COMMUNITY SURVEY ON ICT USAGE AND E-COMMERCE IN ENTERPRISES 2010

General outline of the survey

Sampling unit:	Enterprise.
Scope / Target Population:	**Economic activity:** Enterprises classified in the following categories of NACE Rev. 2: - Section C – *"Manufacturing"*; - Section D,E – *"Electricity, gas and steam, water supply, sewerage and waste management"*; - Section F – *"Construction"*; - Section G – *"Wholesale and retail trade; repair of motor vehicles and motorcycles"*; - Section H – *"Transportation and storage"*; - Section I – *"Accommodation and food service activities"*; - Section J – *"Information and communication"*; - Section L – *"Real estate activities"*; - Division 69 -74 –*"Professional, scientific and technical activities"*; - Section N - *"Administrative and support activities"*; - Group 95.1 - *"Repair of computers"*; <u>Only for modules A to C, E , G and X (X1, X2, X5):</u> - Classes/groups 64.19 + 64.92 + 65.1 + 65.2 + 66.12 + 66.19 - *"Financial and insurance activities"*. **Enterprise size:** Enterprises with 10 or more persons employed; <u>Optional</u>: enterprises with number of persons employed between 1 and 9. **Geographic scope:** Enterprises located in any part of the territory of the Country.
Reference period:	Year 2009 for the % of sales/orders data and where specified. January 2010 for the other data.
Survey period:	First quarter 2010.
Questionnaire:	The layout of the national questionnaire should be defined by the country. However, countries should follow the order of the list of variables enclosed, if possible. The background information (Module X) should be placed at the end of the questionnaire. This information can be obtained in 3 different ways: from national registers, from Structural Business Statistics or collected directly with the ICT usage survey. Every effort should be made to obtain them from the most recent SBS survey. Countries can include additional questions. **Note on the use of "Don't know" response categories:** In general "Don't know" response categories are not recommended as it is considered that such an answer would provide the same information as a blank one. Even if the respondent does not have the information, it should be possible to gather it from records or from someone else in the enterprise. However, there are a few exceptions in which cases a "Don't know" response category is used in the model questionnaire.
Target respondent:	A decision maker with major responsibility for IT-related issues in the

	enterprise (the IT manager or a senior professional in the IT department). In smaller enterprises, the respondent should be someone at the level of managing director or the owner. In any case the respondent should not be someone with responsibilities only in accounting.
Sample size, stratification:	The sampling design and the resulting sample size should be appropriate for obtaining accurate, reliable and representative results on the variables and items in the model questionnaire.
	This objective should be achieved for the overall proportions as well as for the proportions for the different breakdowns of the population defined below: NACE and size class. NACE breakdown and enterprise size class breakdown are not required to be cross-tabulated.
	This requirement aims at ensuring the collection of a complete dataset – without empty, confidential or unreliable cells - for these indicators.
NACE breakdown:	**(To be applied to: all variables; enterprises with 10 or more persons employed; whole territory of the Country.)**
	Data should be broken down by the following NACE Rev. 2 aggregates for possible calculation of **national** NACE Rev. 2 aggregates:

    1   10 - 18
    2   19 - 23
    3   24 - 25
    4   26 - 33
    5   35 - 39
    6   41 - 43
    7   45 - 47
    8   49 - 53
    9   55
    10 58 - 63
    11 68
    12 69 – 74
    13 77 - 82
    14 26.1-26.4, 26.8, 46.5, 58.2, 61, 62.01, 62.02, 62.03, 62.09, 63.1, 95.1

Only for modules A to C, E, G and X (X1, X2, X5):
    15 64.19 + 64.92 + 65.1 + 65.2 + 66.12 + 66.19

Breakdowns for which national data should be provided with the purpose of possible calculation of **European** NACE aggregates:
    1a   10-12
    1b   13-15
    1c   16-18
    4a   26
    4b   27-28
    4c   29-30
    4d   31-33
    7a   45
    7b   46
    7c   47
    9a   55 - 56
    10a 58-60
    10b 61
    10c 62-63
    13a 77-78 + 80-82
    13a 79
    14a 95.1

Only for modules A to C, E, G and X (X1, X2, X5):
    15a 64.19 + 64.92

	15b 65.1 + 65.2 15c 66.12 + 66.19

Size class breakdown:	**(To be applied to: all variables; aggregate of all mandatory NACE aggregates [1 to 15 defined above]; whole territory of the Country.)**
	Data should be broken down by the following size classes of the number of persons employed:
	   1 10 or more
	   2 10 - 49 (small enterprises)
	   3 50 - 249 (medium enterprises)
	   4 250 or more (large enterprises)
	
