



DET NORSKE VERITAS

EBtrust Standard

VERSION 2.0

Foreword

Det Norske Veritas (DNV) is an independent foundation established in 1864 with the objective of safeguarding life property and the environment. DNV is a leading international provider of services for managing risk.

DNV is a knowledge based organization and its prime assets are the creativity, knowledge and expertise of its employees as most of the 5500 employees are highly qualified engineers and technical personnel. DNV is an international company with over 300 offices in 100 different countries, headquartered in Oslo, Norway. DNV's global network is linked by efficient information technology enabling us to create value for our customers in a coherent and consistent manner worldwide.

The growing use of [Internet](#) technologies has resulted in [e-business](#), and to meet the demanding needs of the e-business market, DNV has developed this standard drawn from its long experience of management systems. Predecessors to this version are versions 1.1, 1.2 and 1.3

The application of this standard should generate trust for buyers in e-business, having different mechanism over the conventional businesses where personal interaction generates trust.

The use and implementation of this standard would result in systems, practices and technology which generate trust between buyers and service providers in e-business. The users of this standard will be able to develop and implement methods and technologies to enhance confidence of buyers and partners.

Organizations who have implemented the standard would be able to have the system certified by DNV. [Certification](#) will enable the display of the EBtrust mark on the [website](#). This trust mark communicates the scope, purpose and intent of the certification. The display of the mark is the extension of the DNV brand to create confidence in buyers.

0 General

0.1 Scope

The EBtrust Standard is intended for all [organizations](#) involved in some form of e-business using a website to promote their legal business activities on the [Internet](#). The business type would include Business to Business (B2B), Business to Consumer (B2C), Corporate [Websites](#), General Purpose / Service websites, Vertical or Horizontal Portals, etc.

The intention of the standard is to provide trust and confidence between the organization and interested parties through systems, practices, content and technology. The certification assesses the overall e-business capacity and capability of the organization to operate on Internet, satisfying needs and expectations of interested parties.

0.2 Application

The standard is intended to be modular and applicable to all Websites regardless of business - type, size, service and product provided. It is applicable to any form of e-business.

In addition to a set of general requirements, this standard comprises the following five principal modules:

- a) Ethics
- b) Infrastructure
- c) Security
- d) Process and Organization
- e) Web Marketing

The organization is required to apply those modules that are relevant to their business and at least¹ a minimum of one module shall² be applied in addition to the general requirements. The organization may choose other modules depending upon organization's needs. The reasons for choice of modules shall be documented including reasons for exclusions.

Note1: Not all modules will be relevant to every e-business situation nor can they take into account local market or environmental or technological constraints.

Note2: The term "shall" means that requirements need to be fulfilled and that justification must be made for exclusions, if any, in the Statement of Applicability. The term "should" means that the intent should be satisfied and there may be a degree of flexibility considered.

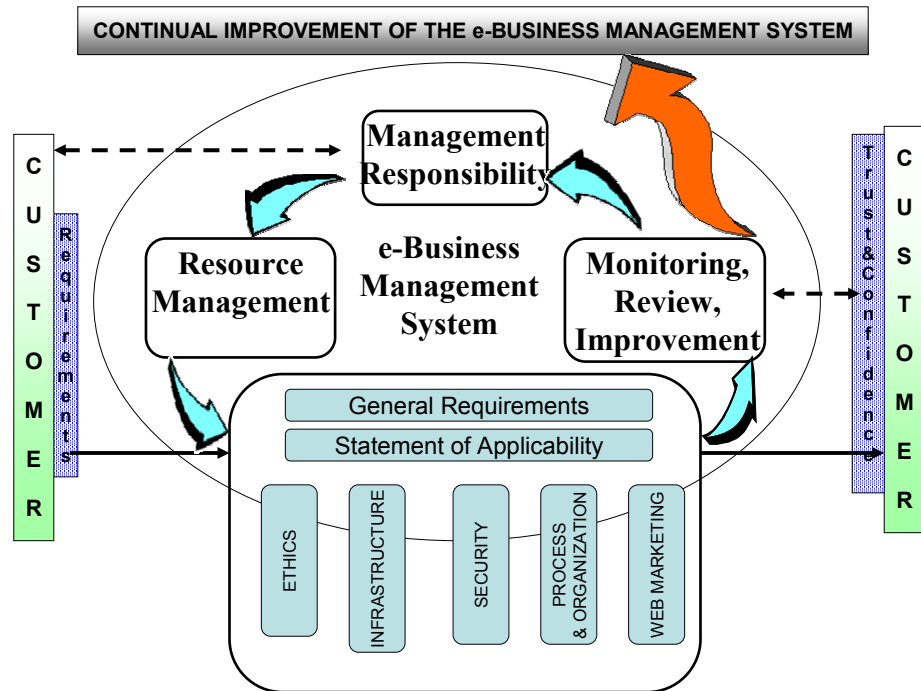


Figure 1.0

1 General Requirements

1.1 Basic requirements

The standard follows the continual improvement cycle and the model depicted in Figure 1.0. This model has been chosen to make it compatible to other management system standards such as ISO 9001, ISO 14001, OHSAS 18001 and BS 7799 so that users of these standards will find the EBtrust standard similar in application and implementation.

The system documentation³ shall include:

- a) Policies related to each module as applied,
- b) Organization chart showing responsibilities,
- c) Customer concern resolution system,
- d) Statement of applicability of the organization with respect to choice of modules,
- e) Other documented system procedures⁴.

