CH-7 Information Technology Regulatory Issues

The IT Act and its Objectives

Objectives of the Act

To give legal recognition	-to Digital signatures for authentication of any information or matter, which requires authentication under any law. -for keeping of books of accounts by banker's in electronic form. -for transactions carried out by means of EDI and other means of electronic communication.
To facilitate	-electronic filing of documents with Government departments -electronic storage of data -and give legal sanction to electronic fund transfers between banks and financial institutions.

-To amend the IPC, the IEA, 1872, the BBEA, 1891, and the RBI Act, 1934.

Section-3. Authentication of Electronic Records

-any subscriber may authenticate an electronic record by affixing his Digital Signature.

-authentication of the electronic record shall be effected by the use of ACS and HF which envelop and transform the initial electronic record into another electronic record.

"Hash function (HF)" means an algorithm translation of one sequence of bits into another, generally smaller, set known as "Hash Sum" such that an electronic record yields the same hash Sum every time the algorithm is executed with the same electronic record as its input making it computationally infeasible.

-person by the use of a public key of the **subscriber(receiver)** can verify the electronic record.

-private key and the public key are unique to the **subscriber(receiver)** and constitute a functioning key pair.

Section 3A - Electronic Signature

a subscriber(receiver) may authenticate any electronic record by such electronic signature or electronic authentication technique which-

- is considered reliable & specified in the 2nd Schedule.

any electronic signature or electronic authentication technique shall be considered reliable if-

the signature creation data	- are, within the context in which they are used, linked to the signatory or the authenticator and of no other person. - were, at the time of signing, under the control of the signatory or the authenticator and of no other person.
any alteration to the	- electronic signature made after affixing such signature is detectable. -information made after its authentication by electronic signature is detectable.

Legal Recognition of	
Electronic Records -Sec.4	**Electronic Signatures – Sec.5**
Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, such requirement shall be deemed to have been satisfied if such information or matter is - **a.** rendered or made available in an electronic form. **b.** accessible so as to be usable for a subsequent reference.	Where any law requires that any information or matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, such requirement shall be deemed to have been satisfied if such information or matter is authenticated by means of electronic signature affixed. **Explanation: "signed",** with its grammatical variations and related 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 interpreted accordingly.

Section 6 - Use of Electronic Records and Electronic 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 license, permit, sanction or approval by whatever name called in a particular manner.

(c) the **receipt** or **payment** of money in a particular manner, then, 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 **method of payment** of any fee for filing, creation or issue any electronic record under clause (a).

Section.6A - Delivery of services by Service Provider

The Appropriate Government (AG) may, for the purposes of efficient delivery of services to the public through electronic means authorize, by order, any service provider to setup, maintain and upgrade the computerized facilities and perform such other services as it may specify by notification.

Explanation –

For the purposes of this section, service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor firm or any such other body or agency which has been granted permission by the AG to offer services through electronic means in accordance with the policy governing such service sector.

(2) The AG may also authorize any service provider authorized under sub-section (1) to collect, retain and appropriate such service charges, for the purpose of providing such services, from the person availing such service.

(3) the AG may authorize the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e- service charges by the service providers.

Section.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 dispatch or receipt of such electronic record are available in the electronic record.

Section 7A. Audit of Documents, etc. maintained in Electronic form

Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form.

Section 10. Power to make rules by Central Government in respect of Electronic Signature (ES)

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

(a) the type of ES.

(b) the manner and format in which the ES shall be affixed.

(c) the manner or procedure which facilitates identification of the person affixing the ES.

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

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

Section 10A. Validity of contracts formed through electronic means

Where in a contract formation,

the communication of proposals,
the acceptance of proposals,
the revocation of proposals and acceptances,

as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

Section 15. Secure Electronic Signature (ES)

An ES shall be deemed to be a secure electronic signature if-

(i) The signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person.

(ii) The signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Penalties, Compensation and Adjudication

Section 43. Penalty and Compensation for damage to computer, computer system, etc.

Section 43A. Compensation for failure to protect data

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

Section 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 the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding 1 lakh and 50000 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, he shall be liable to a penalty not exceeding 5000 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 10000 rupees for every day during which the failure continues.