	Optional:
	   5 1-9
	   6 1-4
	   7 5-9

Weighting of results:	Results should in general be weighted by number of enterprises. Turnover/Purchases weighting should be used for sales/purchases related questions. Quantitative variables in the e-commerce module related to sales/purchases should be weighted by total turnover/total purchases. Weighting by the Number of Persons Employed should be applied for questions A2, B2 and for % using the Internet, % having broadband, % having DSL, % having a website or homepage, % purchasing via computer networks, % receiving orders via computer networks, % receiving orders via computer networks.
Treatment of non-response/'Do not know':	**Unit non-response:** The non-respondent units should be assumed to resemble those who have responded to the survey and be treated as non-selected units. For this, the weighting or the grossing up factors should be adjusted: the design weight N_h / n_h is replaced by N_h / m_h where N_h is the size of stratum h, n_h is the sample size in stratum h and m_h is the number of respondents in stratum h. **Item non-response:** Logical corrections should be made, when information can be deducted from other variables, and priority given to further contacts with enterprises to collect the missing information. For the categorical variables (e.g. the YES/NO questions), respondents with item non response or 'do not know' should not be imputed with values from respondents who answered the question. Numerical variables shouldn't be imputed (see also Methodological Manual).
Tabulation of results:	For the categorical variables, estimates should be made for the total number of enterprises for each response category, tabulated using the breakdowns specified above. For the quantitative variables (turnover, sales, purchases and number of persons employed), when collected in absolute or percentage terms (and not in percentage classes), estimates should be made for the total values in absolute terms, tabulated using the breakdowns specified above.
Data transmission:	Results are to be sent to Eurostat following the transmission format described in another Eurostat document.

COMMUNITY SURVEY ON ICT USAGE AND E-COMMERCE IN ENTERPRISES

2010

Model Questionnaire

(Questions relating to the *i*2010 Benchmarking Indicators are marked with an asterisk *)

	Module A: Use of computers and computer networks		
	(Scope: enterprises with Computers)		
A1.	**Did your enterprise use computers, in January 2010?** (Filter question)	Yes	No → Go to X1
A2.	**How many persons employed used computers at least once a week, in January 2010?** *- Optional* If you can't provide this value, **Please indicate an estimate of the percentage of the number of persons employed who used computers at least once a week, in January 2010. –** *Optional*	*(Number)* ⬚⬚⬚ %	
A3.*	**Was your enterprise using an internal network (e.g. LAN - Local Area Network) connecting at least 2 computers, in January 2010?** (Filter question)	Yes	No → Go to A5
A4*	**Did your enterprise use wireless access 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 (Intranet), in January 2010?**	Yes	No
A6.*	**In January 2010, did your enterprise have an extranet (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, 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		
	(Scope: enterprises with Computers)		
B1.	**Did your enterprise have access to the Internet, in January 2010?** (Filter question)	Yes	No → Go to C1

B2.*	**How many persons employed used computers with access to the World Wide Web at least once a week, in January 2010?**	*(Number)*
	If you can't provide this value, **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 (dial-up access over normal telephone line) or ISDN connection		
	b) DSL (xDSL, 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		
	d1) Mobile **broadband** connection via portable computer using **3G modem**, e.g. laptop, notebook, nettop with 3G modem using e.g. UMTS, CDMA2000 1xEVDO, HSDPA *- optional*		
	d2) Mobile **broadband** connection via **3Ghandset**, e.g. smartphone using e.g. UMTS, CDMA2000 1xEVDO, HSDPA *- optional*		
	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?** *- optional*		
	(as consumer of Internet services)	Yes	No
	a) Banking and financial services		
	b) Training and education		

B5.*	**Did your enterprise use the Internet for interaction with public authorities, during 2009?** (Filter question)	Yes	No → 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. provision of statistical information to public authorities		
	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)		
	e) For submitting a proposal in a public electronic tender system (e-procurement) (in the system itself and **not by e-mail**)		

B7.	**Did your enterprise have a Website or Home Page, in January 2010?** (Filter question)	Yes	No → Go to B9

B8.	**Did the Website or Home Page have any of the following facilities, in January 2010?** *- optional*	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 2010, using a digital signature in any message 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 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) [national examples]		
C1.*	**In January 2010, did your enterprise send or receive electronically such information to or from other enterprises in a format that allowed its automatic processing?** (Filter question)	Yes	No → Go to D1
C2.	**Did your enterprise send or receive electronically such information for the following purposes?**		
		Yes	No
	a) Sending payment instructions to financial institutions *Optional*		
*	b) Sending orders to suppliers		
*	c) Receiving e-invoices		
*	d) Receiving orders from customers		
*	e) Sending e-invoices		
*	f) Sending or receiving product information (e.g. catalogues, price lists)		
*	g) Sending or receiving transport documents (e.g. consignment notes)		
	h) Sending or receiving data to/from public authorities (e.g. tax returns, statistical data, import or export declarations [national examples]) *- optional*		