Note3: The term "document" means information and its supporting media, which may be in any form.

Note4: The extent of e-business system's documentation may differ between organizations due to size and nature of e-business activities, complexity of processes and their interactions.

The organization's website shall meet the following basic requirements:

- a) Appropriately⁵ designed website,
- b) Appropriate⁵ site navigation and search features,
- c) Statement of [privacy](#),
- d) Description of the organization that is promoting the website,
- e) Terms and conditions with provision for arbitration for resolving disputes for products/services provided,
- f) Statement of fair trade practices,
- g) Contact details, e.g. telephone number, e-mail address, and Street address.
- h) Data backup and recovery systems.

Note5: Depending on target group.

1.2 Control of Documents

The documents required by e-business systems shall be controlled. The organization shall define controls needed to effectively manage the processes:

- a) Approval of documents,
- b) Updating and re-approval of documents,
- c) Availability of relevant documents of current issue at points of use.

1.3 Control of Records

The organization shall identify and maintain the records required to demonstrate its effective application and implementation of the e-business management system.

1.4 Management Responsibility

The top management shall provide evidence of its commitment to the e-business management system and shall communicate this commitment for effective implementation and improvement throughout the organization.

1.5 Responsibility and Authority

Top management shall define responsibility and authority for effective implementation of the e-business management system.

1.6 Management Representative

Top management shall appoint a member of the management who shall have the responsibility and authority to ensure that the systems are established, implemented and maintained as required by the standard. The management representative shall also have responsibility for customer concern resolution.

1.7 Management Review

The top management shall review the system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The records of such review shall be maintained⁶.

Note6: Review shall include performance of the modules, status of Corrective and Preventive actions (CAPA) and customer feedback analysis.

1.8 Statement of Applicability

The organization shall select the module/modules relevant to its business needs and expectations of the customer, as a minimum at least one of the modules shall be applicable.

The organization shall document a Statement of Applicability⁷. This document will be subject to assessment by the assessor(s).

Note7: In preparing the Statement of Applicability all mandatory items shall be considered, and details of and justification for any exclusion shall be described. The selection of the modules and the Statement of Applicability could be based on a business risk assessment.

1.9 Monitoring, Review and Improvement

The organization shall have appropriate processes for monitoring and review of its activities, including:

- a) Business policies,
- b) Business practices/model or both,
- c) Service Level Agreements,
- d) Web traffic and [bandwidth](#) adequacy,
- e) Web content for its relevancy and updates,
- f) Products/services promoted,
- g) Continual improvements, including corrective and preventive actions which would enhance the customer's trust for the services provided through the website.

The organization shall take appropriate actions to eliminate the causes of non-conformities in order to prevent recurrence. Corrective Actions shall be initiated when:

- a) Deviations from defined policies are encountered,
- b) Customer complaints are received,

- c) Business goals are not achieved,
- d) Customer expectations are higher than envisaged,
- e) Any other issue arises which has direct/indirect impact on business areas.

The organization shall determine actions to eliminate the causes of potential non-conformities in order to prevent their occurrence. Preventive actions shall be appropriate to the effects of potential problems.

2 Ethics

2.1 Documentation

The organization shall establish and document an [ethical policy](#) to support an ethical organization culture. The ethical policy shall consider vision, mission, values and [stakeholder](#) expectations. The documented policy may include:

- a) Purpose, Values and Vision Statement,
- b) Mission Statement,
- c) Code of Conduct,
- d) [Confidentiality](#),
- e) Compliance to Norms and Standards,
- f) Stakeholder relations management,
- g) Impact assessment
- h) Communication - Internal/External,
- i) Conflict Resolution,
- j) [Crisis Management](#).

2.2 Implementation

2.2.1 Ethical Business Conduct

The organization shall establish an ethical code of conduct, which is in line with its ethical policy. The ethical policy and the code of conduct shall be communicated internally and externally.

Processes for managing unethical and illegal behavior shall be defined.

2.2.2 Human Resources

Adequate training with respect to the ethical code and its applicability to the work performed shall be provided.

2.2.3 Respect of Privacy

The organization shall use information collected from interested parties only for the purpose that is explicitly stated when collected. Information shall be kept confidential at all stages of transmission and storage. The organization shall enable customers to manage their own personal information.

The organization shall have an opt out possibility for those who wish to discontinue contact with the organization.

2.3 Monitoring and Review

The top management shall monitor, analyze and review business conducted with respect to ethics at periodic intervals and take appropriate actions to correct or change if necessary.

3 Infrastructure

3.1 Documentation

The organization shall establish and document a policy for its infrastructure in line with the e-business. The policy should cover:

- a) Business areas,
- b) Operational goals,
- c) Need for Service Level Agreements (SLA) with service providers/suppliers,
- d) Network infrastructure – [LAN/WAN](#),
- e) Ability to deliver the products/services,
- f) System availability and functionality,
- g) [Data mining](#).

The organization shall establish a procedure for web interface design, including:

- a) Type of software and hardware generally used, including the usage of a defined planning process considering the type of access used by prospective customers,
- b) Good practices for [web page](#) design.

The organization shall appropriately state the various methods used for collection of data, including the intended purpose of such collected data.

