

REQUEST FOR QUOTES [RFQ 051/2025-26]

for

Engagement of CERT-IN Auditor to conduct System Audit for CoFT Compliance Requirement for issuer SAR.

**Issued by: Canara Bank
Single Tender Enquiry Processing Section
Centralized Procurement & Vendor Management Vertical, HO (Annexe)
1st Floor, Naveen Complex
14, M G Road
Bengaluru-560 001
Phone No:080-25584873
Email: singletender@canarabank.com**

BID SCHEDULE

Sl. No.	Description	Details
1.	RFQ No. and Date	RFQ 051/2025-26 dated 29/12/2025 for engagement of CERT-IN Auditor to conduct System Audit for CoFT Compliance Requirement for issuer SAR.
2.	Location Address for submission of Bid/s [Address for Communication]	The Senior Manager Canara Bank, Single Tender Enquiry Processing Section Centralized Procurement & Vendor Management Vertical, Head Office (Annexe) 1 st Floor, Naveen Complex 14, M G Road Bengaluru -560 001 Karnataka Tel - 080-25584873 Email: singletender@canarabank.com
3.	Date of Issue	29/12/2025, Monday
4.	Last Date of Submission of Bids	19/01/2026, Monday up to 03:00 PM
5.	Date and Time of Opening Bids	19/01/2026, Monday at 03:30 PM

Dear Vendor,

The Bank intends to conduct System Audit for CoFT Compliance Requirement for issuer SAR.

1.	Details of the Audit	To conduct System Audit for CoFT Compliance Requirement for issuer SAR.
2.	Scope of Work/Technical Requirements	As per Annexure-VI
3.	Time Lines for completion of audit	4 Months from the date of acceptance of PO
4.	Warranty Period (If applicable)	NA
5.	Payment Terms & Conditions	As per Annexure -III
6.	Bill of Material	As per Annexure -II
7.	Mode of Submission of Bid/Quote	Softcopy Softcopy- (Digitally Signed PDF file of the bid which is Password protected should be send to the below mentioned Email ID: singletender@canarabank.com)
8.	Bid Submission Due Date & Time	19/01/2026, Monday up to 03:00 PM
9.	Other Terms and Conditions	As per RFQ 051/2025-26
10.	Any Other Information	NA

Yours Faithfully,

Authorized Signatory

Note: For further clarification, if any, please contact us.

The Senior Manager
Canara Bank,
Single Tender Enquiry Processing Section
Centralized Procurement & Vendor Management Vertical,
Head Office (Annexe)
1st Floor, Naveen Complex
14, M G Road
Bengaluru -560 001
Ph. No: 080- 25584873.

This bid is restricted to following Bank's empaneled CERT-IN auditors selected through EOI-09/2023-24 dated 19/03/2024.

- 1. M/S DIGITAL AGE STRATEGIES PVT LTD**
- 2. M/S AAA TECHNOLOGIES LTD**
- 3. M/S KPMG ASSURANCE AND CONSULTING SERVICES LLP**
- 4. M/S YOGANANDH & RAM LLP**
- 5. M/S SECUREYES TECHNO SERVICES PVT LTD**
- 6. M/S AKS INFORMATION TECHNOLOGY SERVICES PVT LTD**
- 7. M/S PWC PVT LTD.**

ANNEXURE-I

1. Objective:

The Bank seeks to establish a highly professional relationship with the auditor responsible for conducting System Audit for CoFT Compliance Requirement for issuer SAR.

2. Requirement Details:

Bank invites online submission of bids from Cert-In empaneled auditors for conducting System Audit for CoFT Compliance Requirement for issuer SAR in Canara Bank as per the Terms & Conditions, Technical Requirements and Scope of Work described elsewhere in this document.

3. Project Timelines:

Bidders are requested to keep the following timelines with regard to the completion of Assessment.

- The complete activity System Audit for CoFT Compliance Requirement and submission of Final report) has to be completed in 04 months from the date of issue of Purchase Order.
- Re-validation/ incorporation of changes suggested by the respective card network before submission of final assessment report.

4. Penalties & Liquidated damages on delay in completion of Assessment:

If the assessment is not completed within the timelines, Bank may be entitled to charge penalty @0.50% on delay per week or part thereof on the total cost of the Assessment. However, the total Penalty/LD to be recovered shall be restricted to 5% of total cost of the Assessment (exclusive of Taxes).

5. Subcontracting:

The vendor shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the vendor under the contract without the prior written consent of the Bank.

6. Deliverables:

- i. Audit reports should be provided to Bank after completion of the subject assessment in PDF & Excel format along with Two hard copies (optional, if required).
- ii. Email and Phone support till final closure report is to be provided by the Auditor.

We comply with each point mentioned above without any deviations.

Date:	Signature with seal Name: Designation:
-------	--

ANNEXURE-II

Bill of Material

SUB: To conduct System Audit for CoFT Compliance Requirement for issuer SAR.

Ref: RFQ 051/2025-26 dated 29/12/2025.

[Amount in INR]

Sl. No	Audit	Cost Price			
		Price (Excl. of Tax)	Tax for Column A		Price (Incl. of Tax)
		A	B% of tax	C Tax Amt.	D=A+C
1.	To conduct System Audit for CoFT Compliance Requirement for issuer SAR as per Scope of Work mentioned in RFQ-051-2025-26 dated 29/12/2025	-	-	-	-

Date:	Signature with seal Name: Designation:
-------	--

ANNEXURE-III

Payment Terms & Conditions

SUB: To conduct System Audit for CoFT Compliance Requirement for issuer SAR.

Ref: RFQ 051/2025-26 dated 29/12/2025.

1. 100% payment should be released on submission of invoice, Confirmation of work completion from the Card Technology Management section, Credit & Prepaid Cards Vertical, HO.
2. Bank will not pay any amount in advance.
3. Audits are to be conducted onsite only and Remote access cannot be provided.
4. Bidder should employ the resources for the System Audit.
5. The payments will be released through NEFT/RTGS and the selected bidder has to provide necessary bank details like account number, bank's name with branch name, Correct IFSC code etc.
6. **Other Condition:** In case of Multiple L1 Bidders, the Bank may reserve the right to re-negotiate with only the L1 tied bidders to determine a clear L1 by way of seeking revised sealed offers.

Locations details are as mentioned below: Location for conducting audit is from onsite only at the following location of the Bank.

Sl. No	Section / Wing	Location
1.	CTM Section, Credit & Prepaid Cards Vertical	Bengaluru

We comply to all the points mentioned in RFQ, Scope of work, without any deviation.

Date:	Signature with seal:
	Name :
	Designation :

ANNEXURE-IV
SCOPE OF WORK

SUB: To conduct System Audit for CoFT Compliance Requirement for issuer SAR.

Ref: RFQ 051/2025-26 dated 29/12/2025.

Pre-Assessment Checks

Expected Audit period: April 1st 2025 - March 31st 2026

Sr. No.	Domain	Question
1	Audit Period	What is the audit period of the submitted SAR?
2	TSP life cycle	Which category (TR/TSP/ Merchant /Acquirer/Issuer) in the tokenization life cycle does the TSP belong to?
3	Tokenization service	Which tokenization service does the TSP provide? - CoFT/Device/Guest checkout. In case a TSP is involved in providing more than one service, highlight all.
4	Tokenization service	Has the issuer called out the type of card instrument (Debit/Credit/Prepaid/ Commercial etc.) coverage w.r.t tokenization services?
5	Auditor Qualification	Is audit performed by a CERT-IN empaneled auditor?
6	Audit coverage	Does the report cover all controls in the master list and informational controls?
7	Third parties	Are third parties involved OR is any activity outsourced in the tokenization process? Please list out third party names and confirm if relevant controls have been tested for such parties.
8	Payment data flow	Does the report include the payment data flow diagram inclusive of the systems involved in the tokenization lifecycle?
9	Audit coverage	Does the scope of the TSP SAR adequately cover all relevant tokenization circulars?
10	Audit Compliance	Is the SAR signed by the designated TSP auditor?
11	Audit Period Coverage	Is the SAR covering entire audit period? If not then is there an interim SAR covering remaining audit period?
12	Regulatory Compliance	Is item-wise compliance clearly documented within the SAR submission?
13	Audit Observation	Are the status updates, remediation plans, and management comments documented for all identified observations (if any)?
14	Audit Observation	Are the auditor's comments sufficiently detailed and explanatory for observations noted in the SAR (if any)?
15	Observation Tracking	Are there any open observations from the previous years, and have they been addressed or carried forward in the current SAR?

While guidelines have been provided as a reference, TSP auditors are required to cover all 95 controls + 15 pre-assessment checks in the report and provide adequate justification for controls marked not applicable

Master Control List Validation FY 2026													
Sr No	Guideline Date	Para/section	RBI document name	RBI document number	Domain	Guideline	Tokenization type (Device/CoFT/Device and CoFT)	Card Issuer/ Acquirer	Token requestor / merchant/ Others	Token service provider	Issuer Bank Providing Tokens	Informational	Remarks
1	08-Jan-19	Point 3	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Registration by customer	All extant instructions of Reserve Bank on safety and security of card transactions, including the mandate for Additional Factor of Authentication (AFA) / PIN entry shall be applicable for tokenized card transactions also.	Device and CoFT	Y	Y	Y	Y	-	This control is applicable to all entities including acquirers
2	08-Jan-19	Point 5	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Miscellaneous	No charges should be recovered from the customer for availing this service.	Device and CoFT	Y	Y	Y	Y	-	This control is applicable to all entities including acquirers
3	08-Jan-19	Annex 1 definition	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Unique token	The token shall be unique for a combination of card, token requestor and device (referred hereafter as "identified device"). <i>Note: The following additional samples must be tested by auditors to validate the above control.</i>	Device	-	Y	Y	Y	-	For token requestors validation should be done to check if unique tokens are assigned to merchants. <i>Note: This Control also</i>

						<p><i>Additional Sampling Control: For tokenized transactions, is each token generated unique for the specific combination of card, token requestor, and merchant, and can this be evidenced through system logs showing token issuance, token mapping extracts listing card-merchant-requestor combinations, or screenshots from the token vault/system interface confirming that duplicate tokens are not generated for the same combination? Evidence must be captured appropriately for validation.</i></p>								requires additional evidence sampling
4	08-Jan-19	conditi ons I	Tokeniz ation - Card transact ions	DPSS.CO.PDNo.1463 /02.14.003/2018-19	Tokeniz ation - de- tokeniza tion service	Tokenization and de-tokenization shall be performed only by the authorized card network	Device and CoFT	-	-	Y	Y	-	-	
5	08-Jan-19	conditi ons I	Tokeniz ation - Card transact ions	DPSS.CO.PDNo.1463 /02.14.003/2018-19	Tokeniz ation - de- tokeniza tion service	Recovery of original Primary Account Number (PAN) should be feasible for the authorized card network only.	Device and CoFT	Y	Y	Y	Y	-	-	

6	08-Jan-19	conditions I	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Tokenization - de-tokenization service	<p>Adequate safeguards shall be put in place to ensure that PAN cannot be found out from the token and vice versa, by anyone except the card network. Integrity of token generation process shall be ensured at all times.</p> <p><i>Note: The following additional samples must be tested by auditors to validate the above control.</i></p> <p><i>Additional Sampling Control: This control must be tested by auditors under sampling controls for banks that receive and store the tokens from CPN. Please specifically call out if the bank has access to the token and/or is storing the token.</i></p>	Device and CoFT	Y	Y	Y	Y	-	<p>Note: Issuers should store only store the masked PAN received from the networks. A check must be done to validate the same.</p> <p><i>Note: This Control also requires additional evidence sampling</i></p>
7	08-Jan-19	conditions ii	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Tokenization - de-tokenization service	Tokenization and de-tokenization requests should be logged by the card network and available for retrieval, if required.	Device and CoFT	-	-	Y	Y	-	This control is applicable to card issuers only if they create tokens (tokenize and detokenize cards).