	Module D: Sharing electronically information on Supply Chain Management		
	(Scope: enterprises outside the financial sector with Computers)		

	Sharing electronically information on supply chain management means:
	– **exchanging all types of information with suppliers and/or customers in order to coordinate the availability and delivery of products or services to the final consumer;**
	– including information on demand forecasts, inventories, production, distribution or product development;
	– via computer networks between computers of different enterprises.
	– it can be from you to your suppliers/customers or the other way around.
	  This information may be exchanged via websites or other means of electronic data transfer,
	  but it excludes manually typed e-mail messages.		

D1.	**In January 2010, did your enterprise share information electronically on supply chain management with your suppliers or customers?** (Filter question)	Yes	No → Go to E1
D2.	**Did this enterprise share the information electronically with its <u>suppliers</u>, in January 2010?** On Inventory levels, production plans, demand forecasts or progress of deliveries (i.e. distribution of raw materials or finished products)	Yes	No
D3.	**Did this enterprise share the information electronically with its <u>customers</u>, in January 2010?** On Inventory levels, production plans, demand forecasts or progress of deliveries (i.e. distribution of raw materials or finished products)	Yes	No
D4.	**Were the following methods used for the electronic exchange of this information, in January 2010?** *- optional*	Yes	No
	a) Websites (yours, those of your business partners or web portals)		
	b) Electronic transmission allowing automatic processing methods (e.g. EDI-type systems, XML, EDIFACT, etc.)		

Module E: 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.

		Yes	No
E1.*	**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?**		
	a) Your management of inventory levels		
	b) Your accounting		
	c) Your production or services management		
	d) Your distribution management		
E2.*	**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?**		
	a) Your management of inventory levels		
	b) Your accounting		
E3.*	**In January 2010, did your enterprise have in use an ERP (enterprise resource planning) software package to share information between different functional areas (e.g. accounting, planning, production, marketing)?**		
E4.*	**In January 2010, did your enterprise have in use any software application for managing information about clients (so called-Customer Relationship Management – CRM software) that allows it to:**		
	a) Capture, store and make available to other business functions the information about its clients?		
	b) Analyse the information about clients for marketing purposes (setting prices, making sales promotion, choosing distribution channels, etc.)?		

Module F: e-Commerce		
(Scope: enterprises outside the financial sector with Computers)		

e-Commerce means:
- the **placement of orders**, where an order is a commitment to purchase goods or services,
- **via computer networks**, not only the Internet but also other connections between computers of different enterprises,
- where payment and delivery does not have necessarily to be done via computer networks.

e-Commerce may be done
  via **websites**, i.e. orders made at an online store or via web forms on the Internet or extranet,
  via **electronic transmission allowing automatic processing methods (e.g. EDI-type systems**, XML, EDIFACT, etc.) between enterprises or organisations;
  it **excludes** manually typed e-mail messages.

Orders received via computer networks (Sales)			
F1.*	**During 2009, did your enterprise receive orders for products or services via computer networks** (via a website, EDI-type systems or other means of electronic data transfer excluding manually typed e-mails)**?** (Filter question)	Yes	No → Go to F5
F2.*	**Please state the value of the turnover resulted from orders received electronically (in monetary terms, excluding VAT), in 2009.** If you can't provide this value, **Please indicate an estimate of the percentage of the total turnover resulted from orders received electronically, in 2009.**	(National currency) _____ ___ ___ ___ %	
F3.	**Please indicate what percentage represented orders received via each one of the following ways, out of total turnover, in 2009.**		
	a) via a website	___ ___ ___ %	
	b) via electronic transmission allowing automatic processing methods (e.g. EDI-type systems, XML, EDIFACT, etc.)	___ ___ ___ %	
F4.*	**For the reception of orders via the Internet, was your enterprise using a secure protocol, such as SSL and TLS, in January 2010?**	Yes	No

Orders placed via computer networks (Purchases)		
F5.*	**Did your enterprise send orders for products or services via computer networks, during 2009** (via a website, EDI-type systems or other means of electronic data transfer excluding manually typed e-mails)**?** (Filter question)	Yes	No → Go to G1

F6.*	**Please indicate for 2009 the percentage of orders that were sent electronically in relation to the total purchases' value (in monetary terms, excluding VAT).**	Less than 1%
		1% or more and less than 5%
		5% or more and less than 10%
		10% or more and less than 25%
		25% or more and less than 50%
		50% or more and less than 75%
		75% or more

Alternative Question
Please state the value of the purchases resulted from orders that were placed electronically (in monetary terms, excluding VAT), in 2009.