3.2 Implementation

3.2.1 Interface Design

- a) The website shall be designed for meeting the needs of the customers, in terms of adequacy and layout of the content, ease of navigation and compatibility. The content shall be comprehensive, correct, timely and updated.
- b) The content layout, design, use of colors, fonts, images, graphics, etc., shall be appropriate to the business activities and should be easily readable, appealing and consistent throughout the site.
- c) The website navigation structure should be simple, logically arranged with appropriate titles/sections and intra-site search features.
- d) The website should be compatible with generally accepted technological standards.
- e) The website shall clearly state needed plug-ins required to view or browse the contents and should provide appropriate links (internal or external) for customers to download software, mentioning implications of using such software where applicable,
- f) The website shall clearly provide details of file size, estimated downloaded time with required instructions to install or uninstall for all downloaded files and executable programs.

3.2.2 System Availability

- a) The Information and Communication Technology ([ICT](#)) systems shall be under surveillance and processes established to ensure business continuity, optimization of downtime, rapid recovery from any disaster or system failure, and implementation of appropriate emergency plans.
- b) The organization shall implement appropriate mechanisms to protect its website from potential hackers including Denial of Service Attacks or any other type of attacks which are detrimental to its business continuity.

3.2.3 System Functionality

- a) The technology adopted shall be evaluated for its adequacy for the website and for the nature of service to be provided. The website integration with back end systems shall be functionally efficient and adequate for the intended purpose.
- b) Available technologies shall be evaluated to provide state of the art functionality and improve [reach](#). The organization should consider usage of Load Balancers depending upon the web [traffic analysis](#).

3.3 Monitoring and Review

The top management shall monitor, analyze and review *e-business* infrastructure against organization's defined policies, goals and target group expectations.

The monitoring and review should include as appropriate:

- a) Link integrity,
- b) Quality and depth of external links provided,
- c) Page size and complexity,
- d) Download times,
- e) Interface functionality,
- f) Ease of use, usefulness of content, quality of content,
- g) User analysis,
- h) Bandwidth and capacity,
- i) LAN/WAN,
- j) Access mechanisms with the organization,
- k) Software and hardware upgrade.

4 Security

4.1 Documentation

The organization shall establish and document a policy regarding e-business security (including privacy), in line with the business of the organization and based on the security [risk assessment](#).

The security documentation should address as appropriate:

- a) Computer deployment plan,
- b) Identification of network services to be provided for each computer,
- c) Installation of Operating System and other Software on each client/[server](#),
- d) Identification of actions to protect information contained on hardware that is no longer in use,
- e) Determination of privileges of each computer user,
- f) Determination of how the servers / client computers will be connected to network,
- g) Access controls and [authentication](#) methods,

- h) Enforcement of information data access methods,
- i) Use of [Anti-Virus programs](#),
- j) [Firewall](#) deployment and its configuration,
- k) Intrusion detection strategy,
- l) Day-to-Day security administration,
- m) Backup and recovery of information stored on computer hard drives,
- n) Network maintenance and recovery methodology,
- o) Any other issue that may be specifically related to nature of business carried out by the organization.

4.2 Implementation

4.2.1 Risk Assessment and Management

The organization shall identify potential security risks and periodically assess their significance. Significant risks shall be appropriately managed. Risk assessment and management shall be documented. The [risk management](#) shall include:

- a) Identification of known security problems specific to organizational, physical and logical security systems deployed,
- b) Identification of methods for checking the integrity of computer configurations (checking baseline information for computers using cryptographic tools, etc.) after making changes,
- c) Specification of the most secure way of connecting remote computers, eliminating unnecessary open network ports and dead user accounts,
- d) Handling of [log](#) files – security/system/error/intrusion detection, software updates scheduling,
- e) Adequacy of network architecture adopted, user account policies and logical and organizational security.

4.2.2 Organizational and Physical Security

- a) The computer security in the organization and the related responsibilities shall be clearly defined, including appropriate [SLAs](#) for the service providers. The SLAs should have appropriate provisions for confidentiality clauses for subjects that when divulged could be detrimental to organization's business interests.
- b) The organization shall have physical systems in place or electronic entry prevention systems installed that control property access as appropriate.
- c) The organization shall consider physical security threats from Fire and Smoke, Water, Earth movements, Storms, Sabotage/Vandalism, Explosion, Building collapse, Utility Loss (Power, Heating, Cooling, Air), Communication Loss, Equipment Failures, Personnel Loss, Electrical Loss (UPS/Generator) for protecting its computer networks and data.
- d) The organization shall have appropriate policy to protect its physical assets and data from natural disasters and human error in order to ensure business continuity.
- e) Business contingency plans shall be established and tested at regular intervals, and concerned employees shall be trained in their respective roles and responsibilities in these plans.
- f) The organization shall inform its customers of any breach of privacy or compromise of security.

4.2.3 Logical Security

- a) The organization shall continually verify the data access controls and authentication methods for its continued suitability and application, including as appropriate:
 - i) Data to be protected,
 - ii) Data access controls,
 - iii) Password complexity,
 - iv) Password aging,
 - v) Password management policy for changing, handling password compromise, including any guest accounts,
 - vi) User account creation/deletion and its authorization.
- b) The organization shall also address restricting the access to software resources not required in the work of specific users, screen locking after a period of inactivity, use of [encryption](#) methods to prevent access to sensitive files. The organization shall document:
 - i) The Access Control Techniques (Discretionary / Mandatory / Lattice Based / Rule Based / Role Based / ACL Access Controls),

- ii) Access Control Administration (Account Administration, Account, Log and Journal Monitoring, Access Rights and Permissions, Principles of least Privilege, Maintenance, and Revocation).
- c) The event logs should support accountability by providing a trace of user actions, and audit trails should be designed and implemented to record appropriate information that can assist in intrusion detection and re-mediation.

