TECHNICAL GUIDE ON E-COMMERCE–CONSIDERATIONS FOR AUDIT OF FINANCIAL STATEMENTS

The basic draft of the Technical Guide was prepared by CA. Gunjan Bansal, New Delhi. The views expressed in this Technical Guide are those of the author and may not necessarily be the views of the organisation he represents.

The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

First Edition : June, 2008

Price : Rs. 125

ISBN : 978-81-8441-065-5

E-mail : aasb@icai.org

Website : www.icai.org

Published by : The Publication Department on behalf of Shri Vijay Kapur, Director, Auditing and Assurance Standards Board, The Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi-110 002.

Printed by : Sahitya Bhawan Publications, Hospital Road, Agra 282 003.
June/2008/1100 Copies

FOREWORD

Information technology has grown to be an integral part of our environment, and a common goal of using technology is to simplify the way we do things – achieving a complex task by the simple press of a button. This new environment poses new challenges for the organizations as well as for the auditors thereby requiring auditors to be armed with specialized skills while discharging their professional responsibilities.

I am happy to note that the Auditing and Assurance Standards Board has brought out *Technical Guide on E-Commerce-Considerations for Audit of Financial Statements*. The Technical Guide is an attempt to provide guidance for application of the principles enunciated in the Standards on Auditing while performing audit of entities involved in e-commerce activities. I would also like to appreciate the endeavors of the Board in bringing out technical literature on new areas with the objective of enhancing commitment and competence of our members.

I am confident that the members will find this Technical Guide useful while carrying out their assignments.

June 3, 2008
New Delhi

CA.Ved Jain
President

PREFACE

In a technology savvy environment, e-commerce has increasingly become an integral component of business strategy and a strong catalyst for economic development. With developments in the Internet and Web-based technologies, distinctions between traditional markets and the global electronic marketplace are gradually being narrowed down. The speed and convenience of the new technologies have not only provided unique new business opportunities, but also certain embedded risks.

This new environment poses fresh challenges for auditors engaged in auditing those clients who are adopting e-commerce strategies. Just as businesses are adapting to advances in technology, the auditing profession also needs to respond to the changing environment. Thus, the Auditing and Assurance Board of the Institute of Chartered Accountants of India has developed this Technical Guide to guide auditors when auditing the financial statements of an entity where considerable information is transmitted, processed, maintained or accessed electronically. This Technical Guide apart from giving a brief on e-commerce also explains the risks that sprout up in an e-commerce environment which an auditor must essentially understand for effectively discharging his professional responsibilities. This Technical Guide identifies specific matters related to e-commerce environment and provides guidance to apply relevant Standards on Auditing (SAs) while performing audit in an e-commerce environment.

I must place on record deep appreciation for the efforts put in by CA. Gunjan Bansal for preparing the basic draft of the Technical Guide. I am also thankful to my colleagues at the Auditing and Assurance Standards Board for their considered and uninhibited views so necessary to make the Technical Guide more comprehensive and user friendly. I also need to express my thanks to Shri Vijay Kapur, Director and CA. Jyoti Singh, Assistant Director for their inputs in giving final shape to the publication.

New Delhi
June 3, 2008

CA. Harinderjit Singh
Chairman
Auditing and Assurance Standards Board

CONTENTS

E-commerce-An Introduction

1.1 Electronic commerce (e-commerce) has become a buzzword for businesses over the past few years, with increased awareness about the use of computer and communications technologies to simplify business procedures and increase efficiency. E-commerce is more than a technology, it is a business model built around the application of information and communication technologies to any aspect of the value chain for products and services. Perhaps the clearest indication of the growing importance of e-commerce in the global economy is the rapidity with which internet use has grown and spread during the last decade. The boom in e-commerce also includes increased use of other media for trade, such as the telephone, television, fax, and electronic payment. E-commerce has been the catalyst for the enhancements and greater efficiency in areas that include:

- Selling products and processing orders;
- Tracking customers' buying habits;
- Presenting customers and prospects with product catalogs;
- Presenting financial statements to investors;
- Providing customers with inventory availability information;
- Providing message databases for off-site sales people and staff; and
- Processing purchase orders and invoice from suppliers.

Historical Perspective

1.2 The origin of commerce by exchanging goods occurred before recorded history. Now commerce is a basic activity of goods trading and buying in everyday life. Entering into the electronic era, the way individuals and organizations do business and undertake commercial transactions have been changed. The emergence of large business organizations in the late 1800s and early 1900s triggered the need to create and maintain formal records of business transactions. The process of using a person or a computer to generate a paper form, mailing that form, and then having another person enter the data into the trading partner's computer was slow, inefficient, expensive, redundant and unreliable.

1.3 The history of e-commerce is how information technology has transformed business processes. The meaning of electronic commerce has changed over the last 30 years. Originally, electronic commerce meant the facilitation of commercial transactions electronically, using technology such as Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT). These were both introduced in the late 1970s, allowing businesses to send commercial documents like, purchase orders or invoices electronically. The growth and acceptance of credit cards, automated teller machines (ATMs) and telephone banking in the 1980s were also forms of electronic commerce. From the 1990s onwards, electronic commerce would additionally include enterprise resource planning systems (ERP), data mining and data warehousing.

Traditional Commerce and E-Commerce

1.4 E-commerce has changed the way the organizations operated in their traditional business environments. E-commerce implementations are often coupled with re-engineering of traditional business processes by examining how business should be conducted by taking the advantage of the technology. Specifically, e-commerce replaces the traditional manual business processes with their automated electronic equivalents to accelerate ordering, delivery and payment procedures e.g., on-line booking of train tickets and air tickets, trading in stock market, on-line purchase of movie tickets, on-line auction and shopping, on-line supply chain management, on-line banking, etc. If we look at these changes closely, we will find that e-commerce is an enabler and has not changed the basics of the traditional business.

1.5 To understand e-commerce in the context of the traditional business, we may take an example of a bank, which has enabled on-line banking :

S. No.	Traditional banking environment	On-line banking environment
a)	Customer visits home branch to deposit cash.	Customer may visit any branch/ATM of the bank to deposit cash.
b)	Customer visits home branch to deposit cheque/transfer funds.	Customer may deposit cheque at any branch/ATM of the bank and may use internet banking to transfer funds.
c)	Customer makes a telephone call to branch/ visits branch for balance enquiry. Customer used to receive periodic statements from bank for transactions done.	All this information is available any time by using internet banking to the customer.

d)	For utility bill payment manual process is followed.	Using internet, utility bill payments can be made.
e)	To place fixed deposit or withdraw a fixed deposit customer visits the home branch.	Internet banking can be used to place fixed deposit or withdraw from fixed deposit.

It is clear from the above that e-commerce has brought business and customer closer by directly connecting them and by accelerating ordering, delivery of product and information and payment processes. However, it may be noted that e-commerce can not replace all the functions in the traditional business. For example, take the case of an automobile purchase. Before a buyer actually buys an automobile, he or she needs to test drive it. Such functions, obviously, cannot be performed on-line.

Objectives of the Technical Guide

1.6 The objectives of this Technical Guide is to assist the auditors of financial statements where an entity engages in commercial activities that takes place by means of connected computers over a public network, such as the internet (e-commerce). The guidance in this Technical Guide is particularly relevant to the application of:

- SA 230, Audit Documentation
- SA 250, Considerations of Law and Regulations in an Audit of Financial Statements
- SA 300, Planning an Audit of Financial Statements
- SA 315, Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and its Environment
- SA 330, The Auditor's Responses to Assessed Risks

- SA 500, Audit Evidence

This Technical Guide identifies specific matters to assist the auditor when considering the significance of e-commerce to the entity's business activities, and the effect of e-commerce on the auditor's assessment of the risk for the purpose of forming an opinion on the financial statements.

Definition of E-commerce

2.1 In common parlance, e-commerce is the buying and selling of goods and services on the Internet, especially the World Wide Web. Generally, e-commerce may be comprised of:

- E-tailing or "virtual storefronts" on web sites with on-line catalogs, sometimes gathered into a "virtual mail";
- Gathering and use of demographic data through Web contacts;
- Electronic Data Interchange (EDI), the business-to-business exchange of data;
- E-mail and e-fax and their use as media for reaching prospective and established customers (for example, with newsletters) including internet telephony;
- Business-to-business buying and selling;
- The security of business transactions services;
- Any other activity of similar nature.

2.2 E-commerce has been defined by different organizations in the following manner:

Information Systems Audit and Control Association (ISACA) defines e-commerce as the process by which organizations conduct business electronically with their customers, suppliers and other external business partners, using the internet as an enabling technology. Therefore, it encompasses both business-to-business (B2B) and business-to-consumer (B2C) e-commerce models, but does not include existing non-internet e-commerce methods based on private networks, such as EDI and SWIFT.

Organization for Economic Co-operation and Development (OECD) defines e-commerce as commercial transactions, involving both organizations and individuals, that are based upon the processing and transmission of digitized data, including text, sound and visual images and that are carried out over open networks (like, the internet) or closed networks (like, AOL or Minitel) that have a gateway onto an open network.

The International Fiscal Association (IFA) has, for the purpose of the National and General Reports released at the 55th Congress held in October, 2001, defined e-commerce to be 'commercial transactions in which the order is placed electronically and goods or services are delivered in tangible or electronic form and there is an ongoing commercial relationship'.

2.3 In view of the above, elements of e-commerce may include :

a) A product or service.

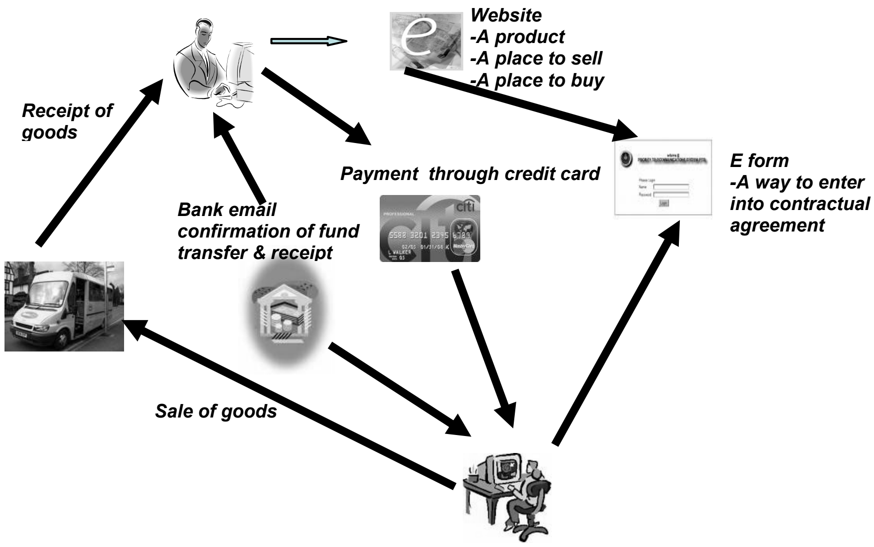
b) A place to sell the product or service - in e-commerce, a Website displays the products in some way and acts as the place.

c) A way to get people to come to your Website (the place).

d) A way to accept orders - normally an on-line form of some sort, e.g., on-line order for purchase of books.

e) A way to accept money - normally a merchant account handling credit card payments. This piece requires a secure ordering page and a connection to a bank. One may also use more traditional billing techniques either on-line (e.g., Real Time Gross Transfer) or through the mail.

f) A fulfillment facility to ship products to customers. In the case of software and information, however, fulfillment can also occur over the Web through a file download mechanism.



g) A way to accept rejected/returned goods and services.

h) A way to handle warranty claims if necessary.

i) A way to provide customer service (often through e-mail, on-line forms, on-line knowledge bases, etc.).

