

Catalyst Series
ISCA SUMMARY NOTES

**ISCA
Summary
Notes in just
67 Pages**

**Strictly as per
Institute study
material, RTP,
Mock test
Papers**

Wide Range of Diagrams, charts, student friendly presentation

Applicable for Nov 2021 exams & onwards

Chapter 7: Information Technology Regulatory Issues

7.1 Introduction:

This chapter provides the knowledge about various sections of IT Act and its rules as relevant for assurance and assessing the impact of noncompliance. Furthermore, it also provides the knowledge about various regulatory bodies such as RBI, SEBI and IRDA.

7.2 IT Act 2000 and its objectives:

This act provides legal recognition for transactions carried out by means of electronic data interchange. Objective of this act:

CODE	ADVANTAGE OF CIS
Storage of Data	Facilitate electronic storage of the data
Amendment in other laws	This act results in simultaneous amendment following laws. Indian Penal Code, The Indian Evidence Act, 1872, The Banker's book Evidence Act, 1891, Reserve Bank of India, 1934.
Legal Recognition	To grant legal recognition for transaction carried out by means of EDI to digital signatures for authentication, for keeping banking BOA* in electronic form.
E-Filing Facilitation	Facilitate e-filing of documents with government departments.

7.3 Definitions:

Sections/Name	Description
Access	Getting entry into logical, arithmetical or memory function resources of computer or computer network.
Addressee	Means a person who is intended by the originator to receive the electronic records not including any intermediary.
Adjudicating officer	Means officer appointed under section 46(1).
Affixing Electronic signature	Means adoption of any methodology or procedure by a person for the purpose of authenticating ELECTRONIC RECORDS by means of electronic signature.
Appropriate Government	Enumerated in LIST II of seventh Schedule to constitution relating to any state law enacted under LIST III of seventh Schedule to constitution.
Asymmetric crypto system	Means a system of a secure key pair consisting of a PRIVATE KEY for creating digital signature & a public key to verify the digital signature.
Certifying authority	Means a person who has been granted a LICENSE to issue an ELECTRONIC SIGNATURE CERTIFICATE under SECTION 24.
Certificate practice statement	Means a statement issued by a CERTIFYING AUTHORITY to specify the practices that certifying authority employs in issuing electronic signature certificate



Computer	Means Electronic, magnetic, optical & high speed data processing machine that Performs logical, arithmetic & memory functions by manipulating of electronic, magnetic & includes all inputs, output, processing facilities which are connected in a computer system.	
Computer Network	Means interaction of ONE or MORE computers/ computers system/ communication device through use of satellite, microwave, wire/ wireless terminals.	
Computer System	It means a device or a collection of the devices , including input & output devices capable for being used in conjunction with the external files containing computer programs, electronic instructions, input data, that performs logic, arithmetic; data storage & retrieval , communication control & other functions.	
Communication Device	Means cell phone, personal digital assistance or combination of both used to communicate, send or transmit text, audio, video or images.	
Controller	Means controller Of Certifying Authorities appointed under section 17(7).	
Data	Representation of facts, knowledge, concepts, information, instructions which are being prepared in a formalized manner & is intended to be processed in a computer system/ network & may be in any form or stored internally in the memory of the computer	
Cyber café	Means any facility from where access to internet is offered by a person in ordinary course of business.	
Cyber security	Means protecting information, equipment, devices, computer, computer resources, communication device & information stored therein from UNAUTHORISED ACCESS, USE, DISCLOSURE etc.	
Digital signature	Means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the section 3.	
Digital signature certificate	Means protecting information, equipment, devices, computer, computer resources, communication device & information stored therein from UNAUTHORISED ACCESS, USE, and DISCLOSURE etc.	
Electronic Form	With the reference to information means information generated, received, stored in any media, magnetic tape, optical devices, computer memory and micro films.	
Electronic records	Means DATA, RECORDS, IMAGES, SOUND (R.I.D.S.) sent, received and stored in an electronic from.	
Electronic signature	Authentication of any records by a subscriber by means of electronic technique as in 2 nd schedule & include digital signature	
Function	In relation to computer includes Logical, control, communication, arithmetic, retrieval, deletion, storage from or within computers.	
Intermediary	Intermediary with respect to any particular electronic records, means person who on behalf of other receives, stores or transmits those records with respect to that records etc.	
Key pair	1. It is asymmetric crypto system, means 2. Private key & its related public key which are so related that public key can verify a digital signature created by the private key.	