4.3 Monitoring and Review

The top management shall review the organization's security risk assessment, policy, practices and performance at regular intervals and make changes as needed.

The organization shall monitor, analyze and review its performance with respect to security periodically, including security breaches, network intrusions, incident handling, audit trails, alarms, anomaly identification, intrusion response, and [virus](#) protection.

5 Process and Organization

5.1 Documentation

The organization shall establish and document a policy for its e-business operations and processes. The policy may include as appropriate:

- a) Business goals model and plan,
- b) The organization's capability to process and deliver the product or service,
- c) Its functional areas required for delivering the product promoted through the websites to its customers as per the statements made in website,
- d) Selection methodology and criteria for channel associates, partners and support services,
- e) Transaction integrity methods,
- f) Customer satisfaction measurement,
- g) Industry specific benchmarking,
- h) Customer retention programs,
- i) Commercial terms and conditions,
- j) Invoicing policy and methods,
- k) Management of account transactions,
- l) Customer complaints and its handling process,
- m) Profiling of customers,
- n) Improving product range and services,
- o) Providing product incentives,

- p) Personalization and customization of web pages for customers,
- q) Analyzing and monitoring web traffic from other referral sites,
- r) Monitoring effectiveness of all internal processes.

The organization shall design and document a [business model](#), including organization business functions and supply value chain/network integration with partners/suppliers.

5.2 Implementation

5.2.1 Business Model

- a) The organization shall implement its business model in order to ensure capability of fulfilling e-business policies and goals and building a sustainable business.
- b) The organization should implement a business plan defining objectives, strategies, resources and actions to achieve business goals and control business sustainability.
- c) The organization should analyze the customer's buying trend and profile customer using data mining techniques.
- d) The organization should revise its selling proposition based on analysis of buying trends.

5.2.2 Request and Order Processing

- a) The organization shall be capable of processing e-transactions. The website shall reveal all relevant information that describes the characteristics of the services/products offered and applicable terms for the e-transaction.
- b) It shall be easy to understand how to make a request/order, and when a request/order is actually placed, its acceptance shall be confirmed in accordance with stated benchmarked time criteria.
- c) The organization shall explicitly state terms and conditions of sale – order processing, delivery, cancellation and invoicing processes, etc.
- d) The terms and conditions of sale shall be in accordance with the local laws prevailing at places of e-transaction.
- e) The organization shall provide all necessary product/service details to complete the e-transaction.
- f) The organization should maintain a database of executed orders.

5.2.3 Production and Delivery

- a) The organization shall ensure appropriate production capacity, processes, delivery methods and customer service.
- b) External partners/suppliers shall be selected on their capability to perform in line with the service requirements.
- c) For selected partners/suppliers adequate Service Level Agreements (SLA) shall be in place.
- d) Outsourced services shall be co-ordinated through SLAs.
- e) Any deviation from the confirmed order shall be promptly communicated to the customer.
- f) The organization shall have an effective system for handling customer complaints.
- g) This shall include recording of all complaints (including verbal), arriving at necessary corrective action, and updating/modifying systems procedures where appropriate, as a preventive measure.
- h) The customer complaints shall be analyzed and be reviewed in the Management Review.

5.2.4 Customer Relations

An effective process shall be established to keep track of and follow up customer requests/orders and to provide customer support.

- a) The organization shall have an escalation process for complaint management.
- b) Customer feedback shall be collected and analyzed.
- c) The customers shall be informed:
 - i. How issued information will be used. This includes information gathered by automatic methods such as through use of cookies,
 - ii. That they can opt out from issuing non-critical information that is not necessary for transactions ,
 - iii. About the consequences of issuing or not issuing information.

The organization should find appropriate means and ways of being in touch with customers.

5.3 Monitoring and Reviewing

- a) The top management shall review the performance of its business processes, including the effectiveness of the value chain/network, real time revenue generated and profitability.
- b) Policies and practices shall be reviewed and evaluated with respect to the objective of performing reliable *e-business*.
- c) Processes shall be established to identify improvement opportunities, and actions shall be taken in order to achieve improvement.
- d) The organization shall measure their customers' satisfaction level.
- e) The SLA with sub-suppliers and partners shall be monitored and if necessary improvement actions shall be taken.
- f) The policies shall be periodically reviewed and updated when appropriate.

6 Web Marketing

6.1 Documentation

The organization shall establish and document a policy related to [web marketing](#) in line with the business.

A web marketing strategy and a market communication strategy shall be established with emphasis on attracting target customers.

The organization shall document an *e-business* strategy (including policies and implementation procedures) as to web marketing. Web marketing documents may consider:

- a) Market situation analysis,
- b) Opportunities and threats,
- c) Strengths and weaknesses – in terms of brand positioning and sales,
- d) Product, promotion and brand objectives,
- e) Strategies, budgets and action plans,
- f) Management and control actions.

The organization shall define its role and its targets with respect to doing e-business.