These elements are not exhaustive considering the continuous changes in the domain of e-commerce.

Internet vis-à-vis World Wide Web- The Common Misconception

2.4 The terms “internet”, “world wide web”, “net”, and the “web” are often used interchangeably. However, from a technical perspective, the internet and world wide web are two separate entities. The internet is a collection of wires, protocols, and hardware that allows the electronic transaction of data over Transmission Control Protocol (TCP)/Internet Protocol (IP). Any data can be transferred over this collection of hardware and software components. Examples include e-mail, faxes, video, voice, and web pages. The internet is the hardware and software infrastructure that allows for this data transfer and global networking

2.5 The world wide web (www) exists on the internet. The web is composed of hypertext pages viewed by a browser, which is served from a web server over TCP/IP. Web pages always begin with http:// or https://, signifying that the content being viewed is in hypertext and transferred using the Hypertext Transfer Protocol. So while the internet is the infrastructure, the web can be thought of as an application for the internet . For example, e-mail, file transfer protocol (FTP), and peer-to-peer applications.

Business Models for E-commerce

2.6 In the most basic sense, a business model is the method of doing business by which an organization can sustain itself- that is, generate revenue. The business model spells out how an organization makes money by specifying where it is positioned in the value chain. Internet commerce will give rise to new kinds of business models. That much is certain. However, the web is also likely to reinvent tried and tested models. Auctions are a perfect example. One of the oldest forms of brokering, auctions have been widely used throughout the world to set prices for such items as agricultural commodities, financial instruments, and unique items like, fine art and antiquities. The web has popularized the auction model and broadened its applicability to a wide array of goods and services.

2.7 Business models have been defined and categorized in many different ways. The basic four categories of business models are discussed in the following table:

Business originating from….

Demand initializing from….	Business	Consumer
Business	B2B	C2B
Consumer	B2C	P2P/C2C

Business-to-Business (B2B)

It refers to the full spectrum of e-commerce that can occur between two organizations. Among other activities, this includes purchasing and procurement, supplier management, inventory, etc.

Business- to- Consumer (B2C)

It refers to exchange between business and consumers, such as those managed by on-line bookshops, e-mail and information websites.

Peer- to-Peer (P2P)

Exchanges involve transactions between and among consumers. These exchanges can include third-party involvement, as in the case of the auction websites. Other operations that support peer-to-peer activity include job search websites.

Consumer- to- Business (C2B)

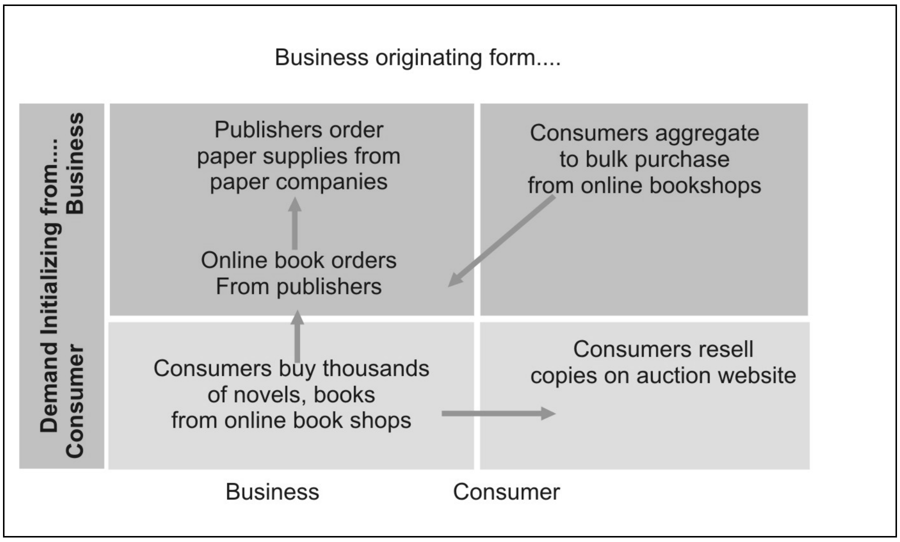
Consumers can band together to present themselves as a buyer group in a consumer-to-business (C2B) relationship. These groups may be economically motivated, as with demand aggregators, or socially oriented, as with cause related advocacy groups.

Apart from the abovementioned four key models, following two new models have also emerged:

(i) Business to Government e.g., electronic submission of corporate tax returns.

(ii) Consumer to Government e.g., electronic submission of individual income tax returns.

2.8 Example illustrating convergence of above stated four key e-commerce models is as follows:



Risks associated with E-commerce

3.1 The risks associated with e-commerce systems are no different than those associated with traditional information systems. These risks include unauthorized access, unauthorized changes to programs or data files, misstatements caused by processing or logic errors, and lack of physical security. Other risks may, however, be unique to e-commerce systems. Following are some potentially unique risks in an e-commerce environment:

- Security of system and protection against malicious intrusion or penetration by outsiders – The intrusion may be to disrupt the system or to steal, modify, or otherwise put the organization at a competitive disadvantage.

- Integrity and completeness of processing – The risks differs from similar risks only in that different paths can be taken that might threaten processing integrity. The internet opens the systems to penetration from many different sources.

- Integrity of data communications – Computer viruses are a large and costly problem. An organization faces additional risks if communications are intercepted, modified, sent to the wrong party, replicated and delivered to many customers, or lost in process. A company dependent on electronic communications is essentially "betting the company" if it does not control the risks associated with data communications.

- Trading partner agreements – Many systems are designed with a group of trading partners in mind. Trading partners usually make contracts that all parties must agree to. Penalties are often severe if the contracts, including the protection of data, are not met.

- Systems interdependencies – The economic advantages associated with these systems creates interdependencies that did not exist in any previous business arrangement. Compromises anywhere along these interdependencies could seriously jeopardize either trading partners.

- Paperless systems coupled with "soft controls" – The movement to e-commerce is just one part of re-engineering a system. These changes are often coupled with just-in-time inventory systems in which the purchasing company specifies (a) quality criteria that must be met, (b) availability requirements, and (c) shipping requirements. The shipping requirements are loaded directly into production with no inspection or counting. The trading partner agreements specify payment terms, penalties, and so forth. The organization must adapt not only to paperless system, but also to a system in which a record of incoming items is not established at its source.

All these unique risks should form a basis for assessing the controls needed and the effectiveness of these controls to mitigate these risks on implementation.

Components of Control System

3.2 There are four major components of control system in an e-commerce environment:

a) ***Security -*** Controls with respect to confidentiality, integrity, availability, accountability and non-repudiation of information.

b) ***Application integrity -*** Controls to ensure integrity of transaction processing at application level like, implementation of firewall, validation of critical data at application level, existence of audit trails, exception monitoring and reporting, customer confirmation, controls on data transmission and reception and backup and recovery controls.

c) ***Development Process*** **-** Controls on development process of e-commerce application including policies and procedures, application design, testing, change management, data conversion and implementation/roll outs.

d) ***Process Control* -** Controls on for controlling the output whether the input data are being correctly routed through the architectural framework of e- commerce.

3.3 The control system would help in yielding reliable information when they meet the following security requirements:

a) ***Integrity*** - This requirement is fulfilled for an IT system when data and information are complete and accurate, systems are complete and appropriate and all of these are protected against unauthorized modification and manipulation. Appropriate testing and release procedures are typical means by which the integrity of data, information and systems can be ensured. Technical measures to achieve this include firewalls and virus scanners. The reliability increases when the IT infrastructure and the data, information and IT applications are used in a specified configuration and only authorized modifications are permitted.

b) ***Availability*** - Under this requirement, the enterprise ensures the constant availability of the hardware, software, data and information to maintain business operations and that the hardware, software, data, information and the requisite IT organization can be made operable within a reasonable period of time (e.g., after an emergency interruption). It is important, therefore, to establish appropriate back-up procedures for emergencies. In addition, the ability to convert digitally maintained books and records into human-readable format within a reasonable period of time is essential.

c) ***Confidentiality*** - This requirement means that data obtained from third parties should not be transmitted or disclosed without authorization. Organizational and technical measures, such as encryption technologies, instructions to restrict the transmission of personal data to third parties, transmit encrypted data to authorized third parties, identify and verify the recipient of data and to delete stored personal data after a certain length of time.

d) ***Authenticity*** - This requirement relates to the traceability of a business transaction to the individual who initiated it. This can be done by, for example, using an authorization procedure. When data or information are exchanged electronically, it is important that the other party be identified or is identifiable e.g., by using digital signature procedures. It may be convenient to use shared external or independent facilities (e.g., trust centers) for this purpose.

e) ***Authorization -*** This requirement means that only certain persons, appointed in advance (so called authorized persons), may access certain data, information and systems (e.g., password protection) and that only authorized persons can use the rights defined for this system. This includes reading, creating, modifying and deleting data or information or the administration of an IT system. Useful methods to achieve this are physical and logical security procedures.

f) ***Non-repudiation*** - This requirement is defined as the ability of IT-aided procedures to bring about desired legal consequences with binding effect. It should be difficult for the person initiating the transaction to deny its validity on the grounds that the transaction was unintended or unauthorized. The use of public key systems can help prevent repudiation.[1]

E-security

3.4 E-security refers to the process of ensuring the confidentiality, integrity, and availability of electronic information and protecting it against malicious attackers who could use or alter the information to disrupt critical national infrastructure and industry.

3.5 The thirteen layers of e-security[2] covers both the hardware and software pertaining to network infrastructures. These thirteen layers comprise a matrix, which manages the externalities associated with open architecture environments:

a) ***Risk Management*** - A broad based framework for managing assets and relevant risks to those assets.

b) ***Policy Management*** - A program should control entity policy and procedural guidelines vis-à-vis employee computer usage.

c) ***Cyber-Intelligence*** - Experienced threat and technical intelligence analysis regarding threats, vulnerabilities, incidents, and countermeasure should provide timely and customized reporting to prevent a security incident before it occurs.

