AUDIT REPORT
OF
REGISTRATION AUTHORITY

Name of the Auditee & Address:

_____

_____

_____

_____

Auditor's Name & Address:

_____

_____

_____

_____

Half-yearly / Annual Audit

Period covered under Audit:

Audit Date(s): _____

Sl. No	Reference	Control Requirement	Description		Observation
1	Rules and Guidelines for RA Office	Registration Authority Officials The RA officials should be officials Preferably not less than the rank of Deputy General Manager (DGM). A letter on official letter head	RA Administrator(s)	M	
			RA Officer(s)	M	

M - Mandatory, O - Optional

		nominating the RA Officials for the bank should be duly signed by the competent authority and the same should be sent to IDRBT. At least two persons are required to be appointed for each RA office (One RA administrator and one/more RA officers). The RA officer must be a person of the rank of an officer.	Secretary	O	
2			Whether the RA officials identified have undergone adequate training to handle RA operations, to understand PKI concepts, have exposure to software and hardware of PKI, computer security and operations of RA functions	M	

			1) RA Administrator can create RA Officer. It is RA Administrator's obligation to verify credentials while creating RA Officer. 2) No. of RA Officers created by RA Administrator Whether the RA officers who have been relieved from RA Office due to transfer/retirement/resignation /death had been made inactive by the existing RA Administrator No. of Active RA Administrators No. of inactive RA Administrators (Transfer/Retirement/Resignation/ others)No. of active RA Officers No. of inactive RA Officers Reasons for inactivation (Transfer/Retirement/Resignation/ others)	M	

			Whether the RA Officials are aware of the requirements from the Certification Practice Statement (CPS)		
3			Whether the RA Office has outsourced RA operations or any part of RA Operations? If so, comment on the adequacy of contracts and agreements for all RA Operations that are outsourced	M	
4	do	Systems and Connectivity	Configuration of System(s) used for RA Operation	M	
			Whether RA maintains a copy of asset register (inventory of systems with configuration details, Date of purchase, list of software and utility software loaded in the system, Antivirus software, AMC etc		
			Whether all media/documents, if any maintained at the RA Office by the RA Officials for RA Operations have external volume identification, internal labels fixed, wherever applicable.		

			Details of Antivirus software installed and whether latest update of Antivirus software is loaded If yes, details of latest antivirus patches loaded		
			Whether Software is loaded to perform RA operations	M	
			Token(s)	M	
5		Previous Audit Report	Whether previous audit report as per IT ACT 2000 stands attended	M	
6			Are there any observations pending to be attended in the previous audit report	M	

M - Mandatory, O - Optional

7	do	Physical Security	Whether Storage for Subscriber(s)' Information is appropriately ensured		M	
			Security arrangements for storage area (adequate or not)		M	
			Whether the Key Custodian of subscriber's information is identified and whether he is aware of the legal requirements of storage?		M	
8		Connectivity to CA Services (https:// 10.0.67.57/idrbtra)	Through INFINET		M	
9	do	Subscribers' Information	Total No. of Users created		M	
			Total No. of active users			
			Total No. of inactive users and reason			

M - Mandatory, O - Optional

			Application form received?	M	
			Presence of Signature of Applicant/ Signature of higher authority on both the sides of the application form?	M	
			Applications Class wise maintained?	O	
			Are Supporting documents attached?	M	
			Whether Verification procedures are followed as per Identity Verification Details released in September 5, 2019 by CCA, New Delhi.	M	
			Whether instructions are followed for class 2 physical verification?	M	
			Personal verification & Proof of ID Verification in case of Class 3?	M	
			Whether Date of Creation of user id recorded)	M	
			No. of certificates generated during the period covered under audit	M	

M - Mandatory, O - Optional

10	do	Revocation details	No. of certificates revoked during the period covered under audit	M	
			No. of Revocation requests received?	M	
			Whether the ink-signed application forms for the revocation obtained from the Subscribers	M	
			No. of revocation requests initiated by Subscribers / RA	M	
			Whether approval has been obtained for initiating revocation requests on behalf of subscribers	M	

			Revocation request(s) forwarded to IDRBT CA?	M	
			List of compromised users maintained?	M	
11	do	Communication to subscribers	Paper/ electronic communication with subscribers and CA maintained?	M	
12	do	Self audit trails	Audit trails maintained? (to ensure that all applications for the issue of Digital Signature Certificates are duly filled in, checklist duly filled in with date , time and initials, date of creation of user id, Application ID and date of processing)	M	
13	do	Disposal of information	Any information or record pertaining to RA Operations disposed / destroyed without permission from IDBRT CA?	M	

M - Mandatory, O - Optional

			Are the disposal records maintained? (if any)	M	
14	Audit Procedures for RA Offices	Certificate details	Certificate details maintained? (As per Annexure – 1)	M	
15	do	Revocation details	Whether Revocation details are maintained? as per Annexure – 2)	M	

M - Mandatory, O - Optional

16	do	Financial records	Whether Financial records are maintained as per Annexure – 3	M	
17	do	Master Agreement	Whether the RA Office holds a Copy of Master Agreement?	M	
18	do	RA officials' transfer/termination of duty/revocation details	Whether Records are maintained?	M	
19	IDRBT CA CPS	Private Key Compromise	Notified IDRBT CA regarding compromise of the private key of RA Official?	M	
			If so, records for the same	M	

M - Mandatory, O - Optional

20	do	Certificate Expiry	Notified Subscribers regarding the expiry of certificates?	O	
			If so, records for the same	O	
21	do	Rejected applications	Records of rejected applications are maintained?	M	
			Does RA intimate subscribers regarding the rejection of requests?	M	
22	do	Key length & Algorithm	Does RA verify the Distinguished Name Details (Certificate Details) while processing Application ID and also whether the key length is of 2048 bits and algorithm is SHA 256	M	

M - Mandatory, O - Optional

23			Whether the RA maintains the following records as per the guidelines issued by the CA? 1. Electronic/manual backup of various reports generated 2. Financial records received from the subscriber 3. Necessary e-mail communication with the subscriber in paper/electronic media 4. E-mail communication with CA Office in paper/electronic media	M	
24			Whether the Subscriber's records are archived for seven years as per the legal requirements?	M	
25		No. of SSL Certificates issued		M	
26		SSL Guidelines	Whether the RA adheres to the SSL Guidelines issued by CCA and circulated to RAs by IDRBT CA while issuing SSL Certificates	M	

M - Mandatory, O - Optional