8	08-Jan-19	conditi ons iii	Tokeniz ation - Card transact ions	DPSS.CO.PDNo.1463 /02.14.003/2018-19	Tokeniz ation - de- tokeniza tion service	Actual card data, token and other relevant details shall be stored in a secure mode. <i>Note: Auditor must specify any and every card information such as card expiry, cardholder name etc. being stored by the token service participant.</i>	Device and CoFT	Y	Y	Y	Y	-	This control is applicable to all entities including acquirers
9	08-Jan-19	conditi ons iii	Tokeniz ation - Card transact ions	DPSS.CO.PDNo.1463 /02.14.003/2018-19	Tokeniz ation - de- tokeniza tion service	Token requestors shall not store PAN or any other card detail.	Device and CoFT	-	Y	-	-	-	-
10	08-Jan-19	conditi ons iv	Tokeniz ation - Card transact ions	DPSS.CO.PDNo.1463 /02.14.003/2018-19	Certific ation of systems of card issuers /acquir ers, token request ors and their app, etc.	Card network shall get the token requestor certified for (a) token requestor's systems, including hardware deployed for this purpose, (b) security of token requestor's application, (c) features for ensuring authorized access to token requestor's app on the identified device, and (d) other functions performed by the token entity, including customer onboarding, token provisioning and storage, data storage, transaction processing, etc.	Device and CoFT	-	Y	Y	-	-	While the point is to be exclusively tested for card networks, Auditors reviewing token requestors must validate if such certificatio n is undertake n actively by these entities.

1 1	08-Jan-19	conditi ons v	Tokeniz ation - Card transact ions	DPSS.CO.PDNo.1463 /02.14.003/2018-19	Certific ation of systems of card issuers /acquir ers, token request ors and their app, etc.	Card networks shall get the card issuers / acquirers, their service providers and any other entity involved in payment transaction chain, certified in respect of changes done for processing tokenized card transactions by them. <i>Note: The following additional samples must be tested by auditors to validate the above control.</i> <i>Additional Sampling Control: Is there any change in the environment on tokenization during the audit period from FY 2025- FY 2026. If any, then evidence demonstrating compliance before the change must be captured appropriately for validation.</i>	Device and CoFT	Y	Y	Y	Y	-	While the point is to be exclusively tested for card networks, auditors reviewing other entities (card issuers / acquirers, their service providers and any other entity) must validate if such certificatio n is undertake n actively by these entities. <i>Note: This Control also requires additional evidence sampling</i>
1 2	08-Jan-19	conditi ons vi	Tokeniz ation - Card transact ions	DPSS.CO.PDNo.1463 /02.14.003/2018-19	Certific ation of systems of card issuers /acquir ers, token request ors and their app,	Card network shall ensure that certification of systems of card issuers / acquirers, token requestors and their application shall conform to international best practices / globally accepted standards.	Device and CoFT	Y	Y	Y	Y	-	While the point is to be exclusively tested for card networks, auditors reviewing other entities (card

					etc.								issuers / acquirers, their service providers and any other entity) must validate if such certification is undertaken actively by these entities.
13	08-Jan-19	conditions vii	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Registration by customer	<p>Registration of card on token requestor's app shall be done only with explicit customer consent through Additional Factor of Authentication (AFA), and not by way of a forced / default / automatic selection of check box, radio button, etc.</p> <p><i>Note: The following additional samples must be tested by auditors to validate the above control.</i></p> <p><i>Additional Sampling Control: Is tokenization of card data performed only after obtaining explicit customer consent with issuer-provided AFA and not by way of a forced / default / automatic selection</i></p>	Device and CoFT	-	Y	Y	Y	-	<p><i>Note: This Control also requires additional evidence sampling</i></p>

						<p><i>of check box, radio button. Can this be evidenced through provisioning logs from the issuer showing AFA validation records, audit logs linking the AFA event ID to the token creation request, and exception reports where tokenization attempts failed due to missing or failed AFA validation? Evidence must be captured appropriately for validation.</i></p>							
14	08-Jan-19	conditions viii	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Registration by customer	<p>AFA validation during card registration, as well as, for authenticating any transaction, shall be as per extant Reserve Bank instructions for authentication of card transactions.</p> <p><i>Note: The auditor must validate AFA for sample cases including only tokenization, tokenized card transaction and tokenization + transaction.</i></p>	Device and CoFT	Y	Y	Y	Y	-	-

15	08-Jan-19	conditions	Tokenization - Card transactions	DPSS.CO.PDNo.1463 /02.14.003/2018-19	Registration by customer	<p>Customers shall have option to register / de-register their card for a particular use case, i.e., contactless, QR code based, in-app payments, etc.</p> <p><i>Note: The following additional samples must be tested by auditors to validate the above control.</i></p> <p><i>i. Additional Sampling Control: Does the merchant application or platform provide a visible option for the cardholder to deregister the token, and can this be evidenced through screenshots of the user interface showing the deregistration feature, system configuration settings, or logs confirming token deregistration requests? Evidence must be captured appropriately for validation.</i></p> <p><i>ii. Additional Sampling Control: Does the system successfully process a deregistration request and confirm completion to the cardholder, and can this be evidenced</i></p>	Device	Y	Y	-	Y	-	<p>Applicable for device token requestors having a customer facing application .</p> <p><i>Note: This Control also requires additional evidence sampling</i></p>
----	-----------	------------	----------------------------------	--------------------------------------	--------------------------	--	--------	---	---	---	---	---	--

						through system logs showing deregistration events, confirmation messages/notifications sent to the cardholder, screenshots from the application interface displaying successful deregistration status, and exception or failure logs where deregistration requests could not be processed? Evidence must be captured appropriately for validation.							
16	08-Jan-19	conditions x	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Registration by customer	Customers shall be given option to set and modify per transaction and daily transaction limits for tokenized card transactions.	Device and CoFT	Y	-	-	Y	-	-
17	08-Jan-19	conditions xi	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Registration by customer	Suitable velocity checks (i.e., how many such transactions will be allowed in a day / week / month) may be put in place by card issuers / card network as considered appropriate, for tokenized card transactions. <i>Note: The following additional samples must be tested by auditors to validate the above control.</i>	Device and CoFT	Y	-	Y	Y	-	<i>Note: This Control also requires additional evidence sampling</i>

						<i>Additional Sampling Control: For tokenized transactions, are suitable velocity limits (daily/weekly/monthly) applied by the organization, and can this be evidenced through transaction logs or reports for a sample of tokenized transactions showing that limits were enforced and no breaches occurred? Evidence must be captured appropriately for validation.</i>							
18	08-Jan-19	conditions xii	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Registration by customer	For performing any transaction, the customer shall be free to use any of the cards registered with the token requestor app.	Device and CoFT	-	Y	-	-	-	Applicable for token requestors having a customer facing application
19	08-Jan-19	conditions xiii	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Secure storage of tokens	Secure storage of tokens and associated keys by token requestor on successful registration of card shall be ensured.	Device and CoFT	-	Y	Y	Y	-	-
20	08-Jan-19	conditions xiv	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Customer service and dispute resolution	Card issuers shall ensure easy access to customers for reporting loss of "identified device" or any other such event which may expose tokens to unauthorized usage.	Device	Y	-	Y	Y	-	-
21	08-Jan-19	conditions xiv	Tokenization - Card	DPSS.CO.PDNo.1463/02.14.003/2018-19	Customer service	Card network, along with card issuers and token	Device and CoFT	Y	Y	Y	Y	-	-

			transact ions		and dispute resoluti on	requestors, shall put in place a system to immediately deactivate unauthorized/expos ed tokens and associated keys.							
2 2	08- Jan- 19	conditi ons xv	Tokeniz ation - Card transact ions	DPSS.CO.PDNo.1463 /02.14.003/2018-19	Custom er service and dispute resoluti on	Dispute resolution process shall be put in place by card network for tokenized card transactions. <i>Note: The following additional samples must be tested by auditors to validate the above control.</i> <i>Additional Sampling Control: Does the customer grievance redressal framework cover disputes related to tokenization/organi zation, and can this be evidenced through sample grievance or complaint records related to tokenization issues, along with documentation or logs showing the resolution process followed? Evidence must be captured appropriately for validation.</i>	Device and CoFT	-	-	Y	Y	-	<i>Note: This Control also requires additional evidence sampling</i>
2 3	08- Jan- 19	conditi ons xvi	Tokeniz ation - Card transact ions	DPSS.CO.PDNo.1463 /02.14.003/2018-19	Safety and security of transact ions	Card network shall put in place a mechanism to ensure that the transaction request has originated from an "identified	Device	-	-	Y	Y	-	-

						device”.							
2 4	08-Jan-19	conditi ons xvii	Tokeniz ation - Card transact ions	DPSS.CO.PDNo.1463 /02.14.003/2018-19	Safety and security of transact ions	Card network shall: a) ensure monitoring to detect any malfunction, anomaly, suspicious behavior, or the presence of unauthorized activity within the tokenization process and; b) implement a process to alert all stakeholders.	Device and CoFT	-	-	Y	Y	-	-
2 5	08-Jan-19	conditi ons xviii	Tokeniz ation - Card transact ions	DPSS.CO.PDNo.1463 /02.14.003/2018-19	Safety and security of transact ions	Based on risk perception, etc., card issuers may decide whether to allow cards issued by them to be registered by a token requestor.	Device and CoFT	Y	-	-	Y	-	-
2 6	07-Sep-21	3.b	Tokeniz ation - Card Transac tions: Permitt ing Card- on-File Tokeniz ation (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S -516/02-14- 003/2021-22	Tokeniz ation - de- tokeniza tion service	Card issuers can offer card tokenization services as Token Service Providers .	Device and CoFT	Y	-	-	Y	-	-
2 7	07-Sep-21	3.c	Tokeniz ation - Card Transac tions: Permitt ing Card- on-File Tokeniz ation (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S -516/02-14- 003/2021-22	Tokeniz ation - de- tokeniza tion service	The facility of tokenization shall be offered by the Token Service Providers only for the cards issued by / affiliated to them.	Device and CoFT	-	-	Y	Y	-	Applicable for Token service providers. Applicable to card issuers only if they create tokens