6.2 Implementation

6.2.1 Market Analysis

The organization shall identify potential markets and customers within those markets. The expectations of the target customers relative to e-business policy shall be determined and analyzed. The competitors shall be monitored and actions taken to remain competitive.

6.2.2 Strategy Planning

- a) The organization should view web marketing strategies as a natural extension of traditional marketing strategies.
- b) The organization shall use a marketing plan to position its products/services, increase brand awareness and value, and to help define and refine its business model and service offering in order to effectively meet target market needs and expectations.
- c) The web-marketing plan shall define pricing of the product/services provided, the promotion campaigns and the returns expected, and resolve conflict between distribution channels. The web-marketing plan shall identify adequate resources to support the implementation of the plan.
- d) The organization shall make test launch when the product/service is new or substantially revised in order to evaluate the capability of providing the product/service and to confirm that the market appropriately perceives the concepts.

6.2.3 Plan Implementation

- a) The organization shall define interfaces between marketing function and other departments.
- b) The organization shall collect, review and analyze market information, and update the marketing plan as necessary.
- c) Market information system shall consider internal accounting, marketing intelligence, market research and marketing management systems.
- d) The organization shall identify critical aspects (including resources) that can influence the implementation of the marketing plan.

6.2.4 Communication Strategy

A communication strategy shall focus on increasing on-line brand value, website identity, reputation and web traffic. Emphasis shall be placed on attracting target customers. The communication strategy should include offline communication activities to promote the website.

6.3 Monitoring and Review

The top management shall monitor the performance of its web marketing activity. It shall review and evaluate policies and practices, and make changes as appropriate.

Key performance indicators shall be defined and measured in order to monitor the organization's web marketing performance. The strategies for web marketing shall be reviewed and updated when appropriate.

7 Glossary

Anti virus program

Software that monitors a computer for viruses and eliminates them before damage occurs

Applet

A small *Java* program that can be sent from a server and called by a web page. Applets differ from full-fledged Java applications in that they are not allowed to access certain resources on the local computer, such as files and serial devices (modems, printers, etc.), and are prohibited from communicating with most other computers across a network. The common rule is that an applet can only make an Internet connection to the computer from which the applet was sent.

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system

Availability

The degree to which a system actually is, or is agreed to be, in operating order and accessible to the user.

Bandwidth

A measure of how much data that can be transmitted through a connection. Usually measured in bits-per-second

Business Model

Definition of a business model (*European Commission, Directorate-General III Industry*)

- ◆ An architecture for the product, service and information flows, including a description of the various business actors and their roles; and
- ◆ A description of the potential benefits for the various business actors; and
- ◆ A description of the sources of revenues.

A business model in itself does not yet provide understanding of how it will contribute to realise the business mission of any of the companies who is an actor within the model. We need to know the marketing strategy of the company in order to assess the commercial viability and to answer questions like: how is competitive advantage being built, what is the positioning, what is the marketing mix, which product-market strategy is followed. Therefore it is useful to identify beyond business models also "marketing models".

Definition of a marketing model

- ◆ A business model; and
- ◆ The marketing strategy of the business actor under consideration.

The classification developed below is for -business models only.

Value chains and business models

A systematic approach to identifying architectures for

business models can be based on value chain de-construction and re-construction, which is identifying value chain elements, and identifying possible ways of integrating information along the chain. It also takes into account the possible creation of electronic markets.

Certification	Any assessment made by an independent third party in accordance with established criteria.
Click Through Rate (CTR)	The average number of click-throughs per hundred advertisement impressions, expressed as a percentage. Usually calculated by taking the number of responses the ad received, dividing that number by the number of impressions and multiplying by 100 to obtain a percentage
Compliance Norms and Standards	Statutory norms and regulations in respective business areas.
Confidentiality	The security objective that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit.
Cookies	Client-side text files that are created by web browsers on request by Web servers, typically to store information about the site visitor and visitor behavior. Information pertaining to a site can be stored in such a way as only to be readable from the site that wrote the information. Used to identify repeat visitors and track visitor behavior. Cookies were originally designed to allow user-side customization of Web information.
Crisis Management	Management of any event which affects organization's reputation, stakeholders, business functions. Proactive crisis management activities include forecasting potential crises and planning how to deal with them. Crisis management in the face of a current, real crisis includes identifying the real nature of a current crisis, intervening to minimize damage and recovering from the crisis.
CRM - Customer Relationship Management	A strategy (technology-enabled) in response to, and in anticipation of, actual customer behavior. From a technology perspective, CRM represents the systems and infrastructure required capturing, analyzing and sharing all facets of the customer's relationship with the enterprise. From a customer care perspective, it represents a process to measure and allocate organizational resources to those activities that have the greatest return and impact on profitable customer relationships
Data integrity	The condition that exists when data has not been altered in an unauthorized manner. Data integrity covers data in transit, during processing, and while in storage.
Data mining	The process of searching through data in order to find patterns, e.g. to investigate customer behavior.
e-business	A business activity conducted over the Internet – buying