Section 45. Residuary Penalty – Compensation 25000/- Penalty 25000/-

Offences

Section 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	Imp-3 Yrs or Fine- 2Lks or both

Section 66 Computer Related Offences	If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with	Imp-3 Yrs or Fine- 5 Lks or both
Section 66A Punishment for sending offensive messages through communication service, etc.	Note: A Division bench of Supreme Court decided on 24th March, 2015 in **Shreya Singhal v. Union of India** to struck down section 66A of Information Technology Act, 2000 as unconstitutional, as it is violative of Article 19(1)(a) related to freedom of speech and expressions. Now comments on social networking sites will not be offensive unless they come under the provisions of the Indian Penal Code, 1860.	
Section 66B Punishment for dishonestly receiving stolen computer resource or communication device	Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with	Imp-3 Yrs or Fine- 1 Lk or both
Section 66C Punishment for identity theft	Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with	Imp-3 Yrs and Fine- 1 Lk
Section 66D Punishment for cheating by personation by using computer resource	Whoever, by means of any communication device or computer resource cheats by personating, shall be punished with	Imp-3 Yrs or Fine- 1 Lk or both
Section 66E Punishment for violation of privacy	Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with	Imp-3 Yrs or Fine- 2 Lk or both
Section 66F Punishment for cyber terrorism	intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people or Whoever commits or conspires to commit cyber terrorism	Life
Section 67 Punishment for publishing or transmitting obscene material in electronic form	Whoever publishes or transmits or causes to be published or transmitted 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	Imp-3 Yrs and Fine- 5 Lk 2nd &…. Imp-5 Yrs and Fine- 10 Lk
Section 67A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form	Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall	Imp-5 Yrs and Fine- 10 Lk 2nd &…. Imp-7 Yrs and Fine- 10 Lk
Section 67B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form		Imp-5 Yrs and Fine- 10 Lk 2nd &…. Imp-7 Yrs and Fine- 10 Lk

Section 67C Preservation and Retention of information by intermediaries		Imp-3 Yrs and Fine
Section 68 Power of the Controller to give directions		Imp-2 Yrs or Fine- 1 Lk or both
Section 69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource		Imp-7 Yrs and Fine
Section 69A Power to issue directions for blocking for public access of any information through any computer resource		Imp-7 Yrs and Fine
Section 69B Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security	Any intermediary who intentionally or knowingly contravenes the provisions of sub - section (2) shall be punished with	Imp- 3 and Fine.
Section 71 Penalty for misrepresentation	Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Electronic Signature Certificate, as the case may be, shall be punished with	Imp- 2 yrs or Fine- 1 lakh or Both
Section 72 Penalty for breach of confidentiality and privacy	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	Imp- 2 yrs or Fine- 1 lakh or Both
Section 72A Punishment for Disclosure of information in breach of lawful contract	has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person	Imp- 3 yrs or Fine- 5 lakh or Both
Section 73 Penalty for publishing Electronic Signature Certificate false in certain particulars	Not issued/not accepted/revoked or suspended	Imp- 2 yrs or Fine- 1 lakh or Both
Section 74 Publication for fraudulent purpose	Whoever knowingly creates, publishes or otherwise makes available an Electronic Signature Certificate for any fraudulent or unlawful purpose	Imp- 2 yrs or Fine- 1 lakh or Both

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

(1) any police officer, not below the rank of an Inspector or any other officer of the Central Government or a State Government authorized 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 of having committed or of committing or of being about to commit any offence under this Act.

"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.

Requirements of Various Authorities for System Controls & Audit

Requirements of IRDA for System Controls & Audit

It focuses on compliance with laws and regulations, which are given as follows:

(i) System Audit

All insurers shall have their systems and process audited at least once in 3 years by a CA firm.

CA firm must be having a minimum of 3-4 year's experience of IT systems of banks or mutual funds or insurance companies.

Who are not eligible: current internal or concurrent or statutory auditor.

(ii) Preliminaries.

Auditor is expected to obtain the following information at the audit location:

-Location(s) from where Investment activity is conducted.
-IT Applications used to manage the Insurer's Investment Portfolio.
-Obtain the system layout of the IT and network infrastructure including:
-Server details, database details, type of network connectivity, firewalls other facilities/ utilities (describe).
-Are systems and applications hosted at a central location or hosted at different office?
-Internal circulars and guidelines of the Insurer.
-Standard Operating Procedures (SOP).
-List of new Products/funds introduced during the period under review along with IRDA approvals for the same.
-Scrip wise lists of all investments, fund wise, classified as per IRDA Guidelines, held on date.

(iii) System Controls

1.There should be Electronic transfer of Data without manual intervention.
All Systems should be seamlessly integrated.
Audit Trail required at every Data entry point.
Procedures for reviewing and maintaining audit trail should be implemented.

2.The auditor should comment on the audit trail maintained in the system for various activities.

The auditor should review the Front Office Systems (FOS), MOS (Mid Office Systems) and BOS (Back Office Systems) and confirm that the system maintains audit trail for data entry, authorization, cancellation and any subsequent modifications.