													(tokenize and detokenize cards).
28	07-Sep-21	3.d	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S -516/02-14-003/2021-22	Tokenization - de-tokenization service	The ability to tokenize and de-tokenize card data shall be with the same Token Service Providers.	Device and CoFT	-	-	Y	Y	-	Applicable for Token service providers. Applicable to card issuers only if they create tokens (tokenize and detokenize cards).
29	07-Sep-21	3.e	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S -516/02-14-003/2021-22	Registration by customer	Tokenization of card data shall be done with explicit customer consent requiring Additional Factor of Authentication (AFA) validation by card issuer.	Device and CoFT	Y	Y	Y	Y	-	-
30	07-Sep-21	4.b.	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S -516/02-14-003/2021-22	Transaction tracking / reconciliation	For transaction tracking and / or reconciliation purposes, entities can store limited data - last four digits of actual card number and card issuer's name - in compliance with the applicable standards. <i>Note: The following additional samples must be tested by auditors to validate</i>	Device and CoFT	Y	Y	-	-	-	Applicable for all entities including Acquirers except issuers and card networks <i>Note: This Control also requires additional evidence sampling</i>

						<p><i>the above control.</i></p> <p><i>Additional Sampling Control: Does the entity store only the last four digits of the card number and the cardholder's name, with no PAN, CVV, or expiry details retained, and can this be evidenced through database extracts with masked card details, system configuration or data schema documentation, screenshots from the application interface showing only permissible data, and system monitoring or alert logs capturing any unauthorized attempt to store full PAN, expiry, or CVV data? Evidence must be captured appropriately for validation.</i></p>							
31	07-Sep-21	Annex 1	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S -516/02-14-003/2021-22	Unique token	<p>For the purpose of CoFT, the token shall be unique for a combination of card, token requestor and merchant,</p> <p><i>Note: The following additional samples must be tested by auditors to validate the above control.</i></p> <p><i>Additional Sampling</i></p>	CoFT	-	Y	Y	Y	-	Applicable for card networks. Additionally for token requestors validation should be done to check if unique tokens are assigned to merchants .

						<p><i>Control: For tokenized transactions, is each token generated unique for the specific combination of card, token requestor, and merchant, and can this be evidenced through system logs showing token issuance, token mapping extracts listing card-merchant-requestor combinations, or screenshots from the token vault/system interface confirming that duplicate tokens are not generated for the same combination? Evidence must be captured appropriately for validation.</i></p>							<p>Applicable to card issuers only if they create tokens (tokenize and detokenize cards).</p> <p><u>Note:</u> This Control also requires additional evidence sampling</p>
32	07-Sep-21	Annex 2	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S-516/02-14-003/2021-22	Registration by customer	<p>If card payment for a purchase transaction at a merchant is being performed along with the registration for CoFT, then AFA validation may be combined.</p>	CoFT	Y	Y	Y	Y	-	-

33	07-Sep-21	Annex 3	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S-516/02-14-003/2021-22	Token de-registration	<p>The merchant shall give an option to the cardholder to de-register the token.</p> <p><i>Note: The following additional samples must be tested by auditors to validate the above control.</i></p> <p><i>i. Additional Sampling Control: Does the merchant application or platform provide a visible option for the cardholder to deregister the token, and can this be evidenced through screenshots of the user interface showing the deregistration feature, system configuration settings, or logs confirming token deregistration requests? Evidence must be captured appropriately for validation.</i></p> <p><i>ii. Additional Sampling Control: Does the system successfully process a deregistration request and confirm completion to the cardholder, and can this be evidenced through system logs showing deregistration events,</i></p>	Device and CoFT	-	Y	-	-	-	<p><i>Note: This Control also requires additional evidence sampling</i></p>
----	-----------	---------	--	---	-----------------------	---	-----------------	---	---	---	---	---	---

						confirmation messages/notifications sent to the cardholder, screenshots from the application interface displaying successful deregistration status, and exception or failure logs where deregistration requests could not be processed? Evidence must be captured appropriately for validation.							
34	07-Sep-21	Conditions 3	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S-516/02-14-003/2021-22	Token deregistration	Further, a token requestor having direct relationship with the cardholder shall: a) list the merchants in respect of whom the CoFT has been opted through it by the cardholder b) provide an option to deregister any such token	CoFT	-	Y	-	-	-	-
35	07-Sep-21	Annex 4	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S-516/02-14-003/2021-22	Token deregistration	a) A facility shall also be given by the card issuer to the cardholder to view the list of merchants in respect of whom the CoFT has been opted by her / him, and to deregister any such token. b) This facility shall be provided through one or more of the following channels - mobile application, internet banking,	CoFT	Y	-	-	Y	-	-

						Interactive Voice Response (IVR) or at branches / offices.							
36	07-Sep-21	Annex 5	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S -516/02-14-003/2021-22	Registration by customer	<p>Whenever a card is renewed or replaced, the card issuer shall seek explicit consent of the cardholder for linking it with the merchants with whom (s)he had earlier registered the card.</p> <p><i>Note: The following additional samples must be tested by auditors to validate the above control.</i></p> <p><i>Additional Sampling Control:</i> Whenever a card is renewed or replaced, does the issuer seek explicit consent from the cardholder before linking the new card to existing tokens, and can this be evidenced through system logs capturing consent events, screenshots of customer notifications or consent prompts, records of AFA/OTP authentication, and exception logs where consent was not obtained or linking failed? Evidence must be</p>	Device and CoFT	Y	-	-	Y	-	<i>Note: This Control also requires additional evidence sampling</i>

						captured appropriately for validation.							
37	07-Sep-21	Annex 6	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S -516/02-14-003/2021-22	Unique token	The Token service provider shall put in place a mechanism to ensure that the transaction request has originated from the merchant and the token requestor with whom the token is associated.	CoFT	-	-	Y	Y	-	Applicable to card issuers only if they create tokens (tokenize and detokenize cards).
38	23-Dec-21	Point 2.b	Restriction on storage of actual card data [i.e. Card-on-File (CoF)]	RBI/2021-2022/142 CO.DPSS.POLC.No.S -1211/02-14-003/2021-22	Miscellaneous	In addition to tokenization, industry stakeholders may devise alternate mechanism(s) to handle any use case (including recurring e-mandates, EMI option, etc.) or post transaction activity (including chargeback handling, dispute resolution, reward / loyalty programme, etc.) that currently involves / requires storage of CoF data by entities other than card issuers and card networks. <i>Note: The following additional samples must be tested by</i>	Device and CoFT	Y	Y	Y	Y	-	Industry stakeholders may include all entities in the transaction ecosystem <i>Note: This Control also requires additional evidence sampling</i>

					<p><i>auditors to validate the above control.</i></p> <p><i>i. Additional Sampling Control: For a sample of transactions across recurring mandates, EMI, refunds/chargebacks, and loyalty/reward programs, verify that these were processed using network-issued tokens or alternate IDs instead of raw card data, and ensure that evidence was captured appropriately for validation.</i></p> <p><i>ii. Additional Sampling Control: For post-transaction activities such as refunds, disputes, or reward accruals, does the organization ensure that no sensitive card details (PAN/CVV) are stored or accessed beyond the issuer or card network, and can this be evidenced through system or database logs for a sample of such post-transaction activities confirming that only permitted data elements are retained? Evidence</i></p>							
--	--	--	--	--	---	--	--	--	--	--	--	--

						<i>must be captured appropriately for validation.</i>							
39	24-Jun-22	Point 4	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/77 CO.DPSS.POLC.No.S-567/02-14-003/2022-23	CoF data purging	It has been decided to extend the timeline for storing of CoF data by three months, i.e., till September 30, 2022, after which such data shall be purged.	CoFT	Y	Y	-	-	-	This control is applicable for Acquirers not Issuers
40	21-Apr-23	Point 3a	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	CO.DPSS.POLC.No.S-65/02-14-003/2023-24	Guest checkout transactions	Only for guest checkout transaction - a) Other than the card issuer and the card network, the merchant or its Payment Aggregator (PA) involved in settlement of such transactions, can save the CoF data for a maximum period of T+2 days ("T" being the transaction date) or till the settlement date, whichever is earlier. b) This data shall be used only for settlement of such transactions, and must be purged thereafter.	Device and CoFT	-	Y	-	-	-	-
41	21-Apr-23	Point 3b	Restriction on Storage of Actual Card Data [i.e. Card-	CO.DPSS.POLC.No.S-65/02-14-003/2023-2024	Guest checkout transactions	a) The acquiring banks shall not store CoF data for guest checkout transactions beyond a period of T+180 days ("T" being the transaction date). b) For such	Device and CoFT	Y	-	-	-	-	This control is applicable for Acquirers not Issuers

			on-File (CoF)]			transactions processed before the April 21,2023, compliance with the T+180 days' timeline shall be ensured by June 30, 2023.							
4 2	23-Jun-23	Point 3b	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	CO.DPSS.POLC.No. S-65/02-14-003/2023-2024	Guest checkout transactions	c) Only acquiring banks are permitted to store actual card details used for guest checkout transaction (historical) in offline storing mediums.	Device and CoFT	Y	Y	Y	Y	-	This control is applicable to all entities including acquirers
4 3	16-Nov-23	Point 2	Restriction on storage of actual card data [i.e. Card-on-File (CoF)]	CO.DPSS.POLC.No. S-825/02-14-003/2023-2024	Guest checkout transactions	Entities in the transaction/payment chain shall deploy an alternate solution for handling guest checkout transactions by 31 January 2024.	Device and CoFT	Y	Y	Y	Y	-	-
4 4	25-Aug-21	Point 2	Tokenization - Card Transactions : Extending the Scope of Permitted Devices	RBI/2021-22/92 CO.DPSS.POLC.No.S-469/02-14-003/2021-22	Extension to other devices	The scope of tokenization has been extended to include consumer devices - laptops, desktops, wearables (wrist watches, bands, etc.), Internet of Things (IoT) devices, etc. All other provisions of the circular referred to above shall continue to be applicable.	Device	-	Y	Y	Y	-	Control is applicable only if the Issuer provides this service. Issuer may or may not act as a token service provider for this to be tested