Encryption	and selling including any type of collaborative services. To create an illegible copy of a text, usually with the intent of transferring it to a trusted party without revealing the actual content to anyone else, by applying some mathematical function to it. The reverse process of decryption usually involves providing a secret code available only to trusted parties..
Enhanced Internet Security	This is the required level of security needed for applications that deal with higher value and higher sensitivity transactions and information. This consists of enhanced levels of identification, entitlements, verification, privacy, and security management
Ethical organization culture Ethics	An organization culture that promotes ethical behaviour among all stakeholders of the organization The explicit, philosophical reflection on moral beliefs and practices. Ethics is a conscious stepping back and reflecting on morality. Ethics is a body of principles or standards of human conduct that govern the behavior of individuals and groups.
Firewall	Software or hardware that monitors network traffic, limits certain kinds of access to a computer from a network or other outside source and acts as a security barrier set up between a company's internal systems and outside systems.
Frames	Frames are a way of dividing a browser window into two or more parts. This allows the reader to scroll through one part, like our glossary, while leaving another part--the equivalent of the menu bar--available at all times.
FTP	File Transfer Protocol - An internet protocol that allows transfer computer data/files from one computer to another over a network (mostly WAN). FTP is RFC959.
HTTP	Hypertext Transfer Protocol The Internet protocol that specifies how web browsers and web servers communicate. HTTP is RFC1945 (1.0) and RFC2068 (1.1).
ICT (Information and Communication Technology) Identification	ICT systems are made up of hardware and software components. To encrypt a file is to apply a mathematical function that transforms every character in the file into some other character. Encryption renders the file unreadable. This means no one, including you, can read the file until it is decrypted. Only you and the authorized recipients can decrypt the file.
Internet	The Internet is a massive network of networks, a networking infrastructure. It connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet. Information that travels over the Internet does so via a variety of languages known as protocols. ¹
JavaScript	JavaScript is a programming language designed to be

¹ http://www.webopedia.com/DidYouKnow/Internet/2002/Web_vs_Internet.asp

EBtrust Standard V 2.0

	<p>executed by web browsers. It is intended to provide a relatively simple means of adding interactivity to web pages i.e. JavaScript is included in an <i>HTML</i> file it relies upon the browser to interpret the JavaScript. When JavaScript is combined with <i>Cascading Style Sheets (CSS)</i>, and later versions of HTML (4.0 and later) the result is often called <i>DHTML</i>. It is only supported on a few different browsers, and tends not to work exactly the same on different versions. JavaScript was originally developed by Netscape.</p>
LAN	<p>A group of computer connected at particular location, providing access to data on the network, is termed Local Area Network</p>
Log	<p>This is a record of events. It is also an abbreviation for logarithm, which is a mathematical operation.</p>
Organization	<p>A community of stakeholders for whom a set of structures, systems, practices and policies provide identity and purpose.</p>
Organization Culture	<p>Organizational culture is the personality of the organization. Culture is comprised of the assumptions, values, norms and tangible signs of organization members and their behaviors. Members of an organization soon come to sense the particular culture of an organization</p> <p>Corporate culture can be looked at as a system. Inputs include feedback from, e.g., society, professions, laws, stories, heroes, values on competition or service, etc. The process is based on our assumptions, values and norms, e.g., our values on money, time, facilities, space and people. Outputs or effects of our culture are, e.g., organizational behaviors, technologies, strategies, image, products, services, appearance, etc.</p>
Organizational Ethics	<p>A code of values – formal/informal to guide its member's choices and actions along with system practices, policies to effect them</p>
Page view	<p>When a Web page is requested by somebody through a browser. Page views are often used to track the number of impressions a banner gets</p>
PDF	<p>Portable Document Format. A standard used by software applications to display documents on any computer irrespective of its operating system platform. It is developed by Adobe Software and is based on the PostScript page description language.</p>
Policy	<p>A document containing formal/informal expression of its values in order to provide the capacity, continuity and actions required for the organization to achieve its set goals.</p>
Privacy	<p>Privacy entails keeping data confidential while in transit and in storage from end to end of the transaction lifecycle or information exchange. It also constitutes the policy surrounding the use and disclosure of this information within the enterprise</p>
Protocol	<p>A communication procedure when transmitting and receiving data in a network.</p>
Reach	<p>Reach is commonly used in marketing to determine the</p>

Response time	degree of penetration into a target audience. It can be given as either a number of individuals or as a percentage. The time the server uses to display the information that has been requested (e.g. by clicking on a hyperlink). The response time increases when there is high traffic, and the capacity depends on the hardware, and the network connections.
RFC	Request for Comment RFCs specify the protocols that the Internet and related technologies should follow. The most important body related to RFCs are the Internet Engineering Task Force ² . RFC2026 documents best current practices for the Internet Community. RFCs related to e-Business are handled by the trade working group that works in the Internet Open Trading Protocol. ³
Risk Analysis / Risk Assessment	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.
Risk Management	The total process of identifying, controlling, and mitigating information technology related risks. It includes risk analysis; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission/business and constraints due to policy, regulations, and laws.
Search Engines	Search Engines are the automated card catalogues of the Web. Completely automated, Search Engines keep huge files with short catalogue entries of millions of Websites. It is a utility that locates resources via searches for keywords and phrases
Secure Servers	A Secure Server uses a special code to make sensitive information difficult to read for anyone not authorized to access it. They're not perfect, but they're far better than unsecured servers.
Security Management	The act of effectively and efficiently managing identification, entitlements, verification, and privacy such that there is less burden of administration for end users and administrators regardless of application or platform
Server	A computer, or a software package, that provides a specific kind of service to <i>client</i> software running on other computers. A single server machine can (and often does) have several different server software packages running on it, thus providing many different servers to <i>clients</i> on the <i>network</i> . It is typically either a workstation or a mainframe and is expected to handle far greater loads than ordinary desktops systems.
Service Level Agreement	An agreement between two mutually agreed parties on quality of service expectations from each other, for