License	1. It means license granted to certifying authority under section 24. Here originator means who Send generates, stores or transmit any electronic, or cause any electronic message to be sent, generated, stored to any person. 2. Prescribed: means prescribed by rules made under this act 3. Private key: Key used to create a digital signature 4. Public key: Key used to verify a digital signature & listed in DSC.								
Secure System	Means computer hardware, software & procedure that:- <table border="1"> <tr> <td>P</td><td>Performing the intended functions</td></tr> <tr> <td>U</td><td>Security from Unauthorized access & misuse.</td></tr> <tr> <td>R</td><td>Reasonable level of Reliability & correct operation.</td></tr> <tr> <td>A</td><td>Adhere to general accepted security procedures.</td></tr> </table>	P	Performing the intended functions	U	Security from Unauthorized access & misuse.	R	Reasonable level of Reliability & correct operation.	A	Adhere to general accepted security procedures.
P	Performing the intended functions								
U	Security from Unauthorized access & misuse.								
R	Reasonable level of Reliability & correct operation.								
A	Adhere to general accepted security procedures.								
Security Procedure	Security procedure prescribed under section 16 by central government								
Subscriber	Means a person in whose name the electronic signature certificate is issued.								
Verify	In relation to a digital signature, electronic records or public key, to determine whether → a. Initial electronic records were affixed with the digital signature by use of private key corresponding to the public key of the subscriber. b. Initial electronic records are retained intact or have been altered since such electronic record was so affixed with the digital signature								

7.4 Digital Signature & Electronic Signature:

CHAPTER II	Creation of digital Signature	(a) Electronic records are converted into message digest by using mathematical functions called hash. (b) Identity of the person affixing the digital signature is authenticated through the use of private key which can be verified by the receiver by using public key corresponding to that private key.
	Section 3 Authentication Of Electronic Records	a) Subject to provisions of this section, any subscriber may authenticate electronic records affixing his digital signature. b) Authentication is affected by use of asymmetric crypto system & hash function which transforms the electronic record in another ELECTRONIC RECORD. c) Any person by use of public key of the subscriber can verify electronic records. d) Private and Public key are unique to subscriber & constitute a functioning key pair.
	Section 3A Electronic Signature	a) Notwithstanding anything contained in section 3,a subscriber may authenticate any electronic records by such electronic signature/ authentication technique which Is considered reliable & May be specified in 2nd schedule. b) Electronic signature/ authentication technique will be considered reliable If: • Any alteration to information made after authentication is detectable. • Any alteration to electronic signature made after affixing is detectable. • Signature creation/authentication data are linked to authenticator & no other person • Signature creation/authentication data at time of signing are under control of the authenticator & no other person. • Other conditions as prescribed c) Central government may prescribe the procedure of ascertaining whether electronic signature is that of person by whom it is supposed to be affixed. d) Central government (Notification in OZ) may add or omit any electronic signature/ authentication. e) Such notification in OZ shall be laid before each house of parliament.