---

1 The primary advantage of public key cryptography is that private keys never need to be transmitted. A sender cannot repudiate a message by claiming the key was compromised during transmission by the other party. Users have sole responsibility for protecting their private keys.

2 World Bank publication – "Electronic Security: Risk Mitigation in the Financial Transactions".

d) ***Access Controls/Authentication*** - Establish the legitimacy of a node or user before allowing access to requested information. The first line of defense is access controls; these can be divided into passwords, tokens, biometrics, and public key infrastructure (PKI).

e) ***Firewalls*** - Create a system or combination of systems that enforces a boundary between two or more networks.

f) ***Active content filtering*** - At the browser level, it is prudent to filter all material that is not appropriate for the workplace or that is contrary to established workplace policies.

g) ***Intrusion detection system (IDS)*** - This is a system dedicated to the detection of break-ins or break-in attempts, either manually or via software expert systems that operate on logs or other information available on the network. Approaches to monitoring vary widely, depending on the types of attacks that the system is expected to defend against, the origins of the attacks, the types of assets, and the level of concern for various types of threats.

h) ***Virus scanners*** - Worms, Trojans, and viruses are methods for deploying an attack. Virus scanners hunt malicious codes, but require frequent updating and monitoring.

i) ***Encryption*** - Encryption algorithms are used to protect information while it is in transit or whenever it is exposed to theft of the storage device (e.g., removable backup media or notebook computer).

j) ***Vulnerability testing*** - Vulnerability testing entails obtaining knowledge of vulnerabilities that exist on a computer system or network and using that knowledge to gain access to resources on the computer or network while bypassing normal authentication barriers.

k) ***Systems administration*** - This should be complete with a list of administrative failures that typically exist within financial institutions and corporations and a list of best practices.

l) ***Incident response plan (IRP)*** - This is the primary document used by a corporation to define how it will identify, respond to, correct, and recover from a computer security incident. The main necessity is to have an IRP and to test it periodically.

m) ***Wireless Security*** - This section covers the risks associated with GSM, GPS and the 802.11 standards.

Technology Considerations

4.1 Various types of e-commerce applications and technologies are being used by the organizations to increase scope of business. As a result, business processes have become more complex than ever. In such a scenario auditor may also consider factors enumerated in the following paragraphs during its risk assessment process. It may be noted that the points discussed below are not exhaustive. New methods for building and running websites are constantly evolving, and the specific technology used may differ greatly from one organization to the next. For these reasons, if required, the auditor may involve an expert or specialist as an effort to consider key control issues.

Identification, Authentication and Authorization

4.2 *Identification* is the process of providing unique credentials to an individual for usage of the respective system e.g., user name or user ID provided to a user of the system. *Authentication* is the process of identifying an individual, usually based on a username and password. Authentication is distinct from *authorization*, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. The use of passwords, tokens (such as smart cards), digital certificates or biometrics (more commonly fingerprint, hand geometry and voice biometrics) are used to verify the identity of a user. Most computer security systems are based on a two-step process. The first stage is authentication, which ensures that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user's identity.

4.3 Strong customer identification and authentication processes are also important in the cross-border context given the difficulties that may arise from doing business electronically with customers across national and international borders, including the risk of identity impersonation and the difficulty in conducting effective credit checks on potential customers. Auditor should ensure that all the users have been uniquely identified in the system and suitable and adequate procedures to authenticate the users of the system have been implemented. Auditor should also ensure that all the users have been granted access (authorization) to various resources on a *'need to know'* and *'need to do'* basis. Auditor should also ensure that sufficient controls exist in the organization for potential areas of vulnerability and periodic reviews of all users and authorizations granted to them is carried out by the management.

Alignment of Business Processes

4.4 An e-commerce transaction may travel though a series of applications and systems from the stage of initiation to its completion. For example, a customer may enter a transaction using organization’s website. The transaction may then be passed to application system by the web server. Finally, the application system may pass the transaction to the accounting system. In an e-commerce environment, it is important that the transactions generated from the website are processed properly by the internal systems (such as accounting system, inventory management system, etc.). In case the transactions are not properly captured and transferred to other interconnected systems, it may affect:

a) The completeness and accuracy of transaction processing and information storage;

b) The timing of recognition of sales revenue, purchases and other transaction; and

c) Identification and recording of disputed transactions.

Therefore, the auditor may consider controls over integration of various internal systems and applications involved in the processing of transactions. Further, the auditor should also consider controls over systems changes and data conversion to automate process alignment.

Internet Technology

4.5 Keeping in view the exposure created by internet in e-commerce transactions, auditor may examine following internet specific considerations having impact on risk assessment:

a) ***Plug-ins, Programs, and Components*** - Organization should utilize the most commonly used plug-ins for their site's supported browsers. Use of internally developed or custom plug-ins may not be practical when a commercially available plug-in exists.

b) ***Browsers*** - Organization should consider the importance of building applications that can run on current and past versions of the most popularly used browsers like, Netscape Navigator, Microsoft Internet Explorer, etc.

c) ***Internet Service Providers (ISPs)*** - If the organization internally develops portal and supporting infrastructure, it is advised to consider making it the standard for hosting all applications. If business requires the use of an external Internal Service Provider (ISP), it should consult the information security team early in the project development process to ensure that the ISP does not breach the company's firewall security.

d) ***Cookies and Push Technology*** - Organization should have a company policy regarding the use of cookies and push technology. The auditor may also discuss the policy regarding information gathered via cookies, as well as the use of push technology, with the organization’s legal department to prevent violations of local legislations.

Application Development and Change Management Process

4.6 In an e-commerce environment, practices for developing e-commerce applications and change management thereof do not differ greatly from those associated with other types of systems, except that "time to development/changes" is generally much shorter. The need to enter the market quickly shortens e-commerce development life cycles. In this regard, the auditor should consider following:

a) ***Policies and Standards*** - Organization should have internal policies and standards regarding information security and application development.

b) ***Application Design*** - Auditor should verify controls in place to ensure application design is reviewed before coding begins.

c) ***Testing*** - Adequate controls should be in place to ensure web applications testing, which covers unit, system, integration, and user acceptance testing.

d) ***System Performance*** - Adequate controls should be in place to ensure developers test and monitor system performance, resolving any problems with network engineering promptly.

e) ***Change Management*** - Change Management Process of adherence to program change management procedures should be in place.

f) ***Capacity Planning and Management*** - Auditor should ensure that planning for future capacity growth has been carried out during the systems planning phase.

g) ***Data Conversion*** - Auditor should ensure that a data conversion plan that is tested and approved by users has been developed by the organization.

h) ***Implementation/Rollout*** - Auditor should ensure that there is a detailed rollout plan subject to review and approval by users before rollout is generated.

Storage of Information

4.7 Information takes many "states" within an e-commerce environment. Data "at rest" can be found stored on mainframes, web servers or even proliferated to an infinite number of desktops. The same information can be stored to back-up tapes at off-site storage facilities or even on CDs and USB drives. In an e-commerce environment, as information moves through operational processes both within and outside the enterprise, it becomes data "in transit." Data moves throughout the enterprise from one computing platform to another. Data on the mainframe can be sent to servers or desktops and vice versa.

4.8 Auditor should consider if a suitable and secure encryption mechanism has been implemented by the organization to ensure 'integrity' of the data during its all states. It will ensure that only authorized information is stored in the systems and the stored information is protected from unauthorized changes. The common thread in most legislation today is that customer data must be vigilantly protected. Therefore, the auditor should also consider confidentiality aspect of information by considering access control mechanism implemented in the organization.

Non-Repudiation

4.9 In an e-commerce environment non-repudiation means to ensure that a transferred electronic message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Non-repudiation can be obtained through the use of:

a) ***Digital signatures*** - function as a unique identifier for an individual, much like a written signature.

b) ***Confirmation services*** - the message transfer agent can create digital receipts to indicate that messages were sent and/or received.

c) ***Timestamps*** - timestamps contain the date and time a document was composed and proves that a document existed at a certain time.

Business Continuity Planning

4.10 E-commerce information is a valuable asset and must be thoroughly protected, along with ensuring the ability to resume business operations should an incident occur. The threats related to Information Technology may be classified as follows:

(a) ***Physical threats*** are those that result from physical access or damage to information resources such as servers, network equipment, computer rooms, etc.

(b) ***Logical threats*** are those that allow information to be compromised without needing the physical presence of a person, e.g., via the Internet.

(c) ***Technical failure*** is a common threat for IT systems. For example, if key data is stored only on the hard disk of one server then the failure of that hard disk would be catastrophic.

(d) ***Infrastructure failure*** can be a subtle form of threat. For example, if business relies on Internet connection to receive orders from customers, it could miss out on new purchase orders if that connection fails.

(e) ***Human error*** is major threat. If an honest mistake by a user or system manager could cause an irrevocable loss of data, action needs to be taken to prevent it from happening

4.11 Thus, to manage the associated risks rigorous business continuity planning is essential. Business continuity planning is the process of planning for the unexpected. An effective plan will provide procedures to minimize the effects of the unexpected disruptions. For this purpose, the auditor should ensure that suitable security, availability and recovery procedures have been designed and are operating effectively. Further, the auditor should also ensure that the organization has tested the Business Continuity Plan to ensure that it has covered all the angles and also whether the plan is achievable.

Audit Considerations in an E-commerce Environment

5.1 The advent of web-based ordering and operating systems increases the challenges many auditors face when auditing clients who are adopting e-commerce strategies. E-commerce produces new and more complex value added models and in this process several integrated applications are developed and deployed at a rapid pace. Therefore, it is important for the auditor to understand the extent of dependence of the business on e-commerce and also its impact both on the business model and operations. For example, e-commerce might be used to:

- Provide only information about the entity and its activities, which can be accessed by third parties such as investors, customers, suppliers, finance providers, and employees;
- Facilitate transactions with established customers whereby transactions are entered via the Internet;
- Gain access to new markets and new customers by providing information and transaction processing via the internet;
- Access Application Service Providers (ASPs); and
- Create an entirely new business model.

At an organizational level the auditor would need to understand what business activities and processes have been replaced by e-commerce and what risks do these changes pose. Further, the new processes/activities and technology that have been introduced bring their own set of issues relating to risks and controls and need to be properly understood and addressed.

Skills and knowledge

5.2 Auditor should have sufficient knowledge of the business of the organization and the industry in which the organization operates. Relevant industry factors include industry conditions such as the competitive environment, supplier and customer relationships, and technological developments. In addition to business knowledge auditor should have appropriate knowledge of Information Technology. This will help auditor to:

- Determine the extent and complexity of e-commerce activities in the organization;
- Understand e-commerce strategy of the organization,
- Determine nature, timing and extent of audit procedures.

