**	**Yes**	**No**
	a) Compulsory training or presentations	□	□
	b) By contract, e.g. contract of employment	□	□
	c) Voluntary training or generally available information (e.g. on the Intranet, news letters or paper documents)	□	□
E4.	**During 2009, what kind of ICT related security incidents affected your ICT systems resulting in**	**Yes**	**No**
	a) unavailability of ICT services, destruction or corruption of data[15] due to hardware or software failures?	□	□
	b) unavailability of ICT services due to attack from outside, e.g. Denial of Service attack[23]?	□	□
	c) destruction or corruption of data[15] due to infection of malicious software or unauthorised access?	□	□
	d) disclosure of confidential data[15] due to intrusion[20], pharming[21], phishing[22] attacks?	□	□
	e) disclosure of confidential data[15] in electronic form by employees whether on intention or unintentionally?	□	□

E5.	**In January 2010, did your enterprise use one of the following internal security facilities or procedures?**		
		Yes	**No**
	a) Strong password authentication[24] i.e. minimum length of 8 mixed characters, maximum duration of 6 months, encrypted transmission and storage	□	□
	b) User identification[25] and authentication[24] via hardware tokens, e.g. smart cards	□	□
	c) User identification[25] and authentication[24] via biometric methods	□	□
	d) Offsite data backup[26]	□	□
	e) Logging activities for analyses of security incidents	□	□

Module X: Background information

X1.	**Main economic activity of the enterprise, during 2009** (description)	………………………..…………… ………………………..…………… ………………………..…………… ………………………..……………
X2.	**Average number of persons employed, during 2009**	|___|___|___|___|

Module Z: General Information

Z1. **If you have any comments about the survey, please write down below:**

....

....

....

....

Z2.	**Name of the person who answered the questionnaire:**
	Position in the enterprise:
	Telephone:
	Fax:
	E-mail:
Z3.	**Name of the person who completed the questionnaire:**
	Time needed to fill out this questionnaire:
	Signature:
	Date:

TO BE COMPLETED BY THE ENUMERATOR:

Z4. **Completion of the questionnaire::**

a) The questionnaire is completed……………………………………………………….…… 1

b) The enterprise has closed…………..…………....…………………..…………………… 2

c) The enterprise can not be located…………………………..…………………………… 3

d) The enterprise refuses to cooperate………………………………..…………………... 4

e) The enterprise was closed during the collection of the data………………..…………… 5

f) Merge with another enterprise………………………………………..…...……… 6

g) Other reasons for no completion …………………………………………………………. 7

Please specify:

....

....

....

FOR OFFICIAL USE ONLY

Z5. **Name of the person who checked the questionnaire:**

GLOSSARY

(1) **Internal computer network**

An internal computer network is a group of at least two computers connected together using a telecommunication system for the purpose of communicating and sharing resources within an enterprise. It typically connects personal computers, workstations, printers, servers, and other devices. It is used usually for internal file exchange between connected users; intra business communications (internal e-mail, internal web based interface etc), shared access to devices (printers etc) and other applications (databases) or for joint business processes.

LAN (Local Area Network) - A network for communication between computers confined to a single building or in closely located group of buildings, permitting users to exchange data, share a common printer or master a common computer, etc.

(2) **Wireless access**

The use of wireless technologies such as radio-frequency, infrared, microwave, or other types of electromagnetic or acoustic waves, for the last internal link between users devices (such as computers, printers, etc) and a LAN backbone line(s) within the enterprise’s working premises. It includes mainly Wi-fi and Bluetooth technologies.

(3) **Intranet**

An internal company communications network using Internet protocol allowing communications within an organisation.

(4) **Extranet**

A closed network that uses Internet protocols to securely share enterprise's information with suppliers, vendors, customers or other businesses partners. It can take the form of a secure extension of an Intranet that allows external users to access some parts of the enterprise's Intranet. It can also be a private part of the enterprise's website, where business partners can navigate after being authenticated in a login page.

(5) **Free / Open Source operating systems**

Open source operating system software refers to computer software under an open source license. An open-source license is a copyright license for computer software that makes the source code available under terms that allow for modification and redistribution without having to pay the original author. Such licenses may have additional restrictions such as a requirement to preserve the name of the authors and the copyright statement within the code.

Related to the Open Source Definition is the Free Software definition by the Free Software Foundation, which attempts to capture what is required for a program license to qualify as being free-libre software. In practice, licenses meet the open source definition almost always also meet the Free software definition. All licenses reported to meet the free software definition as of 2005 also meet the open source definition.

(6) **Internet**

Relates to Internet Protocol based networks: www, Extranet over the Internet, EDI over the Internet, Internet-enabled mobile phones.

(7) **Modem**

Device that modulates outgoing digital signals from a computer or other digital device to analogue signals for a conventional copper twisted pair telephone line and demodulates the incoming analogue signal and converts it to a digital signal for the digital device.

(8) **ISDN**

Integrated Services Digital Network.

(9) **DSL (Digital Subscriber Line)**

A high-bandwidth (broadband), local loop technology to carry data at high speeds over traditional (copper) telephone lines.

(10) **xDSL**

Digital Subscriber Line. DSL technologies are designed to increase bandwidth available over standard copper telephone wires. Includes IDSL, HDSL, SDSL, ADSL, RADSL, VDSL, DSL-Lite.

xDSL, ADSL etc.

DSL technologies designed to increase bandwidth over standard copper telephone wires; includes ADSL (Asymmetric Digital Subscriber Line) etc.

(11) **E-mail**

Electronic transmission of messages, including text and attachments, from one computer to another located within or outside of the organisation. This includes electronic mail by Internet or other computer networks.