4 5	20-Dec-23	Annexure 1	Card-on-File Tokenization (CoFT) - Enabling Tokenization through Card Issuing Banks	RBI/2023-24/91 CO.DPSS.POLC.No.S -919/02-14-003/2023-24	Enable tokenization through card issuing banks	Does the card issuing entity provide CoF tokens option for multiple merchants through mobile/internet banking channels? (note: Issuing bank may/may not issue tokens in order to provide this feature)	CoFT	Y	-	Y	Y	-	Control is applicable only if the Issuer provides this service. Issuer may or may not act as a token service provider for this to be tested
4 6	20-Dec-23	Annexure 2	Card-on-File Tokenization (CoFT) - Enabling Tokenization through Card Issuing Banks	RBI/2023-24/91 CO.DPSS.POLC.No.S -919/02-14-003/2023-24	Enable tokenization through card issuing banks	CoFT generation shall be done only on explicit customer consent, and with AFA validation. If the cardholder selects multiple merchants for which to tokenize his/her card, AFA validation may be combined for all these merchants.	CoFT	Y	-	Y	Y	-	-
4 7	20-Dec-23	Annexure 3	Card-on-File Tokenization (CoFT) - Enabling Tokenization through Card Issuing Banks	RBI/2023-24/91 CO.DPSS.POLC.No.S -919/02-14-003/2023-24	Enable tokenization through card issuing banks	The tokens thus generated shall be made available on the merchant's payment page, in the cardholder's account with the merchant.	CoFT	Y	Y	Y	Y	-	-

48	20-Dec-23	Annex 4	Card-on-File Tokenization (CoFT) - Enabling Tokenization through Card Issuing Banks	RBI/2023-24/91 CO.DPSS.POLC.No.S -919/02-14-003/2023-24	Enable tokenization through card issuing banks	<p>The cardholder may tokenize the card at any time of his convenience, either on receipt of the new card or later.</p> <p><i>Note: The following additional samples must be tested by auditors to validate the above control.</i></p> <p><i>Additional Sampling Control: Does the cardholder have the facility to tokenize the card on receipt of a new card or at a later stage, and can this be evidenced through screenshots or a demo of the tokenization option presented during card activation, along with system logs of sample new card tokenization requests successfully initiated by the organization. Evidence must be captured appropriately for validation.</i></p>	CoFT	Y	-	Y	Y	-	<i>Note: This Control also requires additional evidence sampling</i>
49	20-Dec-23	Annex 5	Card-on-File Tokenization (CoFT) - Enabling Tokenization through Card Issuing	RBI/2023-24/91 CO.DPSS.POLC.No.S -919/02-14-003/2023-24	Enable tokenization through card issuing banks	The card issuer shall provide a complete list of merchants for whom it can provide tokenization services. The cardholders shall select the merchants with whom he/she wishes to maintain tokens.	CoFT	Y	-	Y	Y	-	-

			Banks			(Alternatively - "The cardholder can make his selection from the list").							
50	20-Dec-23	Annexure 6	Card-on-File Tokenization (CoFT) - Enabling Tokenization through Card Issuing Banks	RBI/2023-24/91 CO.DPSS.POLC.No.S-919/02-14-003/2023-24	Enable tokenization through card issuing banks	The card token so issued may be either by the card network or the issuer or both.	CoFT	Y	-	Y	Y	-	-
51	Apr 2018 and Feb 22	Apr 2018 and Feb 22	1. RBI India data localization circular dated 6 April 2018 2. RBI email to IBA on Local Storage of Domestic Payment Data	1. RBI India data localization circular dated 6 April 2018 2. RBI email to IBA on Local Storage of Domestic Payment Data	India Data localization	1. All system providers (entities involved in payment lifecycle) shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. 2. No payment data element pertaining to the end-to-end payment string can be stored abroad in any form, including hashed, masked, encrypted or tokenized.	Device and CoFT	Y	Y	Y	Y	-	-
52	08-Jan-19	Leading paragraph Point 2 Point 4 Point 6 and 7	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Guidelines	1. Continuing the efforts to improve safety and security of card transactions, Reserve Bank of India had permitted card networks for tokenization in card transactions for a specific use case. For the present, this facility shall be offered through	-	-	-	-	-	Y	-

					<p>mobile phones / tablets only. Its extension to other devices will be examined later based on experience gained.</p> <p>2. It has now been decided to permit authorized card payment networks to offer card tokenization services to any token requestor (i.e., third party app provider), subject to the conditions listed in Annex 1.</p> <p>3. This permission extends to all use cases / channels [e.g., Near Field Communication (NFC) / Magnetic Secure Transmission (MST) based contactless transactions, in-app payments, QR code-based payments, etc.] or token storage mechanisms (cloud, secure element, trusted execution environment, etc.).</p> <p>4. All other instructions related to card transactions shall be applicable for tokenized card transactions as well. The ultimate responsibility for the</p>									
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

					<p>card tokenization services rendered rests with the authorized card networks.</p> <p>5. - Before providing card tokenization services, authorized card payment networks shall put in place a mechanism for periodic system (including security) audit at frequent intervals, at least annually, of all entities involved in providing card tokenization services to customers.</p> <p>- This system audit shall be undertaken by empaneled auditors of Indian Computer Emergency Response Team (CERT-In) and all related instructions of Reserve Bank in respect of system audits shall also be adhered to.</p> <p>- A copy of this audit report shall be furnished to the Reserve Bank, with comments of auditors on deviations, if any, from the conditions listed in Annex 1, along with the compliance thereto.</p>									
--	--	--	--	--	---	--	--	--	--	--	--	--	--	--

						<p>- Further, a report on the details provided in Annex 2 shall be submitted at monthly intervals to the Chief General Manager, Reserve Bank of India, Department of Payment and Settlement Systems, Central Office, Mumbai and by email.</p> <p>-This directive is issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007).</p>									
53	07-Sep-21	3.a	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	DPSS.CO.PDNo.1463/02.14.003/2018-19	Guidelines	<p>On a review of the tokenization framework and to enable cardholders to benefit from the security of tokenized card transactions as also the convenience of CoF, it has been decided to effect the following enhancements:</p> <p>a) Extend the device-based tokenization framework referred to at paragraph above to CoF Tokenization (CoFT) as well.</p>	-	-	-	-	-	Y	-		

54	07-Sep-21	3.f	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	DPSS.CO.PDNo.1463 /02.14.003/2018-19	References	Additional requirements relating to CoFT are listed in the Annex.	-	-	-	-	-	Y	-
55	07-Sep-21	4.a	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	DPSS.CO.PDNo.1463 /02.14.003/2018-19	CoF data purging	With effect from January 1, 2022, no entity in the card transaction / payment chain, other than the card issuers and / or card networks, shall store the actual card data. Any such data stored previously shall be purged.	-	-	-	-	-	Y	-
56	07-Sep-21	4.c	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/202122/96 CO.DPSS. POLC.No.S-516/02-14003/202122	Monitor compliance	Complete and ongoing compliance with the above by all entities involved, shall be the responsibility of the card networks.	Device and CoFT	Y	Y	Y	Y	-	-
57	07-Sep-21	Annex 7 and 8	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/202122/96 CO.DPSS. POLC.No.S-516/02-14003/202122	Conditions to be fulfilled for offering CoFT services	All other provisions of the RBI circulars dated January 8, 2019 and August 25, 2021 shall be applicable. The TSPs shall monitor and ensure compliance in this regard.	-	-	-	-	-	Y	-

58	23-Dec-21	Point 2.a	Restricti on on storage of actual card data [i.e. Card-on-File (CoF)]	RBI/2021-2022/142 CO.DPSS.POLC.No.S -1211/02-14-003/2021-22	CoF data purging	The timeline for storing of CoF data is extended by six months, i.e., till June 30, 2022; post this, such data shall be purged;	-	-	-	-	-	Y	-
59	24-Jun-22	Point 3	Restricti on on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/77 CO.DPSS.POLC.No.S -567/02-14-003/2022-23	Points to note	<p>On a review of the issues involved and after detailed discussions with all stakeholders, it is observed that considerable progress has been made in terms of token creation.</p> <p>Transaction processing based on these tokens has also commenced, though it is yet to gain traction across all categories of merchants.</p> <p>Further, an alternate system in respect of transactions where cardholders decide to enter the card details manually at the time of undertaking the transaction (commonly referred to as “guest checkout transactions”) has not been implemented by the industry stakeholders, so far.</p>	-	-	-	-	-	Y	-

60	28-Jul-22	Point 3.b	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/95 CO.DPSS.POLC.No.S-760/02-14-003/2022-23	Guest checkout transactions	For cases where cardholders decide to enter the card details manually at the time of undertaking the transaction (commonly referred to as “guest checkout transactions”), the following are being permitted as an interim measure -	-	-	-	-	-	Y	-
61	28-Jul-22	Point 3.b.i	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/95 CO.DPSS.POLC.No.S-760/02-14-003/2022-23	Guest checkout transactions	1) Other than the card issuer and the card network, the merchant or its Payment Aggregator (PA) involved in settlement of such transactions, can save the CoF data for a maximum period of T+4 days (“T” being the transaction date) or till the settlement date, whichever is earlier. This data shall be used only for settlement of such transactions, and must be purged thereafter.	CoFT	-	Y	-	-	-	This control is applicable to Merchants /Payment Aggregators.
62	28-Jul-22	Point 3.b.ii	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/95 CO.DPSS.POLC.No.S-760/02-14-003/2022-23	Guest checkout transactions	For handling other post-transaction activities, acquiring banks can continue to store CoF data until January 31, 2023.	-	Y	-	-	-	-	This control is applicable to Acquirers

63	28-Jul-22	Point 2 Point 3a	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/95 CO.DPSS.POLC.No.S-760/02-14-003/2022-23	CoF data purging	With effect from October 1, 2022, no entity in the card transaction / payment chain, other than the card issuers and / or card networks, shall store CoF data, and any such data stored previously shall be purged. There shall be no change in the effective date of implementation of the requirements - all entities, except card issuers and card networks, shall purge the CoF data before October 1, 2022.	CoFT	Y	Y	-	-	-	This control is applicable to Acquirers and Token Requestors / Merchants / Others
64	28-Jul-22	Point 4	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/95 CO.DPSS.POLC.No.S-760/02-14-003/2022-23	Non-compliance measures	Appropriate penal action, including imposition of business restrictions, shall be considered by the RBI in case of any non-compliance.	-	-	-	-	-	Y	-
65	21-Apr-23	Point 3c	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	CO.DPSS.POLC.No.S-65/02-14-003/2023-2024	Guest checkout transactions	Entities in the transaction/payment chain shall deploy an alternate solution for handling guest checkout transactions by October 31, 2023	CoFT	Y	Y	Y	Y	-	-