5.3 With the growing complexity of Information and Internet technology, e-commerce to date has created a basis for new markets and products, as well as customer empowerment. Developments in web technology have opened communication among platforms, networks, and end users, representing a major step forward from the more insular systems of the past. However, the same technology that enables this increased interconnectivity has also introduced numerous opportunities for control breaches.

In such a scenario organization's e-commerce activities may be operating in a more complex environment. To address key control issues, auditor may decide to use the work of an expert to obtain sufficient and appropriate audit evidence for the purpose of the audit. For example, the work of an expert may be used to understand the risks in e-commerce activities, to test technical controls, analysis of audit trails and key transactions, etc. As mentioned earlier, it would be important to give consideration to use of specialists (e.g., IT auditors) to ensure that risks have been identified and addressed appropriately in the audit. If the use of such a professional is planned, the auditor should, in accordance with SA 620, “Using the Work of an Expert”, obtain sufficient appropriate audit evidence that the work performed by the expert is adequate for the purposes of the audit

Legal considerations

5.4 Legal frameworks in different jurisdictions vary in their recognition of e-commerce. Nonetheless, management needs to consider legal and regulatory issues related to the entity’s e-commerce activities, for example, whether the entity has adequate mechanisms for recognition of taxation liabilities in various jurisdictions or documentation requirements for order processing and invoices to comply with tax legislation. Factors to be considered include the place where:

a) The entity is legally registered;

b) Its physical operations are based;

c) Its web server is located;

d) Goods and services are supplied from; and

e) Its customers are located or goods and services are delivered.

These all may be in different jurisdictions. Without understanding the regulations and the law applied in different jurisdictions, organizations may be subject to fines and adverse judgments and may incur other costs, such as legal fees to defend themselves in case they inadvertently breach such laws. This may also give rise to a risk that taxes due on cross-jurisdictional transactions are not appropriately recognized.

5.5 Legal or regulatory issues that may be particularly relevant in an e-commerce environment include:

a) Adherence to national and international privacy requirements;

b) Adherence to national and international requirements for regulated industries;

c) The enforceability of contracts;

d) The legality of particular activities, for example Internet gambling;

e) The risk of money laundering; and

f) Violation of intellectual property rights.

5.6 Standard on Auditing (SA) 250 "Consideration of Laws and Regulations in an Audit of Financial Statements" deals with the auditor's responsibilities relating to laws and regulations when performing an audit of financial statements. The auditor should obtain a general understanding of:

(a) The legal and regulatory framework applicable to the entity and the industry or sector in which the entity operates; and

(b) How the entity is complying with that framework.

After obtaining the above general understanding, the auditor shall obtain sufficient appropriate audit evidence regarding compliance with those laws and regulations generally recognized by the auditor to have a direct effect on the determination of material amounts and disclosures in the financial statements

5.7 While an audit cannot be expected to detect non-compliance with all laws and regulations, the auditor is specifically required to perform procedures to help identify instances of non-compliance with those laws and regulations where non-compliance should be considered when preparing financial statements. When a legal or regulatory issue arises that, in the auditor's judgment, may result in a material misstatement of the financial statements or have a significant effect on the auditor's procedure or the auditor's report, the auditor considers management's response to the issue. In some cases, the advice of a lawyer with particular expertise in e-commerce issues may be necessary when considering legal and regulatory issues arising from an entity's e-commerce activity.

5.8 Auditor may consider provisions of Information Technology Act, 2000 including that related to following:

a) Legal recognition of electronics records;

b) Legal recognition of digital signatures;

c) Use of electronic records and digital signatures in Government and its agencies;

d) Retention of electronic records;

e) Attribution, Acknowledgement and Despatch of Electronic records;

f) Provision for certifying authorities and Subscribers in connection with digital signature; and

g) Provision for penalties for cyber offences.

The text of The Information Technology Act, 2000 is given in Appendix B of the Technical Guide.

Audit Planning

5.9 Standard on Auditing (SA) 300 "Planning an Audit of Financial Statements" lays down that the auditor should plan the audit so that the audit will be performed in an effective manner. In an e-commerce environment, while establishing the overall audit strategy the auditor should consider the effect of information technology on the audit procedures, including the availability of data and the expected use of computer assisted audit techniques.

5.10 In an e-commerce environment the entries in accounting records are often initiated, recorded, processed and reported in electronic form. Accordingly, the auditor should consider the following points during the planning stage:

a) Scope in e-commerce environment e.g., understanding of flow of accounting transactions, records and information, location where the related system are hosted, interfacing of accounting systems with other systems, reporting requirements, etc.

b) Identification of key risk areas with respect to e-commerce environment and plan to address these areas to reduce the risk at acceptable low levels.

c) Request for report of internal audit, if any, covering the e-commerce activities. The considerations in such report may be included in the audit plan by the auditor.

d) Understanding of internal controls instituted by the management with respect to e-commerce activities.

e) Develop and document an e-commerce audit plan as a part of overall audit plan.

f) Keeping in view complexity and specific environment of information technology set up, audit plan should include deployment of appropriate experienced team members.

g) Timing of audit e.g., interim reviews or final reviews with regard to e-commerce activities.

Risks and Control System

5.11 Standard on Auditing (SA) 315 “Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and its Environment” lays down that the auditor should identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertions levels, through understanding the entity and its environment, including the entity’s internal control, thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement. This will help the auditor to reduce the risk of material misstatement to an acceptably low level.

5.12 Wherever e-commerce transactions are used for key business processes, there is significant change in the manner in which some of the activities are performed as compared to traditional transactions. This change can introduce risks by (a) eliminating or reducing efficacy of some traditional controls (b) adding new elements like, technology, new activities, legal considerations, etc. which need to be appropriately considered during audit and (c) speeding up transactions which can bring its own issues with cut-offs, period end procedures, etc. In order to identify risks associated with e-commerce transactions, the auditor should analyze the e-commerce application by considering the following factors:

a) Management

b) Technology

c) Human Interface

5.13 Management faces many risks relating to the entity's e-commerce activities, including:

- Loss of transaction integrity;
- Risk of business process failure;
- E-commerce security risks, including virus attacks, unauthorized access;
- Improper accounting policies related to, for example, capitalization of expenditures such as website development costs, misunderstanding of complex contractual arrangements, title transfer risks, translation of foreign currencies, allowances for warranties or returns, and revenue recognition issues such as :
  - Whether the entity is acting as principal or agent and whether gross sales or commission only are to be recognized;
  - If other entities are given advertising space on the entity's web site, how revenues are determined and

settled (for example, by the use of barter transactions);

- The treatment of volume discounts and introductory offers (for example, free goods worth a certain amount); and
- Cut off (for example, whether sales are only recognized when goods and services have been supplied);

- Non-compliance with taxation and other legal and regulatory requirements, particularly when Internet e-commerce transactions are conducted across international boundaries;
- Failure to ensure that contracts evidenced only by electronic means are binding;
- Over reliance on e-commerce;
- Systems and infrastructure failures or “crashes”; and
- Financial risks e.g., foreign exchange risks, credit risk, etc.

5.14 With regard to “Risks arising from IT”, SA 315 lays down that the use of Information technology affects the way control activities are implemented. From the auditor’s perspective, controls over IT systems are effective when they maintain the integrity of information and the security of the data such systems processes, and includes effective general IT controls and application controls.

General IT controls are policies and procedures that relate to many applications and support the effective functioning of application controls. General IT controls that maintain the integrity of information and security of data commonly include controls over the following:

- Data center and network operations
- System software acquisition, change and maintenance
- Program change
- Access security
- Application system acquisition, development and maintenance

Application controls are manual or automated procedures that typically operate at a business process level and apply to the processing of individual applications. Application controls can be preventive or detective in nature and are designed to ensure the integrity of the accounting records. Accordingly, application controls relate to procedures used to initiate, record, process and report transactions or other financial data.

5.15 Matters that may be relevant to the auditor when considering the entity's e-commerce strategy in the context of the auditor's understanding of the control environment, include:

a) Involvement of those charged with governance in considering the alignment of e-commerce activities with the entity's overall business strategy;

b) Whether e-commerce supports a new activity for the entity, or whether it is intended to make existing activities more efficient to reach new markets for existing activities;

c) Sources of revenue for the entity and how these are changing (for example, whether the entity will be acting as a principal or agent for goods or services sold);

d) Management's evaluation of how e-commerce affects the earnings of the entity and its financial requirements;

e) Management's attitude to risk and how this may affect the risk profile of the entity;

f) The extent to which management has identified e-commerce opportunities and risks in a documented strategy that is supported by appropriate controls, or whether e-commerce is subject to ad hoc development responding to opportunities and risks as they arise; and

g) Management's commitment to relevant codes of best practice or web seal programs.

Outsourcing Arrangements

5.16 Sometimes an entity may depend on service organizations such as Internet Service Providers (ISPs), Application Service Providers (ASPs) or data hosting companies to provide many or all of the IT requirements of e-commerce activities. The entity may also use service organizations for various other functions in relation to its e-commerce activities such as order fulfillment, delivery of goods, operation of call centers and certain accounting functions. Standard on Auditing (SA) 402, "Audit Considerations relating to Entities Using Service Organizations" lays down that when an entity uses service organization the auditor may consider how an entity's use of a service organization affects the entity's internal control systems so as to identify and assess the risks of material misstatement and to design and perform further audit procedures.

5.17 In obtaining an understanding of the entity and its environment, the auditor may determine the significance of service organization's activities to the entity and relevance to the audit. Auditor may use the report of the service organization auditor. While doing so, the auditor may consider the professional competence of that auditor in the context of the specific assignment undertaken by the service organization auditor. With respect to involvement of service organizations (third parties), the auditor may also consider the following points:

a) The responsibility for negotiating should be delegated to levels of management and staff that are experienced in the area. Appropriate service-level agreements should be incorporated in the contract, such as the performance of key control processes, compliance with statutory laws and regulations, non-disclosure agreement or provisions for audit rights.

b) Third parties should have the necessary types and levels of insurance or provide appropriate levels of indemnification in the event of a problem.

c) Involvement of legal department while signing the contracts with the service organizations.

d) Service Organization should provide evidences of Business Continuity Plan / Disaster Recovery Plan and Risk Mitigation Plan in order to minimize business risk.