² <http://www.ietf.org/>

³ <http://www.ietf.org/html.charters/trade-charter.html>

EBtrust Standard V 2.0

SSL	consistent and predictable levels of service, for which the employees responsible can be held accountable. The agreements include expectations by explicitly defining the products, services and support structure that an entity (department, could be outsourced) will provide to its users. Protocol used to maintain data confidentiality only between Web browsers and Web servers. This is a fundamental component of basic Internet security. SSL was originally developed by Netscape.
Stakeholders	All those involved in or affected by the organization's activities, e.g. employees, customers, suppliers, shareholders, local community and society at large.
Telnet	A protocol that allows remote interactive communication with computers, e.g. remote terminal emulation. Telnet is RFC854.
Traffic Analysis	The inference of information from observation of traffic flows (presence, absence, amount, direction, and frequency).
Unique Visitor	A unique visitor is someone with a unique address who is entering a Web site for the first time that day (or some other specified period).
URL or Web Address	A compact string representation for a resource available via the Internet. The URL specifies the protocol used and a path to the resource in question. Web addresses are usually specified as URLs. URL is RFC 1738.
View	A view is, depending on what is meant, either an ad view or a page view. Usually an ad view is what is meant. There can be multiple ad views per page views. View counting should consider that a small percentage of users choose to turn the graphics off (not display the images) in their browser.
Virus	A virus is a program that will seek to duplicate itself in memory and/or on hard disks, but in a subtle way that will not immediately be noticed. A computer on the same network as an infected computer or that uses an infected disk (even a floppy) or that downloads and runs an infected program can itself become infected. A virus can only spread to computers of the same operating platform.
Visit	A visit is a Web user with a unique address entering a Web site at some page for the first time that day (or for the first time in a lesser time period).
WAN	Wide Area Network - A WAN is a data communications network connecting users that covers a relatively broad geographic area and that often over public area and supports lower speeds than LAN.
Web catalogue	An aggregation of information about goods or services for sale on the Internet
Web marketing	Refers to any type of Internet-based promotion, including Websites, targeted e-mail, Internet bulletin boards, sites where customers can dial-in and download files, and so on. The term doesn't have a strict meaning, though, and many marketing managers use it to cover <i>any</i> computer-based marketing tools, including CD-ROM presentations.

Website and Web page

Website is a collection of one or more Web pages. A Web page is a single file that can be displayed on the web

Web site layout

The organization of elements, functionality, and interconnected pages of a web site. Each web site has a home page that is the normal starting point for people visiting the site.

WWW

World Wide Web - Is a way of accessing information over the medium of the Internet. Using HTTP protocol (Hypertext Transport Protocol) to transmit data.

8 SELF ASSESSMENT CHECKLIST

The following are requirements of the standard which can be self-assessed by an organization interested in being certified to the EBtrust standard. This is an indicator of the readiness and maturity for conducting e-business. However, it must not be construed to contain all the requirements of the EBtrust standard.

8.1 General Requirements

#	Checkpoint	Yes	No	NA
1	Is the e-business management system documented?			
2	Is the system documentation controlled with respect to document approval, updating and re-approval, and availability?			
3	Is the website appropriately designed?			
4	Does the website have appropriate navigation and search features			
5	Is there a Statement of Privacy on the website?			
6	Is the organization behind the website described?			
7	Are terms and conditions for doing business over the website defined?			
8	Is there a provision for dispute resolution?			
9	Is there a statement of fair trade practices?			
10	Are contact details (e.g. telephone number, street address, email address) described?			
11	Are there data backup and recovery systems in place?			
12	Are the necessary records identified and maintained?			
13	Has top management defined responsibility and authority for establishment, implementation and maintenance of the e-business management system, including the appointment of a management representative?			
14	Does top management review the system at planned intervals with respect to suitability, adequacy and effectiveness?			
15	Does the organization have appropriate processes for i. Monitoring and review of activities? ii. Continual improvement, including corrective and preventive actions)			

EBtrust Standard V 2.0

8.2 Ethics

#	Checkpoint	Yes	No	NA
1	Has the organization established and documented an ethical policy considering its vision, mission and values, and stakeholder expectations?			
2	Has the organization established an ethical code of conduct in line with the ethical policy?			
3	Are the ethical policy and code of conduct communicated internally and externally?			
4	Are processes for managing unethical and illegal behavior defined?			
5	Do the employees receive training in ethics?			
6	Does the organization show respect of privacy by <ul style="list-style-type: none"> i. Using information collected from interested parties only for the purpose explicitly stated when collected? ii. Keeping the information confidential? iii. Enabling customers to manage their own personal information? 			
7	Does the organization have an "opt out" possibility for those who wish to discontinue contact?			
8	Does top management monitor, analyze and review business conducted with respect to ethics at periodic intervals?			