	Section 4 Legal recognition of Electronic Records	Where the law provides that information is to be in written form, and then such requirement shall deemed to be satisfied if such information is: (a) Made available in an electronic form. (b) Accessible So As To Be Usable For A Subsequent Reference	
	Section 5 Legal recognition of digital Signature	Where the law provides that information should be authenticated by affixing the signature of any person then such requirement shall deem to be satisfied if it is authenticated by means of digital signature affixed in such way as CG prescribed.	
	Section 6 Use Of Electronic Records & Signature In Government & Its Agencies	Where any law provides for: (a) Filing of any form, application etc. with office, authority, government agencies in particular manner, (b) Issue/grant of any license, sanction, approvals in a particular manner. (c) Receipt/payment of money in a particular manner. Such requirement shall be deemed to be satisfied if such Filing of any form, Issue/grant of any license, receipt/payment of money is affected by means of electronic form.	
	Section 7 Retention of Electronic Records	Where law provides that documents, records etc. to be retained for specific period, then such requirement shall be deemed to be satisfied if such records are in electronic form: (a) Information contained remains accessible so as to be usable for subsequent reference (b) Electronic records are maintained in the FROMAT IT IS ORIGINAL GENERATED, sent or received. (c) The details which will FACILITATE the identification of the origin, destination, date & time of dispatch of such electronic records are available in ELECTRONIC RECORD.	
	Section 7A Audit of documents etc. in electronic form	Where law provides, there is provision for audit of documents, records & information, then same rule will applicable in respect of electronic form.	
	Section 8 Publication Of Rules, Regulations etc. In Electronic Gazette	Where law provides, that any rules, regulations, order, bye laws have to publish in Official Gazette, then such requirement deemed to be satisfied if such rules, regulations, order, bye laws published in the ELECTRONIC GAZETTE.	
	Section 10 Power To Make Rules By Central Govt	M.	Manner & format in which electronic signature shall be affixed.
		C.	Control processes / procedures to ensure adequate integrity, security & confidentiality of electronic records/payments.
		P.	Procedure which facilitate identification of person affixing electronic signature
		T.	Type of Electronic Signature.
	<u>SECTION 10A</u>	Where in contract formation, the communication of proposal, acceptance of proposal, revocation of proposal and rejection is being expressed in electronic form or by means of an electronic record. So, validity of the contract cannot be questioned only on the ground that electronic form is being used.	

CHAPTER V	Section 14 Secure Electronic Records	Where any security procedure is applied to an electric record at a specific point of time, then such records shall deemed to be secure electronic record from such point of time to time of verification.
	Section 15 Secure Electronic Signature	An electronic signature shall be deemed to be secured if: (a) Signature creation data, at time of fixing signature was under the exclusive control of signatory & no other person. (b) Signature creation data was stored in such manner as prescribed.
	Section 16 Secure procedures & practices	Central government may prescribe the security procedures & practices. It may take into consideration the commercial circumstances, nature of transaction & other related factors.

7.5 Various authorities for system control and audit:

IRDA is the apex body overseeing the insurance business in India. It protects the interests of the policyholders, regulates, promotes and ensures orderly growth of the insurance in India. Information System Audit aims at providing assurance in respect of Confidentiality, Availability and Integrity for Information systems. It also looks at their efficiency, effectiveness and responsiveness. It focuses on compliance with laws and regulations.

RBI is India's central banking institution, which formulates the monetary policy about the Indian rupee. The Reserve Bank of India (RBI) has been at the forefront of recognizing and promoting IS Audit internally and across all the stakeholders including financial institutions. RBI provides guidelines on key areas of IT implementation by using global best practices. They have constituted various expert committees who review existing and future technology and related risks and provide guidelines, which are issued by all stakeholders. Primarily, RBI suggests that senior management and regulators need an assurance on the effectiveness of internal controls implemented and expect the IS Audit to provide an independent and objective view of the extent to which the IT related risks are managed.

(SEBI) is the regulator for the securities market in India. SEBI has to be responsive to the needs of three groups, which constitute the market - The issuers of securities; The investors, and the market intermediaries. Mandatory audits of systems and processes bring transparency in the complex workings of SEBI, prove integrity of the transactions and build confidence among the stakeholders.