Going Concern

5.18 E-commerce activities in an organization may be complementary to its traditional business. For example, a banking company may use e-commerce for some of its activities (e.g., pay order request, opening of fixed deposit accounts and transfer of funds) in addition to serving its customers by conventional methods. In contrast, e-commerce activities may be a new line of business in the organization or the organization may be carrying out all or significant amount of its business activities through e-commerce e.g., an on-line newspaper which is available free through the website and makes its revenue by selling advertising space on the website. In this context, the auditor should consider effect of entity's dependence on e-commerce activities and on its ability to continue as a going concern. Standard on Auditing (SA) 570, "Going Concern" specifies that when a question arises regarding the appropriateness of the going concern assumption, the auditor should gather sufficient appropriate audit evidence to attempt to resolve, to the auditor's satisfaction, the question regarding the entity's ability to continue operation for the foreseeable future.

5.19 Indications of risk that continuance as a going concern may be questionable could come from the financial statements or from other sources. In an e-commerce environment auditor's consideration may also include the following factors:

a) Robustness of the business model, especially the revenue stream.

b) Ability to attract continued funding from investors especially in the case of continued losses.

c) Fundamental changes in market and/or in technology.

d) Loss of key customers, increase in competitors, cultural differences, etc.

e) Outsourcing arrangements for key e-commerce elements.

f) Allocation of resources and capital.

g) Changes in legislation or government policy.

Audit Evidence

5.20 Electronic records and digital signatures are major shift in business processes. Today, electronic records and digital signatures have legal and commercial equivalence of paper records and written signatures. The Information Technology Act, 2000 gives recognition to electronic records and digital signatures. Therefore, electronic records can be used as audit evidence for the purpose of audit. However, electronic records may be more easily destroyed or altered than paper records without leaving evidence of such destruction or alteration. Electronic audit evidence may include Screen Print, Electronic reports from the auditee's computer system, Audit trails, Access Control List, etc.

For an auditor of financial statements, the objective of audit evidence in e-commerce environment remains same as in the case of non e-commerce environment. However, in an e-commerce environment the audit evidence are mostly in electronic form and, therefore, the auditor should understand and evaluate the effect of electronic records on audit documentation.

5.21 Audit evidence is cumulative in nature and, therefore, it may be noted that electronic evidence does not eliminate the need of paper evidence. In an e-commerce environment it is not necessary for an auditor to gather the audit evidences in electronic form only. Keeping in view the objectivity and availability of audit evidence, it may be gathered either in electronic form or in paper form. In this respect, an auditor may consider following:

a) The scope, objectives, planning, methodology followed for audit and assumptions should be completely documented.

b) Whether the entity's information security policies and security controls as implemented are adequate to prevent unauthorized changes to the accounting system or records, or to systems that provide data to the accounting system.

c) Auditor should enquire and understand how management is gaining comfort on internal controls over financial reporting in an e-commerce environment. In case the auditor finds that internal controls identified by the management are sufficient for the purpose of audit and these internal controls are also operating effectively, auditor may decide to rely upon such internal controls and gather related audit evidence, including electronic audit evidence. In case the auditor finds that the internal controls identified by the management are not sufficient or not operating effectively for the purpose of audit of financial statements, he may decide to obtain additional audit evidence in order to form an opinion on the financial statements.

d) Auditor may consider user of computers to gather, understand, analyse, examine and retain evidences for audit documentation purpose.

e) Integrity of electronic information and records is must to ensure that audit evidence being documented is complete, accurate, valid, sufficient and reliable. Organizations are using increasingly complex software to process and store accounting and business transactions. Therefore, the auditor should consider, understand and evaluate Risks and Control System. This will help ensure the integrity of electronic evidence being documented by the auditor.

f) If the evidence being gathered is in electronic form (i.e., reports, print screens, etc.) then the auditor should gather evidence directly after getting appropriate access to the computer system of the auditee. In case help is taken from the auditee personnel (say, IT or finance team) for gathering of electronic evidence such a process needs to be supervised by an expert possessing such skills, who may either be the auditor's staff or an outside professional engaged by the auditor in order to ensure completeness and accuracy of the evidence gathered.

g) The auditor may test automated controls and control over changes to the electronic information, such as record integrity checks, electronic date stamps, digital signatures and version controls when considering the integrity of electronic evidence.

h) While determining the sufficiency and reliability of electronic information, the auditor may also consider compensatory manual controls in place. For example, depending on the auditor's assessment of automated controls, the auditor may also consider the need to perform additional procedures such as confirming transaction details or account balances with third parties.

Audit Trails

5.22 In an e-commerce environment, employees, customers and providers access services, products and information related to the business. Integrity, confidentiality, efficiency, effectiveness and availability in an e-commerce environment are a prerequisite to ensure that financial records and accounts are sufficiently reliable for reporting. Audit trails are key information to achieve this objective.

5.23 Audit trails may be generated in a variety of systems and equipments. For example, every person who enters the organization's network with a user ID and password is logged and the transactions carried out by the person are recorded for later control. Similarly, an organization may log the customer's transaction from its initiation through collection of the receipt and delivery of the product. Additionally, the organization should keep the security administrator's log because he has the option to assign processing functions, which are assessed as highly confidential to the employees. Furthermore, these tasks should be logged beyond the compensating controls implemented (e.g., dual control).

5.24 Auditor may use audit trails to:

a) Follow the history of a transaction;

b) Investigate the causes when a record is found to be erroneous;

c) Analyze data after massive file destruction;

d) Correctly interpret the file where data damage is program caused;

e) Investigate false information that has been sent to system users; and

f) Monitor procedural violations to highlight possible breaches of security, etc.

Auditor may adopt following strategy to understand the extent of availability and use of audit trails:

a) Interview appropriate management and staff to gain an understanding of the types of audit trails being generated by the applications;

b) Identify information requirements relevant for the business process;

c) Identify inherent IT risks and the overall level of control;

d) Select the audit trails to be reviewed; and

e) Review of audit trails.

Examples of audit trails include - Failed access attempts, Incorrect value assigned to data, Attempts to change restricted data, Excessive use of certain data and Invalid entries in event logs and Transaction logs.

5.25 Auditor may use Computer Assisted Audit Techniques (CAATs) to assess the integrity, effectiveness and efficiency objectives of audit trails. The use of CAATs allows for the complete analysis of audit trails, focusing testing on subsets that appear with errors or irregularities and presenting them in a new format (file or paper). In addition, the following should also be verified by an auditor to ensure integrity, completeness and sufficiency of audit trails:

a) Analyze the security ACL (access control list) assigned to the resources (operating systems generally) where the logs are stored (on-line, off-line, on-site, off-site).

b) Check for existence of policies and procedures about audit trails in applications and products.

c) Review the audit trails towards recreating activity or error analysis as needed.

d) Review the parameters installed in the equipment/software regarding activation/deactivation or deletion.

e) Obtain and assess the risk assessment document for each audit trail generated.

f) Check for the existence of controls over the audit trails considered as highly important with regard to their confidentiality and integrity (e.g., Electronic Fund Transfer systems and their equipment, network, procedures, etc.).

g) Monitor routines to analyze audit trail availability.

h) Review the access control audit trails on the security software or key management reports.

Accounting Policies

5.26 Auditor should examine appropriateness of accounting policies adopted by the organization with respect to its e-commerce activities. These accounting policies may be related to conversion of foreign currencies, capitalization of development cost, revenue recognition, recognition and measurement of cost, disclosures in the financial statements, etc. Accounting Standard (AS) 26 “Intangible Assets” prescribes the accounting treatment for intangible assets. AS 26 also contains illustrative application of the Accounting Standard to Website costs and to Internal Use Computer Software, which can be internally generated or acquired. "Guidance Note on Accounting by Dot-Com Companies" deals with accounting by dot-com companies and other entities engaged in electronic commerce (e-commerce) in respect of certain issues relating to revenue recognition and expense recognition.

Audit Documentation

5.27 Standard on Auditing (SA 230) "Audit Documentation" refers to documentation as "the working papers prepared or obtained by the auditor and retained by him, in connection with the performance of his audit". For documentation of electronic records and evidence auditor should consider the following points:

a) The nature and timing of the audit procedures to be used may be affected by the fact that some of the accounting data and other information may be available only in electronic form. For example, purchase, shipping, billing, cash receipt, and cash disbursement transactions are often consummated entirely by the exchange of electronic messages between the parties. Certain electronic information may exist only at a certain point of time. However, such information may not be retrievable after a specified period of time if files are changed and if backup files do not exist. An organization's data retention policies may require the auditor to request retention of some information for the auditor's review or to perform audit procedures at a time when the information is available.

b) Electronic evidence needs to be preserved electronically by the auditors on their computers for any further reference. Further, measures need to be taken to ensure confidentiality, integrity and availability of such evidence for a period similar to the paper records. In this respect following may be considered by the auditor:

- Enable the determination of when and by whom documentation was created, changed or reviewed;

- Protect the integrity of the information at all stages of the engagement, especially when the information is shared within the engagement team;

- Prevent unauthorized changes to the engagement documentation; and

- Allow access to the engagement documentation by the engagement team and other authorized parties as necessary to properly discharge their responsibilities.

c) There need to be appropriate controls over access to such evidence and eventual destruction after the expiry of the retention period otherwise they could lead to unintentional destruction of evidence or a risk to confidentiality.

d) Enable the retrieval of, and access to, the documentation during the retention period, particularly in the case of electronic documentation since the underlying technology may be upgraded or changed over time.

Appendix A

Glossary of Terms

Application Development Process

Processes to plan, design, develop, test and implement an application system or a major modification to an application system. It considers matters such as: appropriate controls are designed into the system; the application will process information in a complete, accurate and reliable manner; the application will function as intended; the application will function in compliance with any applicable statutory provisions; the system is developed in compliance with the established systems development life cycle process, etc.

Application Service Provider (ASP)

Application Service Provider (ASP) is a third-party entity that manages and distributes software-based services and solutions to customers across a wide area network from a central data center. A common example is a website that other websites use for accepting payment by credit card as part of their on-line ordering systems.

Access Control List

In computer environment, Access Control List is an internal computerized table of access rules regarding the levels of computer access permitted to users and computer terminals. ACL is a set of data that informs a computer's operating system permissions, or access rights that each user or group has to a specific system object, such as a directory or a file. Each object has a unique security attribute that identifies which users have access to it, and the ACL is a list of each object and user access privileges such as read, write or execute.

Audit Trail

A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source. It's an electronic or paper log used to record a sequence of events from which a history may be reconstructed. For example, a record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions.

Browser

A user interface on a computer that allows navigation of objects. For e.g., Web browser used to access the world wide web, File browser for managing files and related objects, etc.

Computer Assisted Audit Techniques (CAATs)

Computer Assisted Audit Techniques (CAATs) are audit tests performed by or with software, rather than manually, and are important tools for the auditor in performing audits. CAATs tools may include generalized audit software, random number generator, etc. CAATs may use any automated audit technique, such as Random sampling (with physical verification), age analysis, gap analysis, duplicate analysis and data stratification.