(12) **Web site**

Location on the World Wide Web identified by a Web address. Collection of Web files on a particular subject that includes a beginning file called a home page. Information is encoded with specific languages (Hypertext mark-up language (HTML), XML, Java) readable with a Web browser, like Netscape's Navigator or Microsoft's Internet Explorer.

(13) **Digital Signature**

A digital signature is some kind of electronic information attached to or associated with a contract or another message used as the legal equivalent to a written signature. Electronic signature is often used to mean either a signature imputed to a text via one or more of several electronic means, or cryptographic means to add non-repudiation and message integrity features to a document. Digital signature usually refers specifically to a cryptographic signature, either on a document, or on a lower-level data structure.

For either of them to be considered a signature they must have a legal value, otherwise they are just a piece of communication.

Some web pages and software EULAs claim that various electronic actions are legally binding signatures, and so are an instance of electronic signature. For example, a web page might announce that, by accessing the site at all, you have agreed to a certain set of terms and conditions. The legal status of such claims is uncertain.

An electronic signature can also be a digital signature if it uses cryptographic methods to assure both message integrity and authenticity. Because of the use of message integrity mechanisms, any changes to a digitally signed document will be readily detectable if tested for, and the attached signature cannot be taken as valid.

It is important to understand the cryptographic signatures are much more than an error checking technique akin to checksum algorithms, or even high reliability error detection and correction algorithms such as Reed-Solomon. These can offer no assurance that the text has not been tampered with, as all can be regenerated as needed by a tamperer. In addition, no message integrity protocols include error correction, for to do so would destroy the tampering detection feature.

Popular electronic signature standards include the OpenPGP standard supported by PGP and GnuPG, and some of the S/MIME standards (available in Microsoft Outlook). All current cryptographic digital signature schemes require that the recipient have a way to obtain the sender's public key with assurances of some kind that the public key and sender identity belong together, and message integrity measures (also digital signatures) which assure that neither the attestation nor the value of the public key can be surreptitiously changed. A secure channel is not required.

A digitally signed text may also be encrypted for protection during transmission, but this is not required when the digital signature has been properly carried out. Confidentiality requirements will be the guiding consideration.

(14) **Message**

Any thought or idea expressed briefly in a plain or secret language, prepared in a form suitable for transmission by any means of communication.

(15) **Data**

Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analogue quantities to which meaning is or might be assigned.

(16) **Information**

1) Facts, data, or instructions in any medium or form.

2) The meaning that a human assigns to data by means of the known conventions used in their representation.

(17) **e-Invoice**

An e-invoice is an invoice where all data is in digital format and it can be processed automatically. A distinctive feature of an e-invoice is automation. E-invoice will be transferred automatically in inter-company invoicing from the invoice issuer's or service provider’s system directly into the recipient's financial or other application.

The transmission protocol might be XML, EDI or other similar format.

(18) **ERP**

Enterprise Resource Planning (ERP) consists of one or of a set of software applications that integrate information and processes across the several business functions of the enterprise. Typically ERP integrates planning, procurement, sales, marketing, customer relationship, finance and human resources.

ERP software can be customised or package software. These latter are single-vendor, enterprise wide, software packages, but they are built in a modular way allowing enterprises to customise the system to their specific activity implementing only some of those modules.

ERP systems typically have the following characteristics:

1. are designed for client server environment (traditional or web-based);
2. integrate the majority of a business’s processes;
3. process a large majority of an organization’s transactions;
4. use enterprise-wide database that stores each piece of data only once;
5. allow access to the data in real time.

(19) **CRM**

Customer Relationship Management (CRM) is a management methodology which places the customer at the centre of the business activity, based in an intensive use of information technologies to collect, integrate, process and analyse information related to the customers.

One can distinguish between:

1. Operational CRM – Integration of the front office business processes that are in contact with the customer.
2. Analytical CRM – Analysis, through data mining, of the information available in the enterprise on its customers. This aims to gather in depth knowledge of the customer and how to answer to its needs.

(20) **Intrusion**

An intrusion is an attempt to bypass security controls on a information system. Means of intrusion can be eavesdropping, viruses, worms, trojan horses, logic or time bombs, brute force attacks, etc.

Intrusion detection

Intrusion detection is a process with the purpose of detecting intrusions or attempts of intrusions into a computer or network to compromise the confidentiality, integrity or availability by observation of system, application and user activity as well as network traffic. Intrusion detection systems take preventive actions against intrusions without direct human intervention.

(21) **Pharming**

The term “pharming” connotes an attack to redirect the traffic of a website to another, bogus website in order to acquire sensitive information.

(22) **Phishing**

Phishing is a criminally fraudulent attempt to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

(23) **Denial of service attack**

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.

One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

(24) **Authentication**

Authentication means to assure the identity of a certain user. In general, identification and authentication of users are used in the context of authorisation, that defines access and usage rights related to specific information or services. Authentication can be done with the help of passwords (authentication by knowledge), or with additional devices, such as smart cards, hardware tokens or identity cards (authentication by ownership). The last possibility would be authentication by characteristics, i.e. using biometrical authentication, such as finger prints or retina patterns. A strong identification is defined by at least a combination of two authentication methods, e.g. passwords and smart cards. The positive reply to the question should at least cover strong authentication for at least a subset of staff or clients.

(25) **Identification**

Identification refers to the ability of identifying and thus distinguishing between individual users

(26) **Offsite data backup**

Offsite data backup is part of the off-site data protection strategy of sending critical data from the main site to another location by means of removable storage media, e.g. magnetic type, external harddisks, or electronically via remote backup services.