66	11-Feb-22	Point 2.ii	Tokenization - Card Transactions: System Audit	CO.DPSS.OVRST.No. S1428/06 -11-001/2021-2022	Guidelines to CPN	The auditors assessing CPNs' tokenization set-up shall also assess whether adequate controls are put in place to ensure certification of tokenization setup of token service participants.	-	-	-	Y	Y	-	-
67	11-Feb-22	Point 2.iii a	Tokenization - Card Transactions: System Audit	CO.DPSS.OVRST.No. S1428/06 -11-001/2021-2022	Guidelines to CPN	a) The system audit report (SAR) submitted by token service participants must contain item-wise compliance status on each requirement specified in extant guidelines on tokenization services issued by RBI.	Device and CoFT	Y	Y	Y	Y	-	-
68	11-Feb-22	Point 2.iii b	Tokenization - Card Transactions: System Audit	CO.DPSS.OVRST.No. S1428/06 -11-001/2021-2022	Guidelines to CPN	b) The auditors of a CPN shall also examine the SARs of token service participants to ensure that relevant areas are covered in the audit. Any observation raised in the SARs shall be tracked by the CPNs for timely closure.	-	-	-	Y	Y	-	-
69	11-Feb-22	Point 3	Tokenization - Card Transactions: System Audit	CO.DPSS.OVRST.No. S1428/06 -11-001/2021-2022	Guidelines to CPN	a) As regards the tokenization SAR of CPNs submitted to RBI, the report must contain item-wise response from the auditors on each requirement specified in the above as well as other relevant circulars.	-	-	-	Y	Y	-	-

						b) In case the CPN offers Card-on-File Tokenization (CoFT), item-wise compliance status for related RBI instructions shall also be specified in the SAR. Further, the report shall contain a certificate issued by the auditors, indicating the deficiencies observed in the SARs of token service participants.								
70	11-Feb-22	Point 2.i.	Tokenization - Card Transactions: System Audit	CO.DPSS.OVRST.No. S1428/06 -11-001/2021-2022	Guidelines to CPN	It is the responsibility of an authorized CPN to ensure that the token requestors and any other participants (cumulatively termed as token service participants, hereafter) involved in providing its card tokenization services to customers, adhere to RBI instructions on card tokenization, data storage, system audit and other relevant instructions.	Device and CoFT	Y	Y	Y	Y	-	-	
71	25-Aug-21	Point 1	Tokenization - Card Transactions : Extending the Scope of Permitt	RBI/2021-22/92 CO.DPSS.POLC.No.S -469/02-14-003/2021-22	Extension to other devices	Card transactions, permitting authorized card networks to offer card tokenization services to any token requestor, subject to the conditions lied card holders	-	-	-	Y	Y	-	-	

			ed Devices												
7 2	07-Sep-21	Point 1	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/202122/96 CO.DPSS. POLC.No.S-516/02-14003/202122	Extension to other devices	Initially limited to mobile phones and tablets, tokenization facility was subsequently extended to laptops, desktops, wearables (wrist watches, bands, etc.), IoT devices, etc.	-	-	-	-	-	Y	-		
7 3	07-Sep-21	4.c Point 5	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/202122/96 CO.DPSS. POLC.No.S-516/02-14003/202122	References	Reference is also invited to our circulars DPSS.CO.PD.No.1810/02.14.008/2019-20 dated March 17, 2020 (as updated from time to time) and CO.DPSS.POLC.No.S 33/02-14-008/2020-2021 dated 31 March 2021 on "Guidelines on Regulation of Payment Aggregators and Payment Gateways", advising that neither the authorized Payment Aggregators (PAs) nor the merchants on-boarded by them shall store customer card credentials [also known as Card-on-File (CoF)]. Conditions to be fulfilled for offering CoFT services	-	-	-	-	-	Y	-		

74	21-Apr-23	Point 1	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	CO.DPSS.POLC.No. S-65/02-14-003/2023-24	References	<p>Reference is invited to the following RBI circulars;</p> <p>I. DPSS.CO.PD.No.1810 / 02.14.008 / 2019-20 dated March 17 , 2020 and CO.DPSS.PPLC.No.S33 /02-14-008 / 2020-2021 dated March 31,2021 on “Guidelines on Regulation of Payment Aggregators and Payment Gateways”,</p> <p>II. CO.DPSS.POLC.No. S-516 / 02-14-003 / 2021-22 dated 7 September 2021 on “Tokenization - Card Transactions : Permitting Card-on-File Tokenization (CoFT) Services”, and,</p> <p>III. CO.DPSS.POLC.No S-1211 / 02-14-003 / 2021-21 dated 23 December 2021, CO.DPSS.POLC.No S-567 / 02-14-003 / 2022-23 dated June 24, 2022 and CO.DPSS.POLC.No S-760 / 02-14-003 / 2022-23 dated 28 July 2022 on “Restriction on Storage of Actual Card Data[i.e. Card-in-File(CoF)].</p>						Y	
----	-----------	---------	--	---	------------	--	--	--	--	--	--	---	--

75	21-Apr-23	Point 2	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	CO.DPSS.POLC.No. S-65/02-14-003/2023-24	Guest checkout transactions	In terms of the above circulars, with effect from 1 October 2022 no entity in the card transaction / payment chain, other than the card issuers and / or card networks, shall store CoF data, and any data stored previously shall be purged. Further, they provide for CoF facility and prescribe certain interim measures in respect of transactions where cardholders decide to enter the card details manually at the time of undertaking the transaction (commonly referred to as "guest check out transactions")	-	-	-	-	-	Y	-
76	21-Apr-23	Point 3	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	CO.DPSS.POLC.No. S-65/02-14-003/2023-24	Guest checkout transactions	On a review of the preparedness for implementing alternate solution for the guest checkout transactions, as also keeping in view that most online / e-commerce card transactions being undertaken these days are CoFT based the following measures are advised for guest checkout transactions -	-	-	-	-	-	Y	-

77	20-Dec-23	Point 1	Card-on-File Tokenization (CoFT) - Enabling Tokenization through Card Issuing Banks	RBI/2023-24/91 CO.DPSS.POLC.No.S-919/02-14-003/2023-24	Guidelines	<p>The card tokenization services are being currently provided by card issuers and card networks in terms of Reserve Bank of India circulars DPSS.CO.PD No.1463/02.14.003/2018-19 dated 8 January 2019 on "Tokenization - Card transactions", CO.DPSS.POLC.No.S-516/02-14-003/2021-22 dated September 07, 2021 on "Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services" and CO.DPSS.POLC.No.S-567/02-14-003/2022-23 dated 24 June 2022 on "Restriction on Storage of Actual Card Data [i.e. Card-onFile (CoF)]". As announced in the Statement on Development and Regulatory Policies dated 6 October 2023, it has been decided to enable CoFT directly through card issuing banks / institutions also. This will provide cardholders with an additional choice to tokenize their cards for multiple merchant sites through a single process.</p>						Y	
----	-----------	---------	---	--	------------	--	--	--	--	--	--	---	--

						Detailed requirements for the same are listed in the Annex								
78	20-Dec-23	Annexure 7	Card-on-File Tokenization (CoFT) - Enabling Tokenization through Card Issuing Banks	RBI/2023-24/91 CO.DPSS.POLC.No.S -919/02-14-003/2023-24	Enable tokenization through card issuing banks	All other provisions of RBI circulars dated 8 January 2019, 25 August 2021, 7 September 2021 and 28 July 2022 shall remain applicable.	-	-	-	-	-	Y	-	
79	28-Jul-22	Point 3	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/77 CO.DPSS.POLC.No.S -567/02-14-003/2022-23	Guidelines	On a review of the issues involved and after detailed discussions thereon with all stakeholders, as also keeping in view that sufficient time has elapsed since the requirements were specified, the following are advised -	-	-	-	-	-	Y	-	
80	28-Jul-22	Point 1	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/95 CO.DPSS.POLC.No.S -760/02-14-003/2022-23	References	Reference is invited to RBI circulars DPSS.CO.PD.No.1810/02.14.008/2019-20 dated 17 March, 2020 and CO.DPSS.POLC.No.S 33/02-14-008/2020-2021 dated 31 March, 2021 on "Guidelines on Regulation of Payment	-	-	-	-	-	Y	-	

						Aggregators and Payment Gateways”, circular CO.DPSS.POLC.No.S 516/02-14-003/2021-22 dated 7 September, 2021 on “Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services” and, circulars CO.DPSS.POLC.No.S 1211/02-14-003/2021-22 dated 23 December, 2021 and CO.DPSS.POLC.No.S-567/02-14-003/2022-23 dated June 24, 2022 on “Restriction on Storage of Actual Card Data [i.e. Card-onFile (CoF)].								
81	21-Apr-23	Additional Control	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	CO.DPSS.POLC.No. S-65/02-14-003/2023-24	Guest checkout transactions	Complete and ongoing compliance with the above by all entities involved, shall be the responsibility of card networks. Appropriate penal action, including imposition of business restrictions, shall be considered by the RBI in case of any non-compliance.	-	-	-	Y	Y	-	-	
82	11-Feb-22	Point 1	Tokenization - Card Transactions: System Audit	CO.DPSS.OVRST.No. S1428/06 -11-001/2021-2022	Guidelines to CPN	A reference is invited to paragraph 6 of the circular on Tokenization - Card transactions dated 8 January 2019 that mandates authorized card	Device and CoFT	Y	Y	Y	Y	-	-	

						payment networks CPNs to put in place a mechanism for periodic system (including security) audit at frequent intervals, at least annually, of all entities involved in providing its card tokenization services to customers.								
83	24-Jun-22	Point 1	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/77 CO.DPSS.POLC.No.S-567/02-14-003/2022-23	References	Reference is invited to RBI circulars DPSS.CO.PD.No.1810/02.14.008/2019-20 dated 17 March, 2020 and CO.DPSS.POLC.No.S33/02-14-008/2020-2021 dated 31 March, 2021 on “Guidelines on Regulation of Payment Aggregators and Payment Gateways”, and CO.DPSS.POLC.No.S-516/02-14-003/2021-22 dated 7 September, 2021 on “Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services”.	-	-	-	-	-	Y	-	
84	24-Jun-22	Point 2	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/77 CO.DPSS.POLC.No.S-567/02-14-003/2022-23	CoF data purging	In terms of these circulars, with effect from 1 January, 2022, no entity in the card transaction / payment chain, other than the card issuers and / or card networks, shall store the CoF data,	-	-	-	-	-	Y	-	

						and any such data stored previously shall be purged. Subsequently, to allow more time to the industry stakeholders for devising alternate mechanism(s) to handle any use case or post transaction activity, this timeline was extended to 30 June, 2022, vide circular CO.DPSS.POLC.No.S-1211/02-14-003/2021-22 dated 23 December, 2021 on "Restriction on storage of actual card data [i.e. Card-on-File (CoF)]".									
85	04-Jul-23	Point 1	Tokenization - Card Transactions - System Audit	CO.DPSS.OVRST.No. S343/06-11-005/2023-24	References	A reference is invited to paragraph 6 of the circular on "Tokenization – Card transactions" dated 8 January 2019 that mandates authorized card payment networks (CPNs) to put in place a mechanism for periodic system (including security) audit at frequent intervals, at least annually, of all entities involved in providing card tokenization services to customers. Reference is also drawn to RBI letters CO.DPSS.OVRST.No. S1428/06-11-	-	-	-	-	-	Y	-		