Generally, CAATs allow the auditor to access data without dependence on the client's system, test the reliability of client software, and perform audit tests more efficiently.

CAATs may be used in performing various audit procedures including:

- Tests of details of transactions and balances

- Analytical review procedures
- Compliance tests of IT General Controls
- Compliance tests of Application Controls.

Cookies

A small file or part of a file stored on a world wide web user's computer, created and subsequently read by a website server, and containing personal information (like, user identification code, customized preferences, or a record of pages visited). It is also commonly referred to as HTTP cookies, web cookies, tracking cookies.

Change Management Process

It is control over the IT process of managing changes that satisfies the business requirement to minimize the likelihood of disruption, unauthorized alterations and errors. It is enabled by a management system which provides for the analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure. The main activities under the process includes identify, analyze and approve change requests, defining changes, design and development, testing, implementation and post implementation review.

Digital Signature

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The sender cannot easily repudiate it later.

A scanned written signature is not a digital signature.

Domain Name

The unique name that identifies a computer or computers on the Internet. These names appear as a component of a website's URL.

Extranet

Extranet, a very popular means for business partners to exchange information is partially accessible to authorized outsiders. Briefly, it can be understood as a private intranet mapped into the internet or some other transmission system not accessible to the general public, but is managed by more than one administrator(s). An extranet provides various levels of accessibility to outsiders.

Electronic Funds Transfer (EFT)

Electronic Funds Transfer (EFT) refers to the computer-based systems used to perform financial transactions electronically. It is a system of transferring money from one bank account directly to another without any paper money changing hands and includes any transfer of funds initiated through an electronic terminal, including credit card, ATM and point-of-sale (POS) transactions, electronic check clearing, etc.

Electronic Data Interchange (EDI)

Electronic Data Interchange (EDI) is a set of standards for structuring information to be electronically exchanged between and within businesses, organizations, government entities and other groups. The standards describe structures that emulate documents, for example purchase orders to automate purchasing. The term EDI is also used to refer to the implementation and operation of systems and processes for creating, transmitting and receiving EDI documents.

Firewall

Firewall can be computer hardware or software, or a combination of both, that prevents unauthorized access to organization's data by outside users. In the normal course of business, organization may receive information to its computer network from outside networks\internet or send information to outside networks\internet from its computer network. All information entering or leaving the company's computer network passes through the firewall, which examines the information and blocks those that do not meet the specified security criteria. In other words, a firewall regulates some of the flow of traffic between computer networks of different trust levels.

With emergence of new technologies like, e-procurement, e-sourcing where organization's system, network, processes are made available to outside people, the risk of unauthorized access to organization's data arises. In such an environment, firewall has been developed to mitigate the risk of unauthorized access form outside users. Several vendors have developed their firewall products which an organization may purchase and use to protect its computer network.

Internet

Internet is a worldwide, publicly accessible series of interconnected computer networks - a network of networks - in which users at any one computer can, if they have permission, get information from any other computer. It is the world's largest network. It is capable of exchanging mail and data through a common addressing and naming system based on TCP/IP protocols.

Internet Service Provider (ISP)

Internet Service Provider (ISP) is a business or organization that provides to consumers access to the Internet and related services. It is also known as Internet access provider or IAP. In addition to Internet access via various technologies such as dial-up and DSL (Digital Subscriber Line), they may provide a combination of services including domain name registration and hosting, web hosting, internet transit, etc.

Non-repudiation

Non-repudiation is the concept of ensuring that a contract cannot later be denied by either of the parties involved. In regard to computer environment, non-repudiation means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively. In other words, non-repudiation of origin proves that data has been sent, and non-repudiation of delivery proves that it has been received.

On-line/Off-line

On-line or off-line are states or conditions of a device or equipment or of a functional_unit. To be considered on-line, a device must be either:

- Under the direct control of another device; or
- Under the direct control of the system with which it is associated; or
- Available for immediate use on demand by the system without human intervention; or
- Connected to a system, and is in operation; or

- Functional and ready for service,

while a device that is off-line is not.

On-site/Off-site

On-site is place where organization's server, application and other IT facilities are installed. Off-site is the opposite of on-site where IT facilities including servers, application, etc may or may not be installed and it can be a remote location.

Password

In computer environment, password means a sequence of characters, often along with a user name, that one must input to gain access to a file, application, or computer system. Passwords are a popular form of authentication. In order to ensure security, when a password is entered, the computer system is careful not to display the password characters on the display screen so that it is kept secret from those not allowed access.

Plug-ins

A hardware or software module that adds a specific feature or service to a larger system. Plug-in help the browser perform specific functions like, viewing special graphic formats or playing multimedia files. For example, there are number of plug-ins for the Netscape Navigator browser that enables it to display different types of audio or video messages. Other examples include Adobes Acrobat Reader, Real Networks' streaming video player, etc.

Proxy Server

A server that catches web content in order to provide quicker access for users when new requests are made for the same content.

Time Stamp

A scheme that records the day and time when something is received, modified, or accessed, such as a document. It registered the date and time of such event in electronic form.

Transaction Logs

A transaction log is a history of updates to a database to guarantee recovery of database in case of problems e.g., hardware failure, loss of power, improper backups or improper shutdown, etc. Physically, a log is a file of updates done to the database stored in a stable storage.

Uniform Resource Locator (URL)

An address of a file located on the internet. It is composed of three parts – a protocol, a domain name and a file name.

Website

A Website is a collection of web pages, images or other digital assets that is hosted on one or more web servers, usually accessible via the Internet. All publicly accessible websites are seen collectively as constituting the "World Wide Web". Each Website contains a home page, which is the first document users see when they enter the site.

Web Server

A server process running at a website which sends out web pages in response to requests from person visiting website using remote browsers. Every Web server has an IP address and possibly a domain name. When remote user inputs the website address in web browser, this sends a request to the server whose domain name matches with website address. The server then fetches the page\data and sends it to user's browser. For example, if a person A wants to visit a web site called www.abc.com, A may use Internet Explorer as a web browser and as a response A will be able to view information sent by web server where web pages relating to www.abc.com are stored.

Web Hosting

A term used for storing and maintaining files, e-mail or domains or a server that is connected with internet.

Appendix B

The Information Technology Act, 2000
(No. 21 OF 2000)

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends *inter alia* that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-cased methods of communication and storage of information;

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

BE it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:—

CHAPTER I
PRELIMINARY

1. Short title, extent, commencement and application

(1) This Act may be called the Information Technology Act, 2000.

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

(3) It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.

(4) Nothing in this Act shall apply to, —

(a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;

(b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;

(c) a trust as defined in section 3 of the Indian Trusts Act, 1882;

(d) a will as defined in clause *(h)* of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;

(e) any contract for the sale or conveyance of immovable property or any interest in such property;

(f) any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

2. Definitions

(1) In this Act, unless the context otherwise requires, —

(a) "access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

(b) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(c) "adjudicating officer" means an adjudicating officer appointed under subsection (1) of section 46;

(d) "affixing digital signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

(e) "appropriate Government" means as respects any matter,—

(i) Enumerated in List II of the Seventh Schedule to the Constitution;

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

(f) "asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(g) "Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certificate under section 24;

(h) "certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

(i) "computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

(j) "computer network" means the interconnection of one or more computers through—

(i) the use of satellite, microwave, terrestrial line or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

(k) "computer resource" means computer, computer system, computer network, data,computer data base or software;

(l) "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (l) of section 17;

(n) "Cyber Appellate Tribunal" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;

(o) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

(p) "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

(q) "Digital Signature Certificate" means a Digital Signature Certificate issued under subsection *(4)* of section 35;

(r) "electronic form" with reference to information means any information generated, sent, received or stored in media,

magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(s) "Electronic Gazette" means the Official Gazette published in the electronic form;

(t) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(u) "function", in relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(v) "information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche:

(w) "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

(x) "key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

(y) "law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, byelaws and orders issued or made thereunder;

(z) "licence" means a licence granted to a Certifying Authority under section 24;

(za) "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(zb) "prescribed" means prescribed by rules made under this Act;

(zc) "private key" means the key of a key pair used to create a digital signature;

(zd) "public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(ze) "secure system" means computer hardware, software, and procedure that—

(a) are reasonably secure from unauthorised access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures;

(zf) "security procedure" means the security procedure prescribed under section 16 by the Central Government;

(zg) "subscriber" means a person in whose name the Digital Signature Certificate is issued;

(zh) "verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether—

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the

corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

CHAPTER II
DIGITAL SIGNATURE

3. Authentication of electronic records.

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation.—For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known'as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

CHAPTER III
ELECTRONIC GOVERNANCE

4. Legal recognition of electronic records.

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

5. Legal recognition of digital signatures.

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (hen, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation.—For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

6. Use of electronic records and digital signatures in Government and its agencies.

(1) Where any law provides for—

(a) the filing of any form. application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe—

(a) the manner and format in which such electronic records shall be filed, created or issued;

(b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause *(a).*

7. Retention of electronic records.

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if—

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

8. Publication of rule, regulation, etc., in Electronic Gazette.

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

9. Sections 6,7 and 8 not to confer right to insist document should be accepted in electronic form.

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

10. Power to make rules by Central Government in respect of digital signature.

The Central Government may, for the purposes of this Act, by rules, prescribe—

(a) the type of digital signature;

(b) the manner and format in which the digital signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the digital signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to digital signatures.

CHAPTER IV
ATTRIBUTION, ACKNOWLEDGMENT AND DESPATCH OF ELECTRONIC RECORDS

11. Attribution of electronic records.

An electronic record shall be attributed to the originator—

(a) if it was sent by the originator himself;

(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(c) by an information system programmed by or on behalf of the originator to operate automatically.

12. Acknowledgment of receipt.

(1) Where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by—

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment

must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

13. Time and place of despatch and receipt of electronic record.

(1) Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely :—

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,—

(i) receipt occurs at the time when the electronic, record enters the designated computer resource; or

(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

(5) For the purposes of this section, —

(a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(c) "usual place of residence", in relation to a body corporate, means the place where it is registered.

CHAPTER V

SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

14. Secure electronic record.

Where any security procedure has been applied to an electronic record at a specific point of time. then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

15. Secure digital signature.

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was—

(a) unique to the subscriber affixing it;

(b) capable of identifying such subscriber;

(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

16. Security procedure.

The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including—

(a) the nature of the transaction;

(b) the level of sophistication of the parties with reference to their technological capacity;

(c) the volume of similar transactions engaged in by other parties;

(a) the availability of alternatives offered to but rejected by any party;

(e) the cost of alternative procedures; and

(f) the procedures in general use for similar types of transactions or communications.