8.3 Infrastructure

#	Checkpoint	Yes	No	NA
1	Has the organization established and documented a policy for its infrastructure for e-business?			
2	Has the organization established a procedure for web interface design?			
3	Has the organization documented the various methods used for collection of data and the intended purpose of such collected data?			
4	Is the website designed for meeting the needs of the users?			
5	Is the website content comprehensive, correct and up-to-date?			
6	Does the website provide details about <ul style="list-style-type: none"> i. Needed plug-ins? ii. File sizes and time estimates for downloading? iii. Instructions to install and uninstall executable programs? 			
7	Are the ICT systems under surveillance and processes established to ensure system availability and business continuity?			
8	Are mechanisms implemented to protect the website from malicious attacks (including Denial of Service attacks)?			
9	Is the technology adopted evaluated with respect to ability to provide necessary functionality?			
10	Are available technologies being evaluated to provide state of the art functionality?			
11	Does top management monitor, analyze and review the infrastructure against defined policies, goals and target group expectations?			

8.4 Security

#	Checkpoint	Yes	No	NA
1	Has the organization established and documented a policy regarding e-business security (including privacy)?			
2	Is the policy based on a security risk assessment for the business of the organization?			
3	Are potential security risks identified and their significance periodically assessed?			
4	Does the risk assessment cover organizational, physical and logical security?			
5	Are significant risks properly managed?			
6	Are responsibilities related to computer security in the organization and its service providers clearly defined?			
7	Is physical access to the organization's premises controlled?			
8	Are physical assets and data protected from accidents and natural disasters?			
9	Are physical assets and data protected from human error?			
10	Are business contingency plans prepared and tested at regular intervals?			
11	Are concerned employees trained in their roles and responsibilities in business contingency plans?			
12	Does the organization have suitable data access controls and authentication methods?			
13	Are tests conducted to verify network security?			
14	Are there backup methods of systems and data?			
15	Is user authentication required?			
16	Are there procedures to handle security breach response?			
17	Are non-disclosure clauses part of all contracts and agreements with external agencies?			
18	Are security assessments/audits on external agencies allowed by contract or agreement and performed?			
19	Are data disposal procedures in place (covering hardcopy, disks, diskettes, magnetic tapes, obsolete equipment)?			
20	Does the organization monitor, analyze and review its performance with respect to security periodically, including <ul style="list-style-type: none"> i. Security breaches? ii. Network intrusions? iii. Incident handling? iv. Audit trails? v. Alarms? vi. Anomaly identification? vii. Intrusion response? viii. Virus protection? 			
21	Does top management review the organization's security risk assessment, policy, practices and performance at regular intervals?			

8.5 Process and Organization

#	Checkpoint	Yes	No	NA
1	Has the organization established and documented a policy for its e-business operations and processes?			
2	Has the organization designed and documented a business model, including organization business functions and supply value chain/network integration with partners/suppliers?			
3	Has the organization implement its business model?			
4	Is the organization capable of processing e-transactions?			
5	Does the website reveal all relevant information that describes the characteristics of the services/products offered and applicable terms for the e-transaction?			
6	Is it easy to understand how to make a request/order?			
7	Is request/order acceptance confirmed to the customer?			
8	Are terms and conditions of sale explicitly stated (such as order processing, delivery, cancellation, invoicing process)?			
9	Are terms and conditions of sale in accordance with local laws?			
10	Are all details about the product/service necessary for completing the e-transaction provided?			
11	Does the organization have appropriate production capacity and processes, delivery methods, and customer service?			
12	Are Service Level Agreements with external partners/suppliers in place?			
13	Are deviations from confirmed orders promptly communicated to the customer?			
14	Does the organization have an effective system for handling customer complaints?			
15	Is there a process established for keeping track of customer requests/orders and providing customer support?			
16	Does the organization have an escalation process for complaint management?			
17	Is customer feedback collected and analyzed?			
18	Are customers informed: <ul style="list-style-type: none"> i. About how collected information will be used? ii. That they can opt out from issuing information that is not necessary for transactions? iii. About the consequences of issuing or not issuing information? 			
19	Are policies and practices periodically reviewed and evaluated?			
20	Are processes established to identify improvement opportunities and to take actions in order to achieve improvement?			
21	Does the organization measure customers' satisfaction level?			
22	Does top management review the performance of the business processes, including the effectiveness of the value chain/network, revenues generated and profitability?			

8.6 Web marketing

#	Checkpoint	Yes	No	NA
1	Has the organization established and documented a policy related to web marketing?			
2	Has a web marketing strategy and a market communication strategy been established?			
3	Has the organization documented an e-business strategy as to web marketing?			
4	Has the organization defined its role and targets with respect to doing e-business?			
5	Has the organization identified potential markets and potential customers within those markets?			
6	Have expectations of target customers relative to e-business policy been determined and analyzed?			
7	Are competitors being monitored?			
8	Does the organization have a marketing plan?			
9	Does the organization make use of test launches when the product/service is new or substantially revised?			
10	Has the organization defined interfaces between the marketing function and other departments?			
11	Is the organization collecting, reviewing and analyzing market information and updating the marketing plan accordingly?			
12	Has the organization identified critical aspects that can influence the implementation of the marketing plan?			
13	Does the organization have a communication strategy focusing on on-line brand value, website identity, reputation and web traffic?			
14	Are key performance indicators defined and measured in order to monitor the organization's web marketing performance, and are strategies for web marketing reviewed and updated accordingly?			
15	Does top management monitor the performance of the web marketing activity?			
16	Does top management review and evaluate policies and practices for web marketing and make changes as appropriate?			