3. Further, the auditor shall also ascertain that the system has separate logins for each user and maintains trail of every transaction with respect to login ID, date and time for each data entry, authorization and modifications.

Requirements of SEBI for System Controls & Audit

(i) Systems Audit: SEBI had mandated that exchanges shall conduct an annual system audit by a reputed independent auditor.

The Audit shall be conducted according to the Norms, Terms of References (TOR) and Guidelines issued by SEBI.

Stock Exchange/Depository (Auditee) may negotiate and the board of the Stock Exchange / Depository shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR.

The Auditors can perform a maximum of 3 successive audits.

The proposal from Auditor must be submitted to SEBI for records.

Audit schedule shall be submitted to SEBI at-least 2 months in advance, along with scope of current audit & previous audit.

The scope of the Audit may be extended by SEBI, considering the changes which have taken place during last year or post previous audit report Audit has to be conducted and the Audit report be submitted to the Auditee.

The report should have specific compliance/non-compliance issues, observations for minor deviations as well as qualitative comments for scope for improvement.

The report should also take previous audit reports in consideration and cover any open items therein.

The Auditee management provides their comment about the Non-Conformities (NCs) and observations.

For each NC, specific time-bound (within 3 months) corrective action must be taken and reported to SEBI.

The auditor should indicate if a follow-on audit is required to review the status of NCs.

The report along with Management Comments shall be submitted to SEBI within 1 month of completion of the audit.

(ii) Auditor Selection Norms:

Auditor must have minimum 3 years of experience in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc.

The audit experience should have covered all the Major Areas mentioned under SEBI's Audit Terms of Reference (TOR).

The Auditor must have experience in/direct access to experienced resources in the areas covered under TOR.

It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as $(ISC)^2$.

The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like CoBIT.

The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange/Depository.

It should not have been engaged over the last 3 years in any consulting engagement with any departments/units of the entity being audited.

The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

Benefits of ISO 27001

-It can act as the extension of the current quality system to include security.
-It provides an opportunity to identify and manage risks to key information and systems assets.
-Provides confidence and assurance to trading partners and clients; acts as a marketing tool.
-Allows an independent review and assurance to you on information security practices.

Information Technology Infrastructure Library (ITIL)

This release of ITIL V3 brought with it an important change of emphasis, from an operationally focused set of processes to a mature service management set of practice guidance. It also brought a rationalization in the number of volumes included in the set.

1.Service Strategy:

The center and origin point of the ITIL Service Lifecycle, the ITIL Service Strategy (SS) volume, provides guidance on clarification and prioritization of service - provider investments in services.

The Service Strategy volume provides guidance on the design, development, and implementation of service management, not only as an organizational capability, but also as a strategic asset.

It provides guidance on the principles underpinning the practice of service management to aid the development of service management policies, guidelines, and processes across the ITIL Service Lifecycle.

IT Service Generation: IT Service Management (ITSM) refers to the implementation and management of quality information technology services and is performed by IT service providers -

-through People, Process and Information Technology.

Service Portfolio Management: IT portfolio management is the application of systematic management to the investments, projects and activities of enterprise Information Technology (IT) departments.

Financial Management: Financial Management for IT Services' aim is to give accurate and cost effective stewardship of IT assets and resources used in providing IT Services.

Demand Management: Demand management is a planning methodology used to manage and forecast the demand of products and services.

Business Relationship Management: BRM is a formal approach to understanding, defining, and supporting a broad spectrum of inter-business activities related to providing and consuming knowledge and services via networks.

II. Service Design:

Service Design translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations.

It provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners, to present feasible service offerings.

It includes design principles and methods for converting strategic objectives into portfolios of services and service assets.

Service Catalogue Management: It maintains and produces the Service Catalogue and ensures that it contains accurate details, dependencies and interfaces of all services made available to customers.

Service Catalogue information includes ordering and requesting processes, prices, deliverables and contract points.

Service Level Management: It provides for continual identification, monitoring and review of the levels of IT services specified in the SLAs.

It is the primary interface with the customer and is responsible for ensuring that the agreed IT services are delivered when and where they are supposed to be;

liaising with availability management,
capacity management,
incident management and problem management.

Supplier Management: The purpose is to obtain value for money from suppliers and contracts.

It ensures that underpinning contracts and agreements align with business needs, Service Level Agreements and Service Level Requirements.

Supplier Management oversees process of identification of

business needs,
evaluation of suppliers,
establishing contracts,
their categorization,
management and termination.

Availability Management: Availability management targets allow organizations to sustain the IT service-availability to support the business at a justifiable cost.