CHAPTER VI
REGULATION OF CERTIFYING AUTHORITIES

17. Appointment of Controller and other officers.

(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

18. Functions of Controller.

The Controller may perform all or any of the following functions, namely:—

(a) exercising supervision over the activities of the Certifying Authorities;

(b) certifying public keys of the Certifying Authorities;

(c) laying down the standards to be maintained by the Certifying Authorities;

(d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;

(g) specifying the form and content of a Digital Signature Certificate and the key,

(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) laying down the duties of the Certifying Authorities;

(n) maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

19. Recognition of foreign Certifying Authorities.

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under subsection (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

20. Controller to act as repository.

(1) The **Controller** shall be the repository of all Digital Signature Certificates issued under this Act.

(2) The Controller shall—

(a) make use of hardware, software and procedures that are secure .iJm intrusion and misuse;

(b) observe such other standards as may be prescribed by the Central Government, to ensure that the secrecy and security of the digital signatures are assured.

(3) The Controller shall maintain a computerised data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

21. Licence to issue Digital Signature Certificates.

(1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a licence to issue Digital Signature Certificates.

(2) No licence shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital Signature Certificates as may be prescribed by the Central Government

(3) A licence granted under this section shall—

(a) be valid for such period as may be prescribed by the Central Government;

(b) not be transferable or heritable;

(c) be subject to such terms and conditions as may be specified by the regulations.

22. Application for licence.

(1) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a licence shall be accompanied by—

(a) a certification practice statement;

(b) a statement including the procedures with respect to identification of the applicant;

(c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(d) such other documents, as may be prescribed by the Central Government.

23. Renewal of licence.

An application for renewal of a licence shall be—

(a) in such form;

(b) accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence.

24. Procedure for grant or rejection of licence.

The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application:

Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

25. Suspension of licence.

(1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has,—

(a) made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;

(b) failed to comply with the terms and conditions subject to which the licence was granted;

(c) failed to maintain the standards specified under clause *(b) of* sub-section (2) of section 20;

(d) contravened any provisions of this Act, rule, regulation or order made thereunder, revoke the licence:

Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1), by

order suspend such licence pending the completion of any inquiry ordered by him:

Provided that no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) No Certifying Authority whose licence has been suspended shall issue any Digital Signature Certificate during such suspension.

26. Notice of suspension or revocation of licence.

(1) Where the licence of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the database maintained by him.

(2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories:

Provided that the data base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock:

Provided further that the Controller may, if he considers necessary, publicise the contents of database in such electronic or other media, as he may consider appropriate.

27. Power to delegate.

The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

28. Power to investigate contraventions.

(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.

29. Access to computers and data.

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person incharge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

30. Certifying Authority to follow certain procedures.

Every Certifying Authority shall, —

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;

(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and

(d) observe such other standards as may be specified by regulations.

31. Certifying Authority to ensure compliance of the Act, etc.

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made thereunder.

32. Display of licence.

Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

33. Surrender of licence.

(1) Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.

(2) Where any Certifying Authority fails to surrender a licence under sub-section (1), the person in whose favour a licence is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

34. Disclosure.

(1) Every Certifying Authority shall disclose in the manner specified by regulations—

(a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;

(b) any certification practice statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall—

(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

CHAPTER VII

DIGITAL SIGNATURE

CERTIFICATES

35. Certifying Authority to issue Digital Signature Certificate.

(1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government

(2) Every such application shall be accompanied by such fee not exceeding twentyfive thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority:

Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants'.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under subsection (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application:

Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that—

(a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(b) the applicant holds a private key, which is capable of creating a digital signature;

(c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant:

Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

36. Representations upon issuance of Digital Signature Certificate.

A Certifying Authority while issuing a Digital Signature Certificate shall certify that--

(a) it has complied with the provisions of this Act and the rules and regulations made thereunder,

(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;

(d) the subscriber's public key and private key constitute a functioning key pair,

(e) the information contained in the Digital Signature Certificate is accurate; and

(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

37. Suspension of Digital Signature Certificate.

(1) Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate,—

(a) on receipt of **a request** to that effect from—

 (i) the subscriber listed in toe Digital Signature Certificate; or

 (ii) any person duly authorised to act on behalf of that subscriber,

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest

(2) A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

(3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

38. Revocation of Digital Signature Certificate.

(1) A Certifying Authority may revoke a Digital Signature Certificate issued by it—

(a) where the subscriber or any other person authorised by him makes a request to that effect; or

(b) upon the death of the subscriber, or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a CertifyingAuthority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that—

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(d) the subscriber has been declared insolvent **or** dead or where a subscriber is a firm or a company, which has been dissolved, wound-up **or** otherwise ceased to exist

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

39. Notice of suspension or revocation.

(1) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may he. in all such repositories.

CHAPTER VIII

DUTIES OF SUBSCRIBERS

40. Generating key pair.

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

41. Acceptance of Digital Signature Certificate.

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate—

(a) to one or more persons;

(b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that—

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

42. Control of private key.

(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by .the regulations.

Explanation.— For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

CHAPTER IX

PENALTIES AND ADJUDICATION

43. Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, —

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.—For the purposes of this section,—

(i) "computer contaminant" means any set of computer instructions that are designed—

   (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

   (b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, daia or instruction is executed or some other event takes place in that computer resource;

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

44. Penalty for failure to furnish information return, etc.

If any person who is required under this Act or any rules or regulations made thereunder to—

(a) furnish any document, return or report to the Controller or? he Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

45. Residuary penalty.

Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

46. Power to adjudicate.

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer'for holding an inquiry in the manner prescribed by the Central Government.

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology

and legal or judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred oh the Cyber Appellate Tribunal under sub-section (2) of section 58, and—

(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code;

(b) shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.

47. Factors to be taken into account by the adjudicating officer.

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely:—

(a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(b) the amount of loss caused to any person as a result of the default;

(c) the repetitive nature of the default

CHAPTER X

THE CYBER REGULATIONS APPELLATE TRIBUNAL

48. Establishment of Cyber Appellate Tribunal.

(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in subsection (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

49. Composition of Cyber Appellate Tribunal.

A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Residing Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government

50. Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal.

A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he—

(a) is, or has been. or is qualified to be, a Judge of a High Court; or

(b) is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years.

51. Term of office

The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

52. Salary, allowances and other terms and conditions of service of Presiding Officer.

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of. the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed:

Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

53. Filling up of vacancies.

If, for reason other than temporary absence, any vacancy occurs in the office n the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

54. Resignation and removal.

(1) The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

Provided that the said Presiding Officer shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

(2) The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.

55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.

No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

56. Staff of the Cyber Appellate Tribunal.

(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

(3) The salaries, allowances and other conditions of service of the officers and employees or' the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

57. Appeal to Cyber Appellate Tribunal.

(1) Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of tony-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of tony-five days if it is satisfied that there was sufficient cause tor not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to" the parties to the appeal and to the concerned Controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

58. Procedure and powers of the Cyber Appellate Tribunal.

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely:—

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses or documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it *ex pane;*

(g) any other matter which may be prescribed.

(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

59. Right to legal representation.

The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

60. Limitation.

The provisions of the Limitation Act, 1963, shall, as far as may be, *apply* to an appeal made to the Cyber Appellate Tribunal.

61. Civil court not to have jurisdiction.

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

62. Appeal to High Court.

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order

Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

63. Compounding of contraventions.

(1) Any contravention under this Chapter may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorised by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded. (2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Explanation.—For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention. (3) Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

64. Recovery of penalty

A penalty imposed under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the licence or the Digital Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

CHAPTER XI

OFFENCES

65. Tampering with computer source documents.

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.—For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

66. Hacking with computer system.

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack:

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

67. Publishing of information which is obscene in electronic form.

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

68. Power of Controller to give directions.

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.

(2) Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a Fine not exceeding two lakh rupees or to both.

69. Directions of Controller to a subscriber to extend facilities to decrypt information.

(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person incharge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.

70. Protected system.

(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

71. Penalty for misrepresentation.

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be. shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72. Penalty for breach of confidentiality and privacy.

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book. register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

73. Penalty for publishing Digital Signature Certificate false in certain particulars.

(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that—

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

74. Publication for fraudulent purpose.

Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

75. Act to apply for offence or contravention commited outside India.

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

76. Confiscation.

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act. rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

77. Penalties or confiscation not to interfere with other punishments.

No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

78. Power to investigate offences.

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

CHAPTER XII

NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

79. Network service providers not to be liable in certain cases.

For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation.—For the purposes of this section, —

(a) "network service provider" means an intermediary;

(b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary;

CHAPTER XIII

MISCELLANEOUS

80. Power of police officer and other officers to enter, search, etc.

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search

and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act

Explanation.—For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

81. Act to have overriding effect.

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

82. Controller, Deputy Controller and Assistant Controllers to be public servants.

The Presiding Officer and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code.

83. Power to give directions.

The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made thereunder.

84. Protection of action taken in good faith.

No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Presiding Officer, adjudicating officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made thereunder.

85. Offences by companies.

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation.—For the purposes of this section,—

(i) "company" means any body corporate and includes a firm or other association of individuals; and

(ii) "director", in relation to a firm, means a partner in the firm.

86. Removal of difficulties.

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of

this Act as appear to it to be necessary or expedient for removing the difficulty:

Provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

87. Power of Central Government to make rules.

(1) The Central Government may, by notification in the Official Gazette and in the Electronic Gazette make rules to carry out the provisions of this Act

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following mailers, namely:—

(a) the manner in which any information or matter may be authenticated by means of digital signature under section 5;

(b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;

(c) the manner and format in which electronic records shall be filed, or issued and the method of .payment under sub-section (2) of section 6;

(d) the matters relating to the type of digital signature, manner and format in which it may be affixed undersection 10;

(e) the security procedure for the purpose of creating secure electronic record and secure digital signature under section 16;

(f) the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers under section 17;

(g) other standards to be observed by the Controller under clause (b) *of* subsection (2) of section 20;

(h) the requirements which an applicant must fulfil under sub-section (2) of section 21;

(i) the period of validity of licence granted under clause (a) of sub-section (3) of section 21;

(j) the form in which an application for licence may be made under sub-section (1) of section 22;

(k) the amount of fees payable under clause (c) of sub-section (2) of section 22;

(l) such other documents which shall accompany an application for licence under clause (a) of sub-section (2) of section 22;

(m) the form and the fee for renewal of a licence and the fee payable there of under section 23;

(n) the form in which application for issue of a Digital Signature Certificate may be made under sub-section (1) of section 35;

(o) the fee to be paid to the CertifyingAuthority for issue of a Digital Signature Certificate under sub-section (2) of section 35;

(p) the manner in which the adjudicating officer shall hold inquiry under subsection (1) of section 46;

(q) the qualification and experience which the adjudicating officer shall possess under sub-section *(3) of* section 46;

(r) the salary, allowances and the other terms and conditions of service of the Presiding Officer under section 52;

(s) the procedure for investigation of misbehaviour or incapacity of the Presiding Officer under sub-section *(3)* of section 54;

(t) the salary and allowances and other conditions of service of other officers and employees under sub-section *(3}* of section 56;

(u) the form in which appeal may be filed and the fee thereof under sub -section (3) of section 57;

(v) any other power of a civil court required to be prescribed under clause *(g)* of subsection (2) of section 58; and

(w) any other matter which is required to be, or may be, prescribed.