						001/2021-2022 dated 11 February 2022 and CO.DPSS.OVRST.No S1395 / 06-11-005 / 2022-2023 dated 23 November 2022								
86	04-Jul-23	Point 2	Tokenization - Card Transactions - System Audit	CO.DPSS.OVRST.No. S343/06-11-005/2023-24	Guidelines to CPN	In view of requests received from the industry, it has been decided to standardise the tokenization audit period of CPNs. Accordingly, authorized CPNs are advised as follows	-	-	-	-	-	Y	-	
87	04-Jul-23	Point 2.1	Tokenization - Card Transactions - System Audit	CO.DPSS.OVRST.No. S343/06-11-005/2023-24	Guidelines to CPN	In case the tokenization audit is conducted on an annual basis, the audit period shall be for the period of April to March.	Device and CoFT	Y	Y	Y	Y	-	-	
88	04-Jul-23	Point 2.2	Tokenization - Card Transactions - System Audit	CO.DPSS.OVRST.No. S343/06-11-005/2023-24	Guidelines to CPN	For easy transition, as a one-time measure, the CPNs, whose audit period fall in the interim period shall submit the report covering period till March 2024. For eg, an entity following audit period of January 2023 to December 2023, shall submit an audit report for the period of January 2023 to March 2024.	-	-	-	-	-	Y	-	
89	04-Jul-23	Point 3	Tokenization - Card Transactions - System Audit	CO.DPSS.OVRST.No. S343/06-11-005/2023-24	Guidelines to CPN	Further, on recent examination of tokenization audit reports of CPNs, several deficiencies have been observed regarding the scope and coverage of the	Device and CoFT	Y	Y	Y	Y	-	-	

						audit reports of CPNs as well as token requestors and any other participants. In this connection, the CPNs are advised to tighten the tokenization audit mechanism to ensure strict adherence with RBI instructions.								
90	04-Jul-23	Point 4, 5	Tokenization - Card Transactions - System Audit	CO.DPSS.OVRST.No. S343/06-11-005/2023-24	Guidelines to CPN	1. This letter may be placed before the board in the next meeting. 2. Please acknowledge the receipt of this letter.	-	-	-	-	-	Y	-	
91	25-Sep-25	Point 7	Reserve Bank of India (Authentication mechanisms for digital payments transactions) Directions, 2025	CO.DPSS.POLC.No. S 668/02-14-015/2025-2026	Interoperability / Open Access	System Providers and System Participants shall offer authentication or tokenisation service that is accessible to all the applications / token requestors functioning in that operating environment for all use cases / channels or token storage mechanisms. Note - i. Operating environment includes device hardware, operating system, etc. ii. The terms, 'tokenisation', 'token requestor',	Device and CoFT	Y	Y	Y	Y	-	Applicable to all System Provider and System Participants. Obtain and review technical documentation, API specifications, and integration guidelines to verify that authentication or tokenization services offered by the system provider/p	

						<p>'use cases/channels' and 'token storage mechanisms' shall have the same meaning as assigned to them in the RBI directions on "Tokenisation - Card Transactions" dated January 08, 2019, as amended from time to time.</p>							<p>participant are interoperable and accessible to all token requestors within the same operating environment (device, hardware, OS). Evidence such as API documentation, integration logs, onboarding records and architecture design documents can be collected.</p> <p><i>Note: This control is "optional" for validation since the compliance needs to be achieved by 1 April 2026.</i></p>
--	--	--	--	--	--	--	--	--	--	--	--	--	---

9 2	07-Sep-21	3.b	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S -516/02-14-003/2021-22	Tokenization - de-tokenization service	<i>Control Based on Regulator Queries: Does the card issuer have access to token number (Device and/or CoFT) during any stage of transaction processing? Evidence must be captured appropriately for validation.</i>	Device and CoFT	Y	-	-	Y	-	Applicable for all card issuing entities All entities have gone live with masking solution - hence a check must be done to verify if historic token data stored by issuer has been deleted
9 3	20-Dec-23	Annexure 6	Card-on-File Tokenization (CoFT) - Enabling Tokenization through Card Issuing Banks	RBI/2023-24/91 CO.DPSS.POLC.No.S -919/02-14-003/2023-24	Enable tokenization through card issuing banks	<i>Control Based on Regulator Queries: Does the card issuer store token number (Device and/or CoFT) during or after the transaction processing? Evidence must be captured appropriately for validation.</i>	Device and CoFT	Y	-	-	Y	-	Applicable for all card issuing entities All entities have gone live with masking solution - hence a check must be done to verify if historic token data stored by issuer has been deleted

94	07-Sep-21	Annex 6	Tokenization - Card Transactions: Permitting Card-on-File Tokenization (CoFT) Services	RBI/2021-22/96 CO.DPSS.POLC.No.S-516/02-14-003/2021-22	Unique token	<p><i>Control Based on Regulator Queries: How did the auditor validate if unique IDs are assigned to each end merchant on-boarded by the TR?</i></p> <p><i>How is it ensured that these unique IDs created for each end merchant are also tagged to the initiation of separate token requests for each merchant?</i></p>	CoFT	-	Y	-	-	-	-
95	08-Jan-19	Annex 1 definition	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Unique token	<p><i>Control Based on Regulator Queries: Does the TR utilize token generated for merchant A in place of merchant B? If no, how is the same ensured.</i></p>	CoFT	-	Y	-	-	-	-
						<p><i>Case A : For cases where entity requests/processes CoF Token transactions for merchants including their sister merchant entities -</i></p> <p><i>Validate whether a unique token is requested/utilized for each merchant (including distinct merchants who may be sister companies or group companies) during creation and subsequent tokenized transaction</i></p>	CoFT	-	Y	-	-	-	e.g. if entity is processing transactions for a large conglomerate, business group with multiple businesses e.g. telecom, DTH, Bank, Wallet, Streaming, etc., are distinct tokens

					<p>requests.</p> <p><i>Note: For the purpose of CoFT, the token shall be unique for a combination of card, token requestor and merchant. The word “merchant” wherever used in the mentioned circular refers to the end-merchant. However, in case of an e-commerce marketplace entity, merchant refers to the said e-commerce entity. Further, token requestor and merchant may or may not be the same entity.</i></p>							<p>been provisioned for transactions at each of these merchants (each business within the conglomerate, business group?)</p>
					<p><i>Case B : For cases where entity requests/processes CoF Token transactions for any of their own sister/group companies:</i></p> <p><i>Validate whether a unique token is requested/utilized for each group/sister entity (legal entity) during creation and subsequent tokenized transaction requests.</i></p> <p><i>Note: For the</i></p>	CoFT	-	Y	-	-	-	<p>e.g. if entity is processing transactions for two sister entities on your mobile app/website where Sister entity A provides telecom services and Sister entity B provides prepaid wallet</p>

A-Validation

Domain	Guideline	Testing criteria	Tokenization type (Device/CoFT/Device and CoFT)	Card Issuer	Token requestor / merchant	Token service provider	Acquirer	Others	Remarks
Registration by customer	All extant instructions of Reserve Bank on safety and security of card transactions, including the mandate for Additional Factor of Authentication (AFA) / PIN entry shall be applicable for tokenised card transactions also.	To be validated	Device and CoFT	Y	Y	Y	Y	Y	
Miscellaneous	No charges should be recovered from the customer for availing this service.	To be validated	Device and CoFT	Y	Y	Y	Y	Y	
Unique token	The token shall be unique for a combination of card, token requestor and device (referred hereafter as "identified device").	To be validated	Device		Y	Y			For token requestors validation should be done to check if unique tokens are assigned to merchants.
Tokenization - de-tokenization service	Tokenisation and de-tokenisation shall be performed only by the authorised card network service	To be validated	Device and CoFT			Y			
Tokenization - de-tokenization service	Recovery of original Primary Account Number (PAN) should be feasible for the authorised card network only.	To be validated	Device and CoFT			Y			
Tokenization - de-tokenization service	Adequate safeguards shall be put in place to ensure that PAN cannot be found out from the token and vice versa, by anyone except the card network. Integrity of token generation process shall be ensured at all times. <i>Note: This control must be tested by auditors for banks that receive and store the tokens from CPN. Please specifically call out if the bank has access to the token and/or is storing the token.</i>	To be validated	Device and CoFT	Y		Y		Y	Applicable for card networks and entities (e.g. issuers) that may store both PAN and token Note: Issuers should store only store the masked PAN received from the networks. A check must be done to validate the same.