_____
(National Currency)

If you can't provide this value
Please indicate an estimate of the percentage of the total purchases that resulted from orders placed electronically, in 2009.

___ ___ ___ %

	Module G: 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 and systems.		
G1.	**In January 2010, did your enterprise have a formally defined ICT security policy with a plan of regular review?**	Yes	No goto G3
G2.	**Were the following risks addressed in the ICT security policy?**	Yes	No
	a) Destruction or corruption of data due to attack or by unexpected incident		
	b) Disclosure of confidential data due to intrusion, pharming, phishing attacks or by accident		
	c) Unavailability of ICT services due to attack from outside (e.g. Denial of Service attack)		
G3.	**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)		
G4.	**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 due to hardware or software failures?		
	b) unavailability of ICT services due to attack from outside, e.g. Denial of Service attack?		
	c) destruction or corruption of data due to infection of malicious software or unauthorised access?		
	d) disclosure of confidential data due to intrusion, pharming, phishing attacks?		
	e) disclosure of confidential data in electronic form by employees whether on intention or unintentionally? *- optional*		
G5.	**In January 2010, did your enterprise use one of the following internal security facilities or procedures?**	Yes	No
	a) Strong password authentication, i.e. minimum length of 8 mixed characters, maximum duration of 6 months, encrypted transmission and storage		
	b) User identification and authentication via hardware tokens, e.g. smart cards		
	c) User identification and authentication via biometric methods *- optional*		
	d) Offsite data backup		
	e) Logging activities for analyses of security incidents		

	Module X: Background information	
	(X1-X4) available in some countries from SBS, the business register or administrative data and thus not to be included; latest available information should be provided	
X1.	**Main economic activity of the enterprise, during 2009**	
X2.	**Average number of persons employed, during 2009**	
X3.	**Total purchases of goods and services (in value terms, excluding VAT), for 2009**	
X4.	**Total turnover (in value terms, excluding VAT), for 2009**	
X5.	***Optional*** **Time needed to fill out this questionnaire**	_____ *(Minutes)*

DSL (Digital Subscriber Line)

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

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.

Electronic commerce (e-commerce)

Transactions conducted over Internet Protocol-based networks and over other computer-mediated networks. The goods and services are ordered over those networks, but the payment and the ultimate delivery of the good or service may be conducted on or off-line. Orders received via telephone, facsimile, or manually typed e-mails are not counted as electronic commerce.

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.

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.

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.

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.
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.
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.

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

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

ISDN Integrated Services Digital Network.

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.

Online payment An online payment is an integrated ordering-payment transaction

Sales via website A part of the e-commerce activities, sales via website are orders made in an online store or filled in and sent by an electronic form on the Internet. Sales in Extranet following the same criteria are included.

SSL/TLS Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols which provide secure communications on the Internet. SSL provides endpoint authentication and communications privacy over the Internet using cryptography. In typical use, only the server is authenticated (i.e. its identity is ensured) while the client remains unauthenticated; mutual authentication requires PKI deployment to clients. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery.

Website 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.

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.

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.

Advanced Encryption Standard[(new)]

Advanced Encryption Standard[1], which has been announced by the American National Institute of Standards and Technology in Oct 2000. The algorithm is freely available and has been integrated in a variety of software and hardware. AES is used by the encryption standard 802.11i for wireless LAN and its Wi-FI equivalent WPA2 as well as in SSH and IPsec. In addition, it is integrated into VoIP communication with protocols like SRTP or Skype. AES is contained in Mac OS X and Windows XP SP1. The service FileVault uses AES and AES is applied for the encryption of compressed archives, e.g. Winzip, 7-zip, pkzip or RAR. The disk encryption softwares free otfe, TrueCrypt, LUKS and DiskCryptor use AES.

Authentication[(new)]

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.

Denial of service attack[(new)]

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.

Data[(new)]

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.
(source: http://www.its.bldrdoc.gov/projects/devglossary/_data.html)

Identification[(new)]

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

Information[(new)]

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

---

[1] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

2) The meaning that a human assigns to data by means of the known conventions used in their representation.
(source: http://www.its.bldrdoc.gov/projects/devglossary/_information.html)

Intrusion detection(new)   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.

Intrusion(new)   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.

Message(new)   Any thought or idea expressed briefly in a plain or secret language, prepared in a form suitable for transmission by any means of communication.
(source: http://www.its.bldrdoc.gov/projects/devglossary/_message.html)

Offsite data backup(new)   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.

Pharming(new)   The term "pharming" connotes an attack to redirect the traffic of a website to another, bogus website in order to acquire sensitive information.

Phishing(new)   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.