7.6 Security Standards:

Information security is essential in the day-to-day operations of enterprises. Any breach of information security might result in adverse effect on the entity. COBIT 5 published by ISACA highlight the need for enterprises to ensure required level of security is implemented. There are many security standards which may ensure protection of vital information of the business. Some of them are:

ITIL : IT INFRASTRUCTURE LIBRARY

It is set of practices for IT Service management (ITSM), That focuses on aligning IT services with the business needs. ITIL describes **procedures, tasks and checklists** that are not organisation specific. Details of ITIL framework:

- 1 - Service strategy
- 2 - service design
- 3 - service transition
- 4 - service operation
- 5 - Continual service improvement

IS 27001

IS 27001 is international best practice and standard for information security management systems (ISMS). It is a systematic approach to manage **confidential or sensitive information**. It consists of **4 phases** that should be implemented in order to minimise the risks:

- Step 1:** THE PLAN PHASE
- Step 2 :** THE DO PHASE
- Step 3 :** THE CHECK PHASE
- Step 4 :** THE ACT PHASE

SA 402

This standard deals with **"Audit Considerations relating to entities using services organizations"**. It deals with aspects like obtaining an **understanding of the services provided by a service organisation including internal controls**, responding to the assessed risks of material misstatement.



PENALTY CHART

PENALTIES & ADJUDICATION	Section 43 Penalties & Compensation For Damage To Computers, Computer System, etc.	If any person without permission of the owner / any other person who is in-charge of computer, computer resources--	
		A	<u>A</u>ccess to computers: Accesses or secure access to such computer, computer resources, computer
		M	<u>M</u>anipulation of information: Destroys, deletes or alters any information in the computer resources, or use it in such a manner that it diminishes/reduces the value of the information
		C	<u>C</u>oncealment of computer resource: Steals, conceals, destroy / or cause any person to steals, conceals, destroy any computer source code with an intention to cause damage.
		D	<u>D</u>ownload of information: Downloads copies or extracts any data, database from such computer, computer resources or computer network.
		V	<u>V</u>irus in computer system: Introduces, or cause to introduce any computer virus/any computer contaminant into any computer system or computer network.
		D	<u>D</u>isruption in computer network: Disrupts or cause disruption of any computer, computer system or computer network.
	Section 44 Penalty For Failure To Furnish Information, Return etc.	Reason Of Penalty Imposition	Amount of Penalty
		Furnish any documents, return or report to the controller or certifying authority, FAILS to furnish the information,	Not exceeding Rs. 1,50,000.00 ≤ 1,50,000.00 [for each failure]
		Return / information not furnished within the time as specified in the regulations	Not exceeding Rs. 50,000.00 ≤ 50,000.00 [for every day during which such failure continues]
	Section 45 Residual Penalty	Book of accounts are not maintained	Not exceeding Rs. 10,000.00 ≤ 10,000.00 [For every day during which such failure continues]
		For which no penalty is separately provided separately.	Not exceeding Rs. 25,000.00 ≤ 25,000.00