Tokenization - de-tokenization service	Tokenization and de-tokenization requests should be logged by the card network and available for retrieval, if required.	To be validated	Device and CoFT			Y			Applicable to card issuers only if they create tokens (tokenize and detokenize cards).
Tokenization - de-tokenization service	Actual card data, token and other relevant details shall be stored in a secure mode. <i>Note: Auditor must specify any and every card information such as card expiry, cardholder name etc. being stored by the token service participant.</i>	To be validated	Device and CoFT	Y	Y	Y	Y	Y	
Tokenization - de-tokenization service	Token requestors shall not store PAN or any other card detail.	To be validated	Device and CoFT		Y				
Certification of systems of card issuers /acquirers, token requestors and their app, etc.	Card network shall get the token requestor certified for (a) token requestor's systems, including hardware deployed for this purpose, (b) security of token requestor's application, (c) features for ensuring authorised access to token requestor's app on the identified device, and (d) other functions performed by the token entity, including customer onboarding, token provisioning and storage, data storage, transaction processing, etc.	To be validated	Device and CoFT		Y	Y			While the point is to be exclusively tested for card networks, Auditors reviewing token requestors must validate if such certification is undertaken actively by these entities.
Certification of systems of card issuers /acquirers, token requestors and their app, etc.	Card networks shall get the card issuers / acquirers, their service providers and any other entity involved in payment transaction chain, certified in respect of changes done for processing tokenized card transactions by them.	To be validated	Device and CoFT	Y	Y	Y	Y	Y	While the point is to be exclusively tested for card networks, auditors reviewing other entities (card issuers / acquirers, their service providers and any other entity) must validate if such certification is undertaken actively by these entities.
Certification of systems of card issuers /acquirers, token	Card network shall ensure that certification of systems of card issuers / acquirers, token requestors and their application shall conform to international best practices / globally accepted standards.	To be validated	Device and CoFT	Y	Y	Y	Y	Y	While the point is to be exclusively tested for card networks,

requestors and their app, etc.									auditors reviewing other entities must validate if such certification is undertaken actively by these entities.
Registration by customer	Registration of card on token requestor's app shall be done only with explicit customer consent through Additional Factor of Authentication (AFA), and not by way of a forced / default / automatic selection of check box, radio button, etc.	To be validated	Device and CoFT		Y	Y		Y	Applicable to issuers only if they are offering an application through which cardholders can tokenize cards
Registration by customer	AFA validation during card registration, as well as, for authenticating any transaction, shall be as per extant Reserve Bank instructions for authentication of card transactions. <i>Note: The auditor must validate AFA for sample cases including only tokenization, tokenized card transaction and tokenization + transaction.</i>	To be validated	Device and CoFT	Y		Y			
Registration by customer	Customers shall have option to register / de-register their card for a particular use case, i.e., contactless, QR code based, in-app payments, etc.	To be validated	Device		Y				Applicable for device token requestors having a customer facing application. Applicable to issuers only if they are offering an application through which cardholders can tokenize cards
Registration by customer	Customers shall be given option to set and modify per transaction and daily transaction limits for tokenized card transactions.	To be validated	Device and CoFT	Y					
Registration by customer	Suitable velocity checks (i.e., how many such transactions will be allowed in a day / week / month) may be put in place by card issuers / card network as considered appropriate, for tokenized card transactions.	To be validated	Device and CoFT	Y					

Registration by customer	For performing any transaction, the customer shall be free to use any of the cards registered with the token requestor app.	To be validated	Device and CoFT						Applicable for token requestors having a customer facing application Applicable to issuers only if they are offering an application through which cardholders can tokenize cards
Secure storage of tokens	Secure storage of tokens and associated keys by token requestor on successful registration of card shall be ensured.	To be validated	Device and CoFT						Applicable for token requestors
Customer service and dispute resolution	Card issuers shall ensure easy access to customers for reporting loss of "identified device" or any other such event which may expose tokens to unauthorized usage.	To be validated	Device		Y				Applicable for card issuing entities
Customer service and dispute resolution	Card network, along with card issuers and token requestors, shall put in place a system to immediately deactivate unauthorized/exposed tokens and associated keys.	To be validated	Device and CoFT		Y	Y	Y		Applicable for card networks, issuing entities and token requestors
Customer service and dispute resolution	Dispute resolution process shall be put in place by card network for tokenized card transactions.	To be validated	Device and CoFT				Y		Applicable for card networks
Safety and security of transactions	Card network shall put in place a mechanism to ensure that the transaction request has originated from an "identified device".	To be validated	Device and CoFT				Y		Applicable for card networks
Safety and security of transactions	Card network shall: a) ensure monitoring to detect any malfunction, anomaly, suspicious behaviour, or the presence of unauthorized activity within the tokenization process and; b) implement a process to alert all stakeholders.	To be validated	Device and CoFT				Y		Applicable for card networks
Safety and security of transactions	Based on risk perception, etc., card issuers may decide whether to allow cards issued by them to be registered by a token requestor.	To be validated	Device and CoFT		Y				Applicable for card issuers

Tokenization - de-tokenization service	Card issuers can offer card tokenisation services as Token Service Providers .	To be validated	Device and CoFT	Y					Applicable for Token service providers
Tokenization - de-tokenization service	The facility of tokenisation shall be offered by the Token Service Providers only for the cards issued by / affiliated to them.	To be validated	Device and CoFT			Y			Applicable for Token service providers. Applicable to card issuers only if they create tokens (tokenize and detokenize cards).
Tokenization - de-tokenization service	The ability to tokenise and de-tokenise card data shall be with the same Token Service Providers.	To be validated	Device and CoFT			Y			Applicable for Token service providers. Applicable to card issuers only if they create tokens (tokenize and detokenize cards).
Registration by customer	Tokenisation of card data shall be done with explicit customer consent requiring Additional Factor of Authentication (AFA) validation by card issuer.	To be validated	Device and CoFT	Y	Y	Y			
Transaction tracking/ reconciliation	For transaction tracking and / or reconciliation purposes, entities can store limited data - last four digits of actual card number and card issuer's name - in compliance with the applicable standards.	To be validated	Device and CoFT		Y		Y	Y	Applicable for all entities except issuers and card networks
Unique token	For the purpose of CoFT, the token shall be unique for a combination of card, token requestor and merchant	To be validated	CoFT		Y	Y			Applicable for card networks. Additionally for token requestors validation should be done to check if unique tokens are assigned to merchants. Applicable to card issuers only if they create tokens (tokenize and detokenize cards).

Registration by customer	If card payment for a purchase transaction at a merchant is being performed along with the registration for CoFT, then AFA validation may be combined.	To be validated	Device and CoFT	Y		Y			Applicable to card issuers and networks
Token de-registration	The merchant shall give an option to the cardholder to de-register the token.	To be validated	Device and CoFT		Y				Applicable to merchants and token requestors that have a customer facing application
Token de-registration	Further, a token requestor having direct relationship with the cardholder shall: a) list the merchants in respect of whom the CoFT has been opted through it by the cardholder b) provide an option to deregister any such token	To be validated	CoFT		Y				
Token de-registration	a) A facility shall also be given by the card issuer to the cardholder to view the list of merchants in respect of whom the CoFT has been opted by her / him, and to deregister any such token. b) This facility shall be provided through one or more of the following channels - mobile application, internet banking, Interactive Voice Response (IVR) or at branches / offices.	To be validated	CoFT	Y					
Registration by customer	Whenever a card is renewed or replaced, the card issuer shall seek explicit consent of the cardholder for linking it with the merchants with whom (s)he had earlier registered the card.	To be validated	CoFT	Y					
Unique token	The Token service provider shall put in place a mechanism to ensure that the transaction request has originated from the merchant and the token requestor with whom the token is associated.	To be validated	CoFT			Y			Applicable to card issuers only if they create tokens (tokenize and detokenize cards).
Miscellaneous	In addition to tokenization, industry stakeholders may devise alternate mechanism(s) to handle any use case (including recurring e-mandates, EMI option, etc.) or post transaction activity (including chargeback handling, dispute resolution, reward / loyalty programme, etc.) that currently involves / requires storage of CoF data by entities other than card issuers and card networks. <i>Note: Auditors must test specific samples for above cases.</i>	To be validated	Device and CoFT		Y	Y	Y		

CoF data purging	<p>It has been decided to extend the timeline for storing of CoF data by three months, i.e., till September 30, 2022, after which such data shall be purged.</p> <p>There shall be no change in the effective date of implementation of the requirements - all entities, except card issuers and card networks, shall purge the CoF data before October 1, 2022.</p> <p>With effect from October 1, 2022, no entity in the card transaction / payment chain, other than the card issuers and / or card networks, shall store CoF data, and any such data stored previously shall be purged.</p>	To be validated	Device and CoFT				Y	Y	Y	
Guest checkout transactions	<p>Only for guest checkout transaction -</p> <p>a) Other than the card issuer and the card network, the merchant or its Payment Aggregator (PA) involved in settlement of such transactions, can save the CoF data for a maximum period of T+2 days ("T" being the transaction date) or till the settlement date, whichever is earlier.</p> <p>b) This data shall be used only for settlement of such transactions, and must be purged thereafter.</p>	To be validated	Device and CoFT				Y		Y	
Guest checkout transactions	<p>a) The acquiring banks shall not store CoF data for guest checkout transactions beyond a period of T+180 days ("T" being the transaction date).</p> <p>b) For such transactions processed before the April 21, 2023, compliance with the T+180 days' timeline shall be ensured by June 30, 2023.</p> <p>c) Additionally, only acquiring banks are permitted to store actual card details used for guest checkout transaction (historical) in offline storing mediums.</p>	To be validated	Device and CoFT					Y		
Guest checkout transactions	Entities in the transaction/payment chain shall deploy an alternate solution for handling guest checkout transactions by January 31, 2024	To be validated	Device and CoFT		Y	Y	Y	Y	Y	

Extension to other devices	<p>The scope of tokenization has been extended to include consumer devices - laptops, desktops, wearables (wrist watches, bands, etc.), Internet of Things (IoT) devices, etc.</p> <p>All other provisions of the circular referred to above shall continue to be applicable.</p>	To be validated	Device	Y	Y	Y	Y	Y	
Enable tokenization through card issuing banks	<p>Does the card issuing entity provide CoF tokens option for multiple merchants through mobile/internet banking channels? (note: Issuing bank may/may not issue tokens in order to provide this feature)</p> <p>a) CoFT generation shall be done only on explicit customer consent, and with AFA validation. If the cardholder selects multiple merchants for which to tokenise his/her card, AFA validation may be combined for all these merchants.</p> <p>b) The tokens thus generated shall be made available on the merchant's payment page, in the cardholder's account with the merchant.</p> <p>c) The cardholder may tokenise the card at any time of his convenience, either on receipt of the new card or later.</p> <p>d) The card issuer shall provide a complete list of merchants for whom it can provide tokenisation services. The cardholders shall select the merchants with whom he/she wishes to maintain tokens. (Alternatively - "The cardholder can make his selection from the list").</p> <p>e) The card token so issued may be either by the card network or the issuer or both.</p>	To be validated	CoFT	Y		Y			Control is applicable only if the Issuer provides this service. Issuer may or may not act as a token service provider for this to be tested
India Data localization	<p>1. All system providers (entities involved in payment lifecycle) shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India.</p> <p>2. No payment data element pertaining to the end-to-end payment string can be stored abroad in any form, including hashed, masked, encrypted or tokenized.</p>	To be validated	Device and CoFT	Y	Y	Y	Y	Y	