The high-level activities comprise of realizing availability requirements, compiling availability plan, monitoring availability and maintenance obligations.

Availability management addresses many IT component abilities like reliability, maintainability, serviceability, resilience and security to perform at an agreed level over a period of time.

Capacity Management: Capacity management supports the optimum and cost-effective provision of IT services by helping organizations match their IT resources to business demands.

The high-level activities include

application sizing;
workload management;
demand management;
modelling;
capacity planning;
resource management and performance management.

IT Service Continuity Management: It covers the processes by which plans are put in place and managed to ensure that IT services can recover and continue even after a serious incident occurs.

Information Security Management: It's basic goal is to ensure adequate information security, which in turn, is to protect information assets against risks, and thus to maintain their value to the organization.

This is commonly expressed in terms of ensuring their

confidentiality, integrity and availability,

along with related properties or goals such as authenticity, accountability, non-repudiation and reliability.

III. Service Transition:

Service Transition provides guidance on the service design and implementation ensuring that the service delivers the intended strategy and that it can be operated and maintained effectively.

Service Transition planning provides guidance on managing the complexity of changes to services and service management processes to prevent undesired consequences whilst permitting for innovation.

The Service Transition volume provides guidance on the development and improvement of capabilities for transitioning new and changed services into operations.

Knowledge Management: Knowledge Management (KM) is the process of capturing, developing, sharing, and effectively using organisational knowledge.

It refers to a multi- disciplined approach to achieving organisational objectives by making the best use of knowledge.

Change management and Evaluation: This aims to ensure that standardized methods and procedures are used for efficient handling of all changes.

A change is an event that results in a new status of one or more configuration items (CIs), and which is approved by management, is cost-effective, enhances business process changes (fixes) – all with a minimum risk to IT infrastructure.

Release and Deployment Management: Release and deployment management is used by the software migration team for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure.

Service Transition Planning and Support: This process ensures the orderly transition of a new or modified service into production, together with the necessary adaptations to the service management processes.

Service Asset and Configuration Management: It is primarily focused on maintaining information (i.e., configurations) about Configuration Items (i.e., assets) required to deliver an IT service, including their relationships.

Service Validation and Testing: The objective of ITIL Service Validation and Testing is to ensure that deployed Releases and the resulting services meet customer expectations, and to verify that IT operations are able to support the new service.

IV. Service Operation:

Service Operation provides guidance on the management of a service through its day-to-day production life.

It also provides guidance on supporting operations by means of new models and architectures such as shared services, utility computing, web services, and mobile commerce.

1.Functions:

The major functions are as follows:

(i) Service Desk: service desk is one of four ITIL functions and is primarily associated with the Service Operation lifecycle stage.

Tasks include handling incidents and requests, and providing an interface for other ITSM processes.

Features include Single Point of Contact (SPOC);
Single Point of Entry and Exit; (SPEE)
easier for customers and streamlined communication channel.

(ii) Application management: ITIL application management encompasses a set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects, with particular attention to gathering and defining requirements that meet business objectives.

(iii) IT Operations: IT Operations primarily work from documented processes and procedures and should be concerned with a number of specific sub-processes, such as:

output management,
job scheduling,
backup and restore,
network monitoring/management,
system monitoring/management,
database monitoring/management storage monitoring/management.

(iv) IT Technical Support: IT technical support provides a number of specialist functions:
research and evaluation,

market intelligence,
proof of concept and pilot engineering,
specialist technical expertise, and
creation of documentation.

2. Request fulfillment: It focuses on fulfilling Service Requests, which are often minor changes (e.g., requests to change a password) or requests for information.

3. Incident Management: It aims to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

4.Access Management: It is a process that focuses on granting authorized users the right to use a service, while preventing access to non-authorized users.

5.Event Management: It generates and detects notifications, while monitoring checks the status of components even when no events are occurring.

6.Problem Management: It aims to resolve the root causes of incidents and thus to minimize the adverse impact of incidents caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors.

V. Continual Service Improvement:(CSI)

CSI provides guidance on the measurement of service performance through the service life-cycle, suggesting improvements to ensure that a service delivers the maximum benefit.

This volume provides guidance on creating and maintaining value for customers through improved design, introduction, and operation of services.

It combines principles, practices, and methods from change management, quality management, and capability improvement to achieve incremental and significant improvements in service quality, operational efficiency, and business continuity.

It provides guidance on linking improvement efforts and outcomes with service strategy, design, and transition, focusing on increasing the efficiency, maximizing the effectiveness and optimizing the cost of services and the underlying IT Service Management processes.

IMPORTANT DEFINITIONS

"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

"Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes;

"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.

"Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through-

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

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