OFFENCES CHART

Section No	Nature of Offense	Penalties for Offences									
CODE TO REMEMBER: CD-SR [C.D. of S.I.R.]											
65	Intentionally C oncealment, destroy, alteration any source code, computer program, computer system, network, resources Etc.	Imprisonment / fine 3 years / ₹ 2,00,000 Or both									
66	D amage to computer, computer resources, by doing acts defined in section 43	Imprisonment / fine 3 years / ₹ 5,00,000 Or both									
66A	S ending offensive messages through communication services etc. (a) Info. Having threat character. (b) Info. which is false & is being communicated to cause danger (c) Email send to deceive to mislead the recipient about message origin point	Imprisonment 3 Years and Fine									
66B	R eceiving dishonestly any stolen computer resources or communication devices	Imprisonment / Fine 3 years / ₹ 1,00,000 Or both									
CODE TO REMEMBER: I. -C.V.C											
66C	Identification theft fraudulently by making use of the ELECTRONIC SIGNATURE, PASSWORD	Imprisonment / fine 3 years / ₹1,00,000.00									
66D	Cheating by personation by using computer resources.	Imprisonment / fine 3 years / ₹1,00,000.00									
66E	Violation of the privacy of any person	Imprisonment / Fine 3 years / ₹ 2,00,000 or both									
66F	Cyber Terrorism done with: (a) Intent to threaten integrity of India (b) Intentionally penetrates a computer resources result in damage to property.	IMPRISONMENT LIFETIME									
67	Punishment for publishing or transmitting OBSCENE MATERIAL in electronic form	<table border="1"> <thead> <tr> <th>Conviction</th> <th>Imprisonment</th> <th>Fine</th> </tr> </thead> <tbody> <tr> <td>1st</td> <td>3 YEARS</td> <td>5,00,000</td> </tr> <tr> <td>Subsequent</td> <td>3 YEARS</td> <td>10,00,000</td> </tr> </tbody> </table>	Conviction	Imprisonment	Fine	1st	3 YEARS	5,00,000	Subsequent	3 YEARS	10,00,000
Conviction	Imprisonment	Fine									
1st	3 YEARS	5,00,000									
Subsequent	3 YEARS	10,00,000									
67A	Punishment for publishing or transmitting of MATERIAL contain sexually explicit act etc. in electronic form	<table border="1"> <thead> <tr> <th>Conviction</th> <th>Imprisonment</th> <th>Fine</th> </tr> </thead> <tbody> <tr> <td>1st</td> <td>5 YEARS</td> <td>5,00,000</td> </tr> <tr> <td>Subsequent</td> <td>7 YEARS</td> <td>10,00,000</td> </tr> </tbody> </table>	Conviction	Imprisonment	Fine	1st	5 YEARS	5,00,000	Subsequent	7 YEARS	10,00,000
Conviction	Imprisonment	Fine									
1st	5 YEARS	5,00,000									
Subsequent	7 YEARS	10,00,000									
67B	Punishment for publishing or transmitting of MATERIAL depicting children in sexually explicit act etc. in electronic form.	<table border="1"> <thead> <tr> <th>Conviction</th> <th>Imprisonment</th> <th>Fine</th> </tr> </thead> <tbody> <tr> <td>1st</td> <td>5 YEARS</td> <td>5,00,000</td> </tr> <tr> <td>Subsequent</td> <td>7 YEARS</td> <td>10,00,000</td> </tr> </tbody> </table>	Conviction	Imprisonment	Fine	1st	5 YEARS	5,00,000	Subsequent	7 YEARS	10,00,000
Conviction	Imprisonment	Fine									
1st	5 YEARS	5,00,000									
Subsequent	7 YEARS	10,00,000									
73	No person shall publish the electronic signature certificate to any other person knowing that: (a) Certifying authority listed in the certificate, has not issued it. (b) Subscriber listed in the certificate has not accepted. (c) Certificate has been revoked or suspended	Imprisonment / Fine 2 years / ₹ 1,00,000 or both									



MISCELLANEOUS PROVISIONS

Section Number	Description
Section 68 Power of controller to give directions	Controller may, by order, direct a certifying authority or any employee of such authority to take measures or cease carrying on the activities so as to ensure compliance with the provisions of this act. Any person who intentionally or willingly fails to comply with the orders under sub section 1, shall be guilty of offence and shall be liable to: <u>IMPRISONMENT</u> OR <u>FINE</u> 2 YEARS 1,00,000.00 (Not exceeding) (Not exceeding) OR BOTH
Section 70 Protected System	1. Appropriate government, by notification in official gazette, declares any computer resources which directly or indirectly affects the facility of critical information infrastructure. 2. The appropriate government, by order in writing, authorizes the person who is authorised to access the protected system. 3. If any person tries to access the protected system in contravention of the provisions shall be punishable with imprisonment (Extend up to 10 years) and fine.
Section 80 Power Of Police Officer And Other Officer To Enter, Search Etc.	Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a 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
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 conferred under the Copyright Act 1957 or the Patents Act 1970.
Section 81A Application of the act to electronic cheque and truncated cheque	The provisions of this Act, for the time being in force, shall apply to, or in relation to, electronic cheques and the truncated cheques subject to such modifications and amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 (26 of 1881) by the Central Government, in consultation with the Reserve Bank of India, by notification in the Official Gazette.
Section 84C Punishment For Attempt To Commit Offences	Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both
Section 85 Offences By Companies	Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under 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.