(3) Every notification made by the Central Government under clause *(f)* of subsection *(4)* of section 1 and every rule made by it shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the notification or the rule or both Houses agree that the notification or the rule should not be made, the notification or the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification or rule.

88. Constitution of Advisory Committee.

(1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.

(2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.

(3) The Cyber Regulations Advisory Committee shall advise—

(a) the Central Government either generally as regards any rules or for any other purpose connected with this Act;

(b) the Controller in framing the regulations under this Act.

(4) There shall be paid to the non-official members of such Committee such travelling and other allowances as the Central Government may fix.

89. Power of Controller to make regulations.

(1) The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely: —

(a) the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority under clause (m) of section 18;

(b) the conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority under sub-section (1) of section 19;

(c) the terms and conditions subject to which a licence may be granted under clause (c) of sub-section *(3)* of section 21;

(d) other standards to be observed by a Certifying Authority under clause *(d)* of section 30;

(e) the manner in which the Certifying Authority shall disclose the matters specified in sub-section (1) of section 34;

(f) the particulars of statement which shall accompany an application under sub-section *(3)* of section 35;

(g) the manner in which the subscriber shall communicate the compromise of private key to the certifying Authority under sub-section (2) of section 42.

(3) Every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any

modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect only in such modified form or he of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under (hat regulation.

90. Power of State Government to make rules.

(1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely: —

(a) the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6;

(b) for matters specified in sub-section (2) of section 6;

(c) any other matter which is required to be provided by rules by the State Government.

(3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

91. Amendment of Act 45 of 1860.

The Indian Penal Code shall be amended in the manner specified in the First Schedule to this Act.

92. Amendment of Act 1 of 1872.

The Indian Evidence Act, 1872 shall be amended in the manner specified in the Second Schedule to this Act.

93. Amendment of Act 18 of 1891.

The Bankers' Books Evidence Act, 1891 shall be amended in the manner specified in the Third Schedule to this Act.

94. Amendment of Act 2 of 1834.

The Reserve Bank of India Act, 1934 shall be amended in the manner specified in the Fourth Schedule to this Act.

THE FIRST SCHEDULE

(See section 91)

AMENDMENTS TO THE INDIAN PENAL CODE

(45 OF 1860)

1. After section 29, the following section shall be inserted, namely:—

Electronic record.

"29A. The words "electronic record" shall have the meaning assigned to them in clause *(t)* of subsection (1) of section 2 of the Information Technology Act, 2000.".

2. In section 167, for the words "such public servant, charged with the preparation or translation of any document, frames or translates that document", the words "such public servant, charged with the preparation or translation of any document or electronic record, frames, prepares or translates that document or electronic record" shall be substituted.

3. In section 172, for the words "produce a document in a Court of Justice", the words "produce a document or an electronic record in a Court of Justice" shall be substituted.

4. In section 173, for the words "to produce a document in a Court of Justice", the words "to produce a document or electronic record in a Court of Justice" shall be substituted.

5. In section 175, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

6. In section 192, for the words "makes any false entry in any book or record, or makes any document containing a false statement", the words "makes any false entry in any book or record, or electronic

record or makes any document or electronic record containing a false statement" shall be substituted.

7. In section 204, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

8. In section 463, for the words "Whoever makes any false documents or part of a document with intent to cause damage or injury", the words "Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury" shall be substituted.

9. In section 464,—

(a) for the portion beginning with the words "A person is said to make a false document" and ending with the words "by reason of deception practised upon him, he does not know the contents of the document or the nature of the alteration", the following shall be substituted, namely:—

"A person is said to make a false document or false electronic record—

First—Who dishonestly or fraudulently—

(a) makes, signs, seals or executes a document or part of a document;

(b) makes or transmits any electronic record or part of any electronic record;

(c) affixes any digital signature on any electronic record;

(d) makes any mark denoting the execution of a document or the authenticity of the digital signature, with the intention of causing it to be believed that such document or part of document, electronic record or digital signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly—Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly—Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alteration. " ;

(b) after *Explanation* 2, the following *Explanation* shall be inserted at the end, namely:—

'*Explanation 3.*—For the purposes of this section, the expression "affixing digital signature" shall have the meaning assigned to it in clause *(d)* of subsection (1) of section 2 of the Information Technology Act, 2000.'.

10. In section 466,—

(a) for the words "Whoever forges a document", the words "Whoever forges a document or an electronic record" shall be substituted;

(b) the following *Explanation* shall be inserted at the end, namely:—

'*Explanation.*—For the purposes of this section, "register" includes any list, data or record of any entries maintained in the electronic form as defined in clause *(r)* of subsection (1) of section 2 of the Information Technology Act, 2000.'.

11. In section 468, for the words "document forged", the words "document or electronic record forged" shall be substituted.

12. In section 469, for the words "intending that the document forged", the words "intending that the document or electronic record forged" shall be substituted.

13. In section 470, for the word "document" in both the places where it occurs, the words "document or electronic record" shall be substituted.

14. In section 471, for the word "document" wherever it occurs, the words "document or electronic record" shall be substituted.

15. In section 474, for the portion beginning with the words "Whoever has in his possession any document" and ending with the words "if the document is one of the description mentioned in section 466 of this Code", the following shall be substituted, namely: —

"Whoever has in his possession any document or electronic record, knowing the same to be forged and intending that the same shall fraudulently or dishonestly be used as a genuine, shall, if the document or electronic record is one of the description mentioned in section 466 of this Code.".

16. In section 476, for the words "any document", the words "any document or electronic record" shall be substituted.

17. In section 477A, for the words "book, paper, writing" at both the places where they occur, the words "book, electronic record, paper, writing" shall be substituted.

THE SECOND SCHEDULE

(*See* section 92)

AMENDMENTS TO THE INDIAN EVIDENCE ACT, 1872

(1 OF 1872)

1. In section 3,—

(a) in the definition of "Evidence", for the words "all documents produced for the inspection of the Court", the words "all documents including electronic records produced for the inspection of the Court" shall be substituted;

(b) after the definition of "India", the following shall be inserted, namely:— 'the expressions "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000.'.

2. In section 17, for the words "oral or documentary,", the words "oral or documentary or contained in electronic form" shall be substituted.

2. After section 22, the following section shall be inserted, namely: —

When oral admission as to contents of electronic records are relevant.

"22A. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.".

4. In section 34, for the words "Entries in the books of account", the words "Entries in the books of account, including those maintained in an electronic form" shall be substituted.

5. In section 35, for the word "record", in both the places where it occurs, the words "record or an electronic record" shall be substituted.

6. For section 39, the following section shall be substituted, namely:—

What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers.

"39. When any statement of which evidence is given forms part of a longer statement, or of a conversation or pan of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made.".

7. After section 47, the following section shall be inserted, namely: —

Opinion as to digital signature where relevant.

"47A. When the Court has 10 form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact.".

8. In section 59, for the words "contents of documents" the words "contents of documents or electronic records" shall be substituted.

9. After section 65, the following sections shall be inserted, namely:—

Special provisions as to evidence relating to electronic record.

'65A. The contents of electronic records may be proved in accordance with the provisions of section 65B.

Admissibility of electronic records.

65B. (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely: —

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in

whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say, —

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in subsection (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section, —

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.

10. After section 67, the following section shall be inserted, namely:—

Proof as to digital signature.

"67A. Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.".

11. After section 73, the following section shall be inserted, namely:—

Proof as to verification of digital signature.

'73A. In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct—

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.

Explanation.—For the purposes of this section, "Controller" means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 2000'.

12. Presumption as to Gazettes in electronic forms.

After section 81, the following section shall be inserted, namely: —

"81 A. The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody.".

13. Presumption as to electronic aggrements.

After section 85, the following sections shall be inserted, namely: —

"85A. The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

Presumption as to electronic records and digital signatures.

85B. (1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that—

(a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;

(b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

Presumption as to Digital Signature Certificates.

85C. The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.".

14. Presumption as to electronic messages.

After section 88, the following section shall be inserted, namely: —

'88A. The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Explanation.—For the purposes of this section, the expressions "addressee" and "originator" shall have the same meanings respectively assigned to them in clauses *(b)* and (za) of sub-section (1) of section 2 of the Information Technology Act, 2000.'.

15. Presumption as to electronic records five years old.

After section 90, the following section shall be inserted, namely: —

"90A. Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorised by him in this behalf.

Explanation.—Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable.

This *Explanation* applies also to section 81A.".

16. For section 131, the following section shall be substituted, namely: —

Production of documents or electronic records which another person, having possession, could refuse to produce.

"131. No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production."

THE THIRD SCHEDULE

(*See* section 93)

AMENDMENTS TO THE BANKERS' BOOKS EVIDENCE ACT ' 891 (18 OF 1891)

1. In section 2—

(a) for clause (3), the following clause shall be substituted, namely:—

'(3) "bankers' books" include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device;

(b) for clause *(8),* the following clause shall be substituted, namely: — '*(8)* "certified copy" means when the books of a bank,—

(a) are maintained in written form, a copy of any entry in such books together with a certificate written;:: the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank's business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title; and

(b) consist of printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2A.'.

2. After section 2, the following section shall be inserted, namely: —

Conditions in the printout.

"2A. A printout of entry or a copy of printout referred to in sub-section *(8) of* section 2 shall be accompanied by the following, namely: —

(a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and

(b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of—

(A) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;

(B) the safeguards adopted to prevent and detect unauthorised change of data;

(C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;

(D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;

(E) the mode of verification in order to ensure that data has been accurately transferred to such removable media;

(F) the mode of identification of such data storage devices;

(G) the arrangements for the storage and custody of such storage devices;

(H) the safeguards to prevent and detect any tampering with the system; and

(I) any other factor which will vouch for the integrity and accuracy of the system.

(c) a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data.".

THE FOURTH SCHEDULE

(*See* section 94)

AMENDMENT TO THE RESERVE BANK OF INDIA ACT, 1934

(2 OF 1934)

In the Reserve Bank of IndiaAct, 1934, in section 58, in sub-section (2), after clause *(p),* the following clause shall be inserted, namely:—

"(pp) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in clause (c) of section 45-1, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers;".