Token access	Does the card issuer have access to token number (Device and/or CoFT) during any stage of transaction processing ? Evidence must be captured appropriately for validation.	To be validated	Device and CoFT		Y					Applicable for all card issuing entities All entities have gone live with masking solution - hence a check must be done to verify if historic token data stored by issuer has been deleted
Token storage	Does the card issuer store token number (Device and/or CoFT) during or after the transaction processing ? Evidence must be captured appropriately for validation.	To be validated	Device and CoFT		Y					Applicable for all card issuing entities All entities have gone live with masking solution - hence a check must be done to verify if historic token data stored by issuer has been deleted
Single token	How did the auditor validate if unique IDs are assigned to each end merchant on-boarded by the TR? How is it ensured that these unique IDs created for each end merchant are also tagged to the initiation of separate token requests for each merchant?	To be validated	CoFT			Y				
Single token	Does the TR utilize token generated for merchant A in place of merchant B? If no, how is the same ensured.	To be validated	CoFT			Y				

	<p>Case A : For cases where entity requests/processes CoF Token transactions for merchants including their sister merchant entities -</p> <p>Validate whether a unique token is requested/utilized for each merchant (including distinct merchants who may be sister companies or group companies) during creation and subsequent tokenized transaction requests.</p> <p>Note: For the purpose of CoFT, the token shall be unique for a combination of card, token requestor and merchant. The word “merchant” wherever used in the mentioned circular refers to the end-merchant. However, in case of an e-commerce marketplace entity, merchant refers to the said e-commerce entity. Further, token requestor and merchant may or may not be the same entity.</p>	To be validated	CoFT		Y		e.g. if entity is processing transactions for a large conglomerate, business group with multiple businesses e.g. telecom, DTH, Bank, Wallet, Streaming, etc., are distinct tokens been provisioned for transactions at each of these merchants (each business within the conglomerate, business group?)
	<p>Case B : For cases where entity requests/processes CoF Token transactions for any of their own sister/group companies:</p> <p>Validate whether a unique token is requested/utilized for each group/sister entity (legal entity) during creation and subsequent tokenized transaction requests.</p> <p>Note: For the purpose of CoFT, the token shall be unique for a combination of card, token requestor and merchant. The word “merchant” wherever used in the mentioned circular refers to the end-merchant. However, in case of an e-commerce marketplace entity, merchant refers to the said e-commerce entity. Further, token requestor and merchant may or may not be the same entity.</p>	To be validated	CoFT		Y		e.g. if entity is processing transactions for two sister entities on your mobile app/website where Sister entity A provides telecom services and Sister entity B provides prepaid wallet (wallet load transactions) for the same card, have distinct tokens been provisioned for transactions at each of these entities (merchants)?

B-Information Control:

TSP auditor is required to consider and cover the below informational controls during the audit and include the same in the report.

Sr No	Guideline Date	Para/section	RBI document name	RBI document number	Domain	Guideline
1	08-Jan-19	Leading paragraph	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Guidelines	Continuing the efforts to improve safety and security of card transactions, Reserve Bank of India had permitted card networks for tokenization in card transactions for a specific use case. For the present, this facility shall be offered through mobile phones / tablets only. Its extension to other devices will be examined later based on experience gained.
2	08-Jan-19	Point 2	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Permission to tokenize	It has now been decided to permit authorised card payment networks to offer card tokenization services to any token requestor (i.e., third party app provider), subject to the conditions listed in Annex 1.
3	08-Jan-19	Point 2	Tokenization - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Guidelines	This permission extends to all use cases / channels [e.g., Near Field Communication (NFC) / Magnetic Secure Transmission (MST) based contactless transactions, in-app payments, QR code-based payments, etc.] or token storage mechanisms (cloud, secure element, trusted execution environment, etc.).
4	08-Jan-19	Point 4	Tokenisation - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Guidelines	All other instructions related to card transactions shall be applicable for tokenised card transactions as well. The ultimate responsibility for the card tokenisation services rendered rests with the authorised card networks.

5	08-Jan-19	Point 6 and 7	Tokenisation - Card transactions	DPSS.CO.PDNo.1463/02.14.003/2018-19	Guidelines	<p>- Before providing card tokenisation services, authorised card payment networks shall put in place a mechanism for periodic system (including security) audit at frequent intervals, at least annually, of all entities involved in providing card tokenisation services to customers.</p> <p>- This system audit shall be undertaken by empanelled auditors of Indian Computer Emergency Response Team (CERT-In) and all related instructions of Reserve Bank in respect of system audits shall also be adhered to.</p> <p>- A copy of this audit report shall be furnished to the Reserve Bank, with comments of auditors on deviations, if any, from the conditions listed in Annex 1, along with the compliance thereto.</p> <p>- Further, a report on the details provided in Annex 2 shall be submitted at monthly intervals to the Chief General Manager, Reserve Bank of India, Department of Payment and Settlement Systems, Central Office, Mumbai and by email.</p> <p>-This directive is issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007).</p>
6	07-Sep-21	3.a	Tokenisation - Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services	DPSS.CO.PDNo.1463/02.14.003/2018-19	Guidelines	<p>On a review of the tokenisation framework and to enable cardholders to benefit from the security of tokenised card transactions as also the convenience of CoF, it has been decided to effect the following enhancements:</p> <p>a) Extend the device-based tokenisation framework referred to at paragraph above to CoF Tokenisation (CoFT) as well.</p>
7	07-Sep-21	3.f	Tokenisation - Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services	DPSS.CO.PDNo.1463/02.14.003/2018-19	References	Additional requirements relating to CoFT are listed in the Annex.
8	07-Sep-21	4.a	Tokenisation - Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services	DPSS.CO.PDNo.1463/02.14.003/2018-19	CoF data purging	With effect from January 1, 2022, no entity in the card transaction / payment chain, other than the card issuers and / or card networks, shall store the actual card data. Any such data stored previously shall be purged.
9	07-Sep-21	4.c	Tokenisation - Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services	RBI/202122/96 CO.DPSS. POLC.No.S-516/02-14003/202122	Monitor compliance	Complete and ongoing compliance with the above by all entities involved, shall be the responsibility of the card networks.
10	07-Sep-21	Annex 7 and 8	Tokenisation - Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services	RBI/202122/96 CO.DPSS. POLC.No.S-516/02-14003/202122	Conditions to be fulfilled for offering CoFT	All other provisions of the RBI circulars dated January 8, 2019 and August 25, 2021 shall be applicable. The TSPs shall monitor and ensure compliance in this regard.

					services	
11	23-Dec-21	Point 2.a	Restriction on storage of actual card data [i.e. Card-on-File (CoF)]	RBI/2021-2022/142 CO.DPSS.POLC.No.S-1211/02-14-003/2021-22	CoF data purging	The timeline for storing of CoF data is extended by six months, i.e., till June 30, 2022; post this, such data shall be purged;
12	24-Jun-22	Point 3	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/77 CO.DPSS.POLC.No.S-567/02-14-003/2022-23	Points to note	<p>On a review of the issues involved and after detailed discussions with all stakeholders, it is observed that considerable progress has been made in terms of token creation.</p> <p>Transaction processing based on these tokens has also commenced, though it is yet to gain traction across all categories of merchants.</p> <p>Further, an alternate system in respect of transactions where cardholders decide to enter the card details manually at the time of undertaking the transaction (commonly referred to as “guest checkout transactions”) has not been implemented by the industry stakeholders, so far.</p>
13	28-Jul-22	Point 3.b.i	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/95 CO.DPSS.POLC.No.S-760/02-14-003/2022-23	Guest checkout transactions	<p>For cases where cardholders decide to enter the card details manually at the time of undertaking the transaction (commonly referred to as “guest checkout transactions”), the following are being permitted as an interim measure -</p> <p>i) Other than the card issuer and the card network, the merchant or its Payment Aggregator (PA) involved in settlement of such transactions, can save the CoF data for a maximum period of T+4 days (“T” being the transaction date) or till the settlement date, whichever is earlier.</p> <p>This data shall be used only for settlement of such transactions, and must be purged thereafter.</p>
14	28-Jul-22	Point 3.b.ii	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/95 CO.DPSS.POLC.No.S-760/02-14-003/2022-23	Guest checkout transactions	For handling other post-transaction activities, acquiring banks can continue to store CoF data until January 31, 2023.
15	28-Jul-22	Point 4	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	RBI/2022-23/95 CO.DPSS.POLC.No.S-760/02-14-003/2022-23	Non-compliance measures	Appropriate penal action, including imposition of business restrictions, shall be considered by the RBI in case of any non-compliance.
16	21-Apr-23	Point 3c	Restriction on Storage of Actual Card Data [i.e. Card-on-File (CoF)]	CO.DPSS.POLC.No. S-65/02-14-003/2023-2024	Guest checkout transactions	Entities in the transaction/payment chain shall deploy an alternate solution for handling guest checkout transactions by October 31, 2023
17	11-Feb-22	2.ii	Tokenisation - Card Transactions: System Audit	CO.DPSS.OVRST.No.S1428/06 -11-001/2021-2022	Guidelines to CPN	The auditors assessing CPNs’ tokenisation set-up shall also assess whether adequate controls are put in place to ensure certification of tokenisation setup of token service participants.

18	11-Feb-22	2.iii	Tokenisation - Card Transactions: System Audit	CO.DPSS.OVRST.No.S1428/06 -11-001/2021-2022	Guidelines to CPN	<p>a) The system audit report (SAR) submitted by token service participants must contain item-wise compliance status on each requirement specified in extant guidelines on tokenisation services issued by RBI.</p> <p>b) The auditors of a CPN shall also examine the SARs of token service participants to ensure that relevant areas are covered in the audit. Any observation raised in the SARs shall be tracked by the CPNs for timely closure.</p>
19	11-Feb-22	3	Tokenisation - Card Transactions: System Audit	CO.DPSS.OVRST.No.S1428/06 -11-001/2021-2022	Guidelines to CPN	<p>a) As regards the tokenisation SAR of CPNs submitted to RBI, the report must contain item-wise response from the auditors on each requirement specified in the above as well as other relevant circulars.</p> <p>b) In case the CPN offers Card-on-File Tokenisation (CoFT), item-wise compliance status for related RBI instructions shall also be specified in the SAR. Further, the report shall contain a certificate issued by the auditors, indicating the deficiencies observed in the SARs of token service participants.</p>
20	11-Feb-22	2.i.	Tokenisation - Card Transactions: System Audit	CO.DPSS.OVRST.No.S1428/06 -11-001/2021-2022	Guidelines to CPN	It is the responsibility of an authorised CPN to ensure that the token requestors and any other participants (cumulatively termed as token service participants, hereafter) involved in providing its card tokenization services to customers, adhere to RBI instructions on card tokenization, data storage, system audit and other relevant instructions.

Date :

Signature with seal

Name:

Designation: