THE INSTITUTE OF
Company Secretaries of India
भारतीय कम्पनी सचिव संस्थान
IN PURSUIT OF PROFESSIONAL EXCELLENCE
Statutory body under an Act of Parliament
(Under the jurisdiction of Ministry of Corporate Affairs)

SUPPLEMENT
PROFESSIONAL PROGRAMME

(NEW SYLLABUS)

for

December, 2020 Examination

BANKING - LAW & PRACTICE

MODULE 3

ELECTIVE PAPER 9.1

Lesson No. and Name	Particulars of Change	Remarks
Lesson 1 **Overview of Indian Banking System**	For providing RRBs additional options for augmenting regulatory capital funds, so as to maintain the minimum prescribed Capital to Risk weighted Assets Ratio, besides meeting the increasing business requirements, it RBI has in November 2019 allowed RRBs to issue Perpetual Debt Instruments (PDIs) eligible for inclusion as Tier 1 capital under specified terms and conditions including the following: ✓ They are not permitted to issue Perpetual Debt Instruments to retail investors / FPIs / NRIs ✓ invest in the Perpetual Debt Instruments of other banks including RRBs. RRBs shall issue the Perpetual Debt Instruments in Indian currency only.	The content has been inserted to provide more understanding .
Lesson 2 **Regulatory Framework of Banks**	**Framework for imposing monetary penalty on authorised payment system operators / banks)** In terms of its Circular No: DPSS.CO.OD.No.1328/06.08.005/2019-20 dated January 10, 2020 RBI has announced a detailed and revised frame work for imposing penalties on authorised payment system operators/ banks for violation of Payment and Settlement Systems Act 2007 provisions and guidelines issued by RBI in this regard.	Regulatory update.
	Section 45 W of RBI Act 1934 Updation of Re-purchase option (Repo) Directions, Updated in 2019 **Salient features:** • Applicable to Repo deals undertaken on recognized stock exchanges, electronic trading platforms (ETP) and Over-the- Counter (OTC) • In case of exchange trades Repo transactions this will be as per SEBI/Stock exchange guidelines. • These directions will not apply to repo/ reverse repo transactions under the Liquidity Adjustment Facility and the Marginal Standing Facility, • Eligible Securities for Repo : Central/State Government Securities, Listed corporate bonds and debentures (other than own securities),Commercial Papers, Certificate of Deposits,	Regulatory update.

	Units of Debt Exchange Traded Funds, Any other security of Local Authority specified by Central Government. • Eligible Participants: Any regulated entity, any listed company, any unlisted company which has been issued special securities by Govt. of India (repo will be available only on such securities),Any of the All-India Financial Institutions, any other approved entity by RBI from time to time. • Tenor: Minimum period of one day and a maximum of one year. • Trading venue: RBI approval is required for any trading venue including recognized stock exchanges. • Specific directions regarding Tri-Party Agent, Trading process, Reporting of trades, Settlement, Sale and Substitution of security, Pricing-Haircut and Margining, Accounting, presentation, valuation and disclosure, Computation of CRR /SLR and borrowing limit, Documentation have also been given by RBI.	
	Marginal Standing Facility ('MSF'): From May 9, 2011 RBI had introduced an additional facility for the scheduled commercial banks to borrow funds, up to 1% of their Net Demand and Time Liabilities (NDTL) against their SLR securities. Subsequently it was raised to 2% and from 27th March 2020 it has been raised for Scheduled Banks (excluding Regional Rural Banks) under the MSF to 3 per cent up to 30th June 2020 of their NDTL outstanding at the end of the second preceding fortnight with immediate effect. In terms of RBI notification RBI/2019-20/259 DOR.No.Ret.BC.77/12.02.001/ 2019-20 the same raised borrowing limit is allowed to continue till September 30,2020. The rate of interest applicable on such advances is fixed at a higher rate than Repo rate. Presently i.e. as at July 2020 the applicable rate is 4.25% % p.a., the same as Bank rate as per the table given below.. In the event, the banks' SLR holdings fall below the statutory requirement up to one per cent of their NDTL, banks will not have the obligation to seek a specific waiver for default in SLR compliance arising out of use of this facility from RBI in terms of notification issued under sub section (2A) of section 24 of the Banking Regulation Act, 1949. The MSF facility acts as a safety valve against sudden short fall in liquidity for a bank.	Regulatory update.
Lesson 3 **Control over**	The minimum paid-up equity capital for SFB should be Rs. 100 crore with a leverage ratio not less than 3 per cent, i.e., its outside liabilities should not exceed 33.33 times its net worth (paid-up capital and reserves). The promoter's minimum initial contribution has to be at least 40% of paid-up equity capital for	This has been inserted to provide more understanding .

Organization of Banks	the first five years from the commencement of its business and gradually brought down to 26 per cent within 12 years from the date of commencement of business of the bank. On 5th December 2019 Reserve Bank of India released on its website, "Guidelines for 'on tap' Licensing of Small Finance Banks in the Private Sector".Major changes from the earlier Guidelines on Small Finance Banks dated November 27, 2014, are (i) The licensing window will be open on-tap; (ii) minimum paid-up voting equity capital / net worth requirement shall be Rs. 200 crore; (iii) for Primary (Urban) Co-operative Banks (UCBs), desirous of voluntarily transiting into Small Finance Banks (SFBs) initial requirement of net worth shall be at Rs. 100 crore, which will have to be increased to Rs. 200 crore within five years from the date of commencement of business. Incidentally, the net-worth of all SFBs currently in operation is in excess of Rs, 200 crore; (iv) SFBs will be given scheduled bank status immediately upon commencement of operations; (v) SFBs will have general permission to open banking outlets from the date of commencement of operations; (vi) Payments Banks can apply for conversion into SFB after five years of operations, if they are otherwise eligible as per these guidelines.	
	Scheme for setting up of IFSC Banking Units (IBU) by Indian Banks The RBI had issued a notification under FEMA vide Notification No. FEMA.339/2015-RB dated March 02, 2015 setting out RBI regulations relating to financial institutions set up in International Financial Services Centres (IFSC). In line with the above Notification, RBI has formulated a detailed scheme applicable for Indian banks and foreign banks already having presence in India for setting up of IFSC Banking Units (IBUs) by banks in IFSCs. The scheme covers Eligibility criteria, Licensing, Capital, Reserve requirements, Resources and deployment, Permissible activities, Prudential regulations, Anti-Money Laundering Measures, Regulation, Supervision, Reporting, Ring fencing of activities, Priority sector Lending, deposit Insurance, Lender of last resort etc. Since these are highly specialised units, elaborate details can be accessed through circulars dated January 21, 2020, December 23, 2019 and April 15, 2015 of RBI.	Regulatory update.
	RBI has in the light of COVID-19 pandemic, has directed banks not to make any further dividend payouts from the profits pertaining to the financial year ended March 31, 2020 until further instructions. This restriction will be reassessed by the RBI on September 30, 2020.	Regulatory update.

	Appointment of MD & CE O / CE O / part-time Chairperson (PTC) in Banks – 'Declaration and Undertaking' and allied matters In the case of Private Sector Banks including Local Area Banks, Small Finance Banks, Payments Banks and Foreign Banks operating in India / RBI vide its Notification dated March 31, 2020 has directed that for the re-appointment of an MD & CEO/ CEO in banks, as above the complete applications in the prescribed format' along with 'Declaration and Undertaking' from candidate(s), along with the remarks of Nomination and Remuneration Committee should be submitted to the Department of Regulation, Central Office, RBI, Mumbai, at least six months before the expiry of the term of office of the incumbent. For appointment of a new MD & CEO/ CEO, the proposal should contain a panel of at least two names in the order of preference. The proposals should be submitted to the Reserve Bank at least four months before the expiry of the term of office of the present incumbent.	Regulatory update.
	Guidelines on Compensation Of Whole Time Directors/ Chie F Executive Officer S/ Material Risk Takers And Control Function Staff A review of these guidelines issued in 2012-13 was carried out to comply with Guidelines with Financial Stability Board's (FSB) Principles and Implementation Standards for Sound Compensation Practices and the Supplementary Guidance issued by FSB in March 2018. After extensive consideration of views of all stake holders, the RBI has amended and superseded the 2012-13 guidelines vide its Circular dated November 4, 2019. These Guidelines will be applicable for pay cycles beginning from/after April 01, 2020. All applications for approval of appointment/re-appointment or approval of remuneration/revision in remuneration of Whole Time Directors (WTDs)/ Chief Executive Officers (CEOs) shall be submitted with full details as prescribed in a amended guidelines. Private sector banks, foreign banks operating under the Wholly Owned Subsidiary mode (WOS), and foreign banks operating in India under the branch mode are required to obtain regulatory approval for grant of remuneration (i.e. compensation) to WTDs/ CEOs in terms of Section 35B of the Banking Regulation Act, 1949 (B.R. Act, 1949).The approval process will involve, an assessment of whether the bank's compensation policies and practices are in accordance with the Guidelines. **Salient features:**	Regulatory update.

	a. The Guidelines are applicable to private sector banks, including Local Area Banks, Small Finance Banks and Payments Banks. b. Foreign banks operating in India under branch mode would be required to continue to submit a declaration to RBI annually from their Head Offices to the effect that their compensation structure in India, including that of CEO's, is in conformity with the FSB Principles and Standards. RBI would take this into account while approving CEOs' compensation. c. The compensation proposals for CEOs and other staff of foreign banks operating in India that have not adopted the FSB principles in their home country are required to implement the compensation Guidelines as prescribed for private sector banks in India, to the extent applicable to them. d. For the foreign banks operating in India by way of Wholly Owned Subsidiary (WOS) structure, the compensation Guidelines as prescribed for private sector banks in India will be applicable. **These guidelines cover in detail :** • Compensation policy including bonuses, ESOPs, pension plan, gratuity etc. • Constitution of Nomination and Remuneration Committee (NRC). • Effective alignment of compensation with prudent risk taking for Whole Time Directors / Chief Executive Officers / Material Risk Takers (MRTs) covering a) Fixed Pay and Perquisites b) Variable Pay c) Malus/ Clawback d) Guaranteed Bonus e) Hedging. • Guidelines for risk control and compliance staff • Guideline for other categories of staff • Identification of Material Risk Takers of the bank • Disclosure •Regulatory and Supervisory Approval / Oversight	
	Highlights of Guidelines on Board of Management (BoM) for Primary (Urban) Co-operative Banks (UCB s) vide Circular dated Dec. 31, 2019 • This was introduced as a part recommendations made by The Malegam Committee in 2011 as well as by The High Powered Committee in 2016. • UCBs with a deposit size of Rs. 100 crores and above	Regulatory update.

	o have to constitute a BoM by making suitable amendments in their bye-laws. This will be a mandatory requirement for future branch expansion programmes of these banks. o prior approval of RBI for appointment of CEO is a must for such UCBs. ➢ for CEO appointment Scheduled UCBs to approach Department of Regulation three months prior the end of the tenure of the incumbent CEO. ➢ Non-scheduled UCBs to approach the respective Regional Office of Department of Supervision (RO – DoS) of RBI in their jurisdiction in the same manner as applicable to Scheduled UCBs. • The BoM shall comprise of persons with special knowledge and practical experience in banking and other specified fields to facilitate professional management and focused attention to the banking related activities of the UCBs. • While forming the BoM, the Board of Directors (BoD) of UCB have to carry due diligence to determine the suitability of the person for appointment as the member of the BoM. , based upon qualification, expertise, track record, integrity and other 'fit and proper' criteria. • Similar process of due diligence is applicable for appointing a candidate as CEO. • The process of due diligence is applicable at the time of renewal of appointment too. • A copy of the amended bye-laws providing for constitution of BoM, along with details of the members of BoM immediately after it's constitution to be reported to the RO – DoS. • Annual Report as on 31st December has to be submitted by concerned UCBs to respective ROs of RBI on or before 15th January.	
	Judicial Pronouncement Case In the matter of *Assistant General Manager and Ors*. vs. *Radhey Shyam Pandey* (02.03.2020-SC) the Honorable Supreme Court was of the opinion that the employees who completed 15 years of service or more as on cutoff date were entitled to proportionate pension under SBI VRS to be computed as per SBI Pension Fund Rules. Let the benefits be extended to all such similar employees retired under VRS on completion of 15 years of service without requiring them to rush to the court. However, considering the facts and circumstances, it would not be appropriate to burden the bank with interest. Let order be complied with and arrears be paid within three months, failing which amount to carry interest at the rate of 6 per cent per annum	Case laws has been added for more clarity.

	from the date of this order. The appeals are accordingly disposed of. No costs were issued.	
Lesson 4 Regulation of Banking Business	The Reserve Bank has created a Central Repository of Information on Large Credits (CRILC) of scheduled commercial banks, all India financial institutions and certain non-banking financial companies with multiple objectives, which, among others, include strengthening offsite supervision and early recognition of financial distress. With a view to building a similar database of large credits extended by primary (urban) co-operative banks (UCBs), it has been decided to bring UCBs with assets of Rs500 crores and above under the CRILC reporting framework vide . Detailed Guidelines have been vide RBI notification dated December 27, 2019 and January 16, 2020.	
	With changes in the NEFT settlement frequency, RBI vide it's announcement dated 13th December 2019, has decided to provide an additional collateralised intra-day liquidity facility, called Liquidity Support (LS), to facilitate smooth settlement of NEFT transactions in the accounts of member banks held by it, on a round-the clock- basis. LS facility will operate on the same terms and conditions as the Intra-Day Liquidity (IDL) facility. Member banks eligible for IDL will also be able to draw LS which will be counted as a part of their borrowings under IDL. LS limits would be set by RBI. Margin requirement is similar to that of IDL. Any outstanding LS drawings at the end of the day will be automatically be counted as a part of RBI's Marginal Standing Facility (MSF).MSF borrowing reversal will take place along with other Liquidity Adjustment Facility operations as per existing practice. By a separate notification on December 16,2019, RBI has directed member banks of the NEFT system, not to levy any charges from their savings bank account holders for funds transfers done through online (viz. internet banking and/or mobile apps of the member banks). This is done further to encourage digital retail payments.	
	Processing of e-mandate in Unified Payments Interface (UPI) for recurring transactions In 2019 RBI had permitted processing of e-mandate on cards / Prepaid Payment Instruments (PPIs) for recurring transactions (merchant payments), with Additional Factor of Authentication (AFA) during e-mandate registration, modification and revocation, as also for the first transaction, and simple / automatic subsequent successive transactions, subject to certain conditions. The same has been extended to cover Unified Payment Interface (UPI) transactions as well vide its Notification dated January 10, 2020.	Regulatory update.

	Enhancing Security of Card Transactions Over the years in India the volume and value of transactions made through cards have increased manifold. To improve user convenience and increase the security of card transactions, RBI through it's notification dated January 15, 2020 has issued the following directives : 1. (a) At the time of issue / re-issue, all cards (physical and virtual) be enabled for use only at contact based points of usage [viz. ATMs and Point of Sale (PoS) devices] within India. Issuers to provide cardholders a facility for enabling card not present (domestic and international) transactions, card present (international) transactions and contactless transactions, as per the process outlined in para 1c). (b) For existing cards, issuers to take a decision, based on their risk perception, whether to disable the card not present (domestic and international) transactions, card present (international) transactions and contactless transaction rights. Existing cards which have never been used for online (card not present) / international / contactless transactions are to be mandatorily disabled for this purpose. (c) Additionally, the issuers to provide to all cardholders: i. facility to switch on / off and set / modify transaction limits (within the overall card limit, if any, set by the issuer) for all types of transactions – domestic and international, at PoS / ATMs / online transactions / contactless transactions, etc. ii. the above facility on a 24x7 basis through multiple channels - mobile application / internet banking / ATMs / Interactive Voice Response (IVR); this may also be offered at branches / offices; iii. alerts / information / status, etc., through SMS / e-mail, as and when there is any change in status of the card. 2. The provisions of this circular are not mandatory for prepaid gift cards and those used at mass transit systems.	Regulatory update.
	Guidelines on Merchant Acquiring Business – Regional Rural Banks RBI has permitted RRBs to act as merchant acquiring banks using Aadhaar Pay – BHIM app and POS terminals by deploying their own devices subject to fulfilling following conditions – • Should have the permission for mobile banking from the RBI • Bank's IT systems & CBS should have been subjected to an Information System Audit not earlier than six months from the date of application to confirm that the system is adequately secure.	Regulatory update.

	• Bank must ensure necessary infrastructure for application development, safety and security of the transactions and handling of customer grievance. • Customer grievance redressal mechanism duly approved by the bank's board should be in place; • Bank should have a board approved policy on merchant acquisition for card transactions; • Should not be any restrictions imposed on the bank for accepting deposits/ withdrawals by RBI. • No penalty should have been imposed in last two financial years. • In the preceding financial year Net worth should be of Rs. 100 crore or more as on March 31, Minimum CRAR of 9% and Net NPA below 5%. Concerned RRB to inform the respective Regional Offices of Reserve Bank, within a period of 15 days from the date of operationalising the merchant acquisition business.	
	Regulation of Payment Aggregators (PA) and Payment Gateways Taking into account the important functions of these intermediaries in the online payments space as also keeping in view their role vis-à-vis handling funds, Vide its circular dated March 17, 2020 RBI has announced detailed guidelines on the regulation of PAs and PGs. PAs are entities that facilitate e-commerce sites and merchants to accept various payment instruments from the customers for completion of their payment obligations without the need for merchants to create a separate payment integration system of their own. They facilitate merchants to connect with acquirers. In the process, they receive payments from customers, pool and transfer them on to the merchants after a time period. Example: PayTM, Bill Desk, Pay Pal etc. PGs are entities that provide technology infrastructure to route and facilitate processing of an online payment transaction without any involvement in handling of funds. In India mostly PGs are banks such as HDFC,AXIS, UBI etc. **Salient features :** 1. Applicable to PAs. PGs are recommended to adopt technology related recommendations of these guidelines. 2. Domestic leg of import and export related payments facilitated by PAs shall also be governed by these guidelines. 3. These guidelines are not applicable to Cash on Delivery (CoD) e-commerce model.	Regulatory update.

	4. Banks which are PAs do not require Authorization under these guidelines. 5. Non-Bank PAs require Authorization from RBI under PSSA and apply for authorisation on or before June 30, 2021. Entities regulated by any of the financial sector regulators shall apply along with a 'No Objection Certificate' from their respective regulator, within 45 days of obtaining such a clearance. 6. PAs should be a company incorporated in India under the Companies Act, 1956 / 2013. The Memorandum of Association (MoA) of the applicant entity must cover the proposed activity of operating as a PA. 7. E-commerce marketplaces providing PA services shall not continue this activity beyond June 30, 2021. Beyond this date if they wish to continue they need to separate E-commerce market place activity from PA activity and apply for Authorization for PA activity by June 30, 2021. These guidelines also cover Capital Requirements, Governance aspects, Safeguards against Money Laundering (KYC/AML/CFT) Provisions, Merchant on-boarding, Settlement and Escrow Account Management, Customer Grievance Redressal and Dispute Management Framework, Reports, General Instructions as well as Baseline Technology-related Recommendations for PGs.	
	Introduction of semi-closed Pre-paid Instruments To give impetus to small value digital payments and for enhanced user experience, by its Notification dated December 24, 2019, RBI has allowed introduction of a new type of semi-closed PPI with the following features: • Such PPIs can be issued by bank and non-bank PPI Issuers after obtaining minimum details of the PPI holder such as a mobile number verified with One Time Pin (OTP) and a self-declaration of name and unique identity / identification number of any 'mandatory document' or 'officially valid document' (OVD) as per KYC norms. • Such PPIs should be ✓ loadable in nature and issued in card or electronic form. ✓ used only for purchase of goods and services and not for funds transfer Loading / Reloading can be only from a bank account; loading during any month not to exceed Rs.10,000 and the total amount loaded during the financial year not to exceed Rs. 1,20,000. • Amount outstanding at any point of time in such PPIs not to exceed Rs.10,000.	Regulatory update.

<table>
<tr><td></td><td>• PPI issuers to provide an option to close the PPI at any time and also allow to transfer the funds ‘back to source’ (payment source from where the PPI was loaded) at the time of closure..
• PPI issuers to communicate features of such PPIs to the purchasers/holder at the time of issue by SMS / e-mail / post or by any other means.
• Other Master Directions instructions issued is applicable to this PPI also.</td><td></td></tr>
<tr><td></td><td>RBI has vide its Notification dated June 4, 2020 has announced extension of time lines with various payment system requirements as per the table below:
Annex to letter DPSS.CO.PD.No.1897/02.14.003/2019-20 dated June 04, 2020
<table>
<tr><th>SN</th><th>Instruction / Circular</th><th>Present Timeline</th><th>Revised Timeline</th></tr>
<tr><td rowspan="2">1.</td><td rowspan="2"><u>PPI-MD dated October 11, 2017 (as updated from time to time)</u>:
(i) All existing non-bank PPI issuers (at the time of issuance of PPI-MD) to comply with the minimum positive net-worth requirement of Rs. 15 crore for the financial position as on March 31, 2020 (audited balance sheet).

(ii) Authorised non-bank entities shall submit the System Audit Report, including cyber security audit conducted by CERT-IN empanelled auditors, within two months of the close of their financial year to the respective Regional Office of DPSS, RBI.</td><td>Financial position as on June 30, 2020</td><td>Financial position as on September 30, 2020</td></tr>
<tr><td>By August 31, 2020</td><td>By October 31, 2020</td></tr>
<tr><td>2.</td><td>Implementing provisions of circular on “Enhancing Security of Card Transactions”.</td><td>w.e.f. June 16, 2020</td><td>By September 30, 2020</td></tr>
</table></td><td>Regulatory update.</td></tr>
</table>

		3.	"Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems", "calendar days" to be read as "working days".	w.e.f. March 24, 2020	Until December 31, 2020	
		4.	"Guidelines on Regulation of Payment Aggregators and Payment Gateways", the activities for which specific timelines are not mentioned and were supposed to come into effect from April 1, 2020.	w.e.f. June 01, 2020	By September 30, 2020	
	In the light of increasing instances of Payment frauds RBI vide its notification dated 26th June 2020 has directed all authorised payment systems operators and participants to undertake targeted multi-lingual campaigns by way of SMSs, advertisements in print and visual media, etc., to educate their users on safe and secure use of digital payments.					
	Reporting Investment in Certificates of Deposit (CDs) RBI has directed banks to adhere to the following practice vide it's notification dated February 26th, 2020 with the reference to reporting their transactions in CDs in Form 'A' Return as below: . A) Based on the statement issued by depositories, if the CDs issued are held by banks on reporting Friday, the issuer bank should report such CDs under item I of the Form 'A' Return i.e., "Liabilities to the Banking System in India". The CDs held by non-bank entities should be reported as "Liabilities to Others in India", as hitherto. If the bank is not in a position to segregate the holders of CDs issued between bank and non-bank entities, then the total CDs issued should be reported under item II of the Form 'A' Return i.e., "Liabilities to Others in India". The reporting of CDs should be done as per the issue price of the CDs. B) Investments in CDs issued by other banks should be reported under item III of the Form 'A' Return i.e., "Assets with the Banking System in India" and these assets could be netted off against "Liabilities to the Banking System in India".					Regulatory update.

Lesson 5 Banking Operation	As per RBI circular dated January 9, 2020 where PAN is obtained, the same shall be verified from the verification facility of the issuing authority. and where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000.	Regulatory update.
	RBI has allowed as per their Master Directions updation dated January 9, 2020 a detailed Video based Customer Identification Process (V-CIP)": It is a method of customer identification by an official of the RE by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face process for the purpose of this Master Direction.	Regulatory update.
	Banks shall obtain the Aadhaar number from an individual who is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016). or he decides to submit his Aadhaar number voluntarily to a bank or the proof of possession of Aadhaar number where offline verification can be carried out or where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address and the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income tax Rules, 1962; and such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the RE (RBI circular dated January 9, 2020): Banks, at receipt of the Aadhaar number from the customer may carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. According to RBI Circular dated January 9, 2020, further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the RE. ii) Where proof of possession of Aadhaar under clause mentioned above where offline verification can be carried out, the RE shall carry out offline verification. iii) an equivalent e-document of any OVD, the RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules/issues thereunder and take a live photo as specified.	Regulatory update.

	iv) any OVD or proof of possession of Aadhaar number under clause above where offline verification cannot be carried out, the RE shall carry out verification through digital KYC as specified under. Provided that for a period not beyond such date as may be notified by the Government for a class of REs, instead of carrying out digital KYC, the RE pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.	
	Risk Assessment A new section (5A) has been added to chapter II of the Master Directions on KYC (vide RBI Circular dated April 20, 2020) requiring REs to carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. While assessing the ML/TF risk, the REs are required to take cognizance of the overall sector specific vulnerabilities, if any, that the regulator/supervisor may share with REs from time to time. Further, the internal risk assessment carried out by the RE should be commensurate to its size, geographical presence, complexity of activities/structure, etc. Also, the REs shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard.	Regulatory update.
Lesson 6 IT in Banking	**Cyber Security controls for Third party ATM Switch Application Service Providers** RBI has vide it's Circular No: RBI/2019-20/130 DoS.CO/CSITE/BC.4084/31.01.015/2019-20 dated December 31, 2019 has advised all Scheduled Commercial Banks (excluding Regional Rural Banks), Small Finance Banks and Payments Banks, Primary (Urban) Co-operative Banks, Local Area Banks and White-Label ATM Operators to implement Cyber Security controls for Third party ATM Switch Application Service Providers. All RBI Regulated Entities (RREs) manage their ATM Switches through shared services of third party ATM Switch Application Service Providers (ASPs). Since these service providers also have exposure to the payment system network, it is felt that some cyber security controls are required to be put in place by them. In view of this, the RREs it is advised that the contract agreement signed between them and the third party ATM Switch ASP shall necessarily mandate the third party ATM Switch ASP to comply with the detailed cyber security controls given in the Annexure to the circular on an ongoing basis and to provide access to the RBI for on-site/off-	Regulatory update.

	site supervision. To this effect, the contract agreements shall be amended at the earliest or at the time of renewal, in any case not later than March 31, 2020. The list of prescribed controls is indicative but and that these controls are applicable to the ASPs limited to the IT ecosystem (such as physical infrastructure, hardware, software, reconciliation system, network interfaces, security solutions, hardware security module, middleware, associated people, processes, systems, data, information, etc.,) providing ATM switch services as well as any other type of payment system related services to the RREs. The annexure to the circular covers 1. Preventing access of unauthorised software 2. Environmental Controls 3. Network Management and Security 4. Secure Configuration 5. Application Security Life Cycle (ASLC) 6. Patch/Vulnerability and Change Management 7. User Access Control / Management 8. Data Leak prevention strategy 9. Audit Logs 10. Incident Response and Management 11. Advanced Real-time Threat Defence and Management 12. Vulnerability assessment and Penetration Test 13. Forensics 14. Arrangement for continuous surveillance - Setting up of Cyber Security Operation Center (C-SOC) 15. Compliance with various standards.	

Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCB s) – A

Graded Approach

RBI has formulated a comprehensive Cyber Security Framework for UCBs vide its notification dated December 31, 2019 based on a graded approach. The Salient

features are as follows:

Level	Criteria	Regulatory Prescription	Remarks
Level I	All UCBs	Level I controls prescribed in Annex I to this circular.	In addition to the controls prescribed bank specific email domain with DMARC controls, two factor authenticati on for CBS etc., are salient controls prescribed.
Level II	All UCBs, which are sub-members of Centralised Payment Systems[1] (CPS) and satisfying at least one of the criteria given below: offers internet banking facility to its customers (either view or transaction based) provides Mobile Banking facility	Level II controls given in Annex II of this circular, in addition to Level I controls.	Additional controls include Data Loss Prevention Strategy, Anti-Phishing, VA/PT of critical applications .

Regulatory update.

	through application (Smart phone usage) is a direct Member of CTS/IMPS/UPI.		
Level III	UCBs having at least one of the criteria given below: Direct members of CPS having their own ATM Switch having SWIFT interface	Level III controls given in Annex III of this circular, in addition to Level I and II controls.	Additional controls include Advanced Real-time Threat Defence and Management, Risk based transaction monitoring[2]
Level IV	UCBs which are members/ sub-members of CPS and satisfy at least one of the criteria given below: having their own ATM Switch **and** havin g SWIFT interface hosting data centre or providing software support to other banks on their own or through their wholly owned subsidiaries	Level IV controls given in Annex IV of this circular, in addition to Level I, II and III controls	Additional controls include setting up of a Cyber Security Operation Center (C-SOC) (either on their own or through service providers), IT and IS Governance Framework

The Board of Directors of the UCB is ultimately responsible for the information security and should play a proactive role in ensuring an effective IT (Information Technology) and IS (Information Security) governance. The major role of top management involves implementing the Board approved cyber security policy, establishing necessary organisational processes for cyber security and providing necessary resources for ensuring adequate cyber security.

UCBs to undertake a self-assessment of the level in which they fit into, based on the criteria given in the table above and report

	the same to their respective RBI Regional Office, Department of Supervision within 45 days from the date of issuance of this circular. All UCBs to comply with the control requirements prescribed in Annex I within 3 months from the date of issuance of this circular. Similarly, Level II, III and IV UCBs are required to implement additional controls prescribed in Annex –II, III and IV to this circular. UCBs may adopt higher level of security measures based on their own assessment of risk and capabilities.	

	Annexure – I (Salient points) Following controls to be implemented: I. Implement bank specific email domains (example, XYZ bank with mail domain xyz.in) with anti-phishing and anti-malware, DMARC controls enforced at the email solution. II. UCBs shall put in place two factor authentication for accessing their CBS and applications connecting to the CBS with the 2nd factor being dynamic in nature. (Eg: 2nd factor should not be a static password and must not be associated with the PC/terminal used for putting through payment transactions). III. Conduct security review of PCs/terminals used for accessing corporate Internet Banking applications of Scheduled Commercial Banks (SCBs), CBS servers and network perimeter through a qualified information security auditor. IV. There should be a robust password management policy in place, with specific emphasis for sensitive activities like accessing critical systems, putting through financial transactions. Usage of trivial passwords shall be avoided. [An illustrative but not exhaustive list of practices that should be strictly avoided are: For example, XYZ bank having password as xyz@123; network/server/security solution devices with passwords as device/solution_name123/device_name/solution@123; hard coding of passwords in plain text in thick clients or storage of passwords in plain text in the databases] V. educate employees to strictly avoid clicking any links received via email (to prevent phishing attacks). VI. Put in place an effective mechanism to report the cyber security incidents in a timely manner and take appropriate action to mitigate the incident. UCBs shall also report all unusual cyber security incidents to CERT-In and IB-CART.	

	Vendor/Outsourcing Risk Management Apart from the general guidelines issued in October, 2013 the following guidelines need to be implemented by UCBs: I. Accountable for ensuring appropriate management and assurance on security risks in outsourced vendor arrangements. UCBs should be a. carefully evaluate the need for outsourcing critical processes and selection of vendor/partner based on comprehensive risk assessment. b. shall regularly conduct effective due diligence, oversight and management of third party vendors/ service providers and partners. II. Required to necessarily enter into agreement with the service provider that, among other things, provides for right to audit by the UCB. The outsourcing agreements should include clauses to recognise a. the right of the RBI to cause an inspection to be made of a service provider of the UCB and b. allow the RBI or persons authorised by it to access the bank's documents, records of transactions, logs and other necessary information given to, stored or processed by the service provider within a reasonable time. Required to thoroughly satisfy about the credentials of vendor/third-party personnel accessing and managing the UCB's critical assets. Background checks, non-disclosure and security policy compliance agreements shall be mandated for all third party service providers.	This has been inserted to provide more understanding
	Annexure II Annexure II Baseline Cyber Security and Resilience Requirements (in addition to the requirements given in Annex I) (for level II). Following controls shall be implemented: UCBs shall identify an official responsible for a) articulating and enforcing the policies that UCBs use to protect their information assets, apart from coordinating the cyber security related issues / implementation within the organisation as well as relevant external agencies. b) ensuring compliance to various instructions issued on information/cyber security by RBI. **1. Network Management and Security** 1.1 Maintain an up-to-date/centralised inventory of authorised devices connected to UCB's network (within/ outside UCB's premises) and related network devices in the UCB's network.	

	1.2 Boundary defences should be multi-layered with properly configured firewalls, proxies, De-Militarized Zone (DMZ) perimeter networks, and network-based Intrusion Prevention System (IPS)/Intrusion Detection System (IDS). Mechanism to filter both inbound and outbound traffic shall be put in place. 1.3 LAN segments for in-house/onsite ATM and CBS/branch network should be different. **2. Secure Configuration** 2.1 Document and apply baseline security requirements/configurations to all categories of devices (endpoints/ workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security systems, etc.), throughout the lifecycle (from conception to deployment) and carry out reviews periodically. **3. Application Security Life Cycle (ASLC)** 3.1 The development/test and production environments need to be properly segregated. The data used for development and testing should be appropriately masked. 3.2 Software/Application development approach should incorporate secure coding principles, security testing (based on global standards) and secure rollout. **4. Change Management** 4.1. UCBs should have a robust change management process in place to record/ monitor all the changes that are moved/ pushed into production environment. Changes to business applications, supporting technology, service components and facilities should be managed using robust configuration management processes that ensure integrity of any changes thereto. **5. Periodic Testing** 5.1 Periodically conduct Vulnerability Assessment/ Penetration Testing (VA/PT) of internet facing web/ mobile applications, servers and network components throughout their lifecycle (pre-implementation, post implementation, after changes etc.). VA of critical applications and those on DMZ shall be conducted atleast once in every 6 months. PT shall be conducted atleast once in a year. 5.2 UCBs having their CBS on a shared infrastructure of an Application Service Provider (CBS-ASP) shall get their CBS application including the infrastructure hosting it subjected to VA/PT through the CBSASP.	

	5.3 Application security testing of web/mobile applications should be conducted before going live and after every major changes in the applications. 5.4 The vulnerabilities detected are to be remedied promptly in terms of the UCB's risk management/ treatment framework so as to avoid exploitation of such vulnerabilities. 5.5 Penetration testing of public facing systems as well as other critical applications are to be carried out by professionally qualified teams. Findings of VA/PT and the follow up actions necessitated are to be monitored closely by the Information Security/Information Technology Audit team as well as Top Management. **6. User Access Control / Management** 6.1 Provide secure access to the UCB's assets/services from within/outside UCB's network by protecting data/information at rest (e.g. using encryption, if supported by the device) and in-transit (e.g. using technologies such as VPN or other standard secure protocols, etc.) **7. Authentication Framework for Customers** 7.1 UCBs should have adequate checks and balance to ensure (including security of customer access credentials held with them) that transactions are put only through the genuine/authorised applications and that authentication methodology is robust, secure and centralised. 7.2 Implement authentication framework /mechanism to securely verify and identify the applications of UCB to customers (Example, with digital certificate). **8. Anti-Phishing** 8.1 Subscribe to Anti-phishing/anti-rogue application services from external service providers for identifying and taking down phishing websites/rogue applications. **9. Data Leak Prevention Strategy** 9.1 Develop and implement a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information. 9.2 Similar arrangements need to be ensured at vendor managed facilities as well.	

	10. Audit Logs 10.1 Capture the audit logs pertaining to user actions in a system. Such arrangements should facilitate forensic auditing, if need be. 10.2 An alert mechanism should be set to monitor any change in the log settings. **11. Incident Response and Management** 11.1 Put in place an effective Incident Response programme. UCBs must have a mechanism/ resources to take appropriate action in case of any cyber security incident. They must have written incident response procedures including the roles of staff / outsourced staff handling such incidents. 11.2 UCBs are responsible for meeting the requirements prescribed for incident management and BCP/DR even if their IT infrastructure, systems, applications, etc., are managed by third party vendors/service providers.	
	Annexure III (in addition to the requirements given in Annex I & II) (For level III) **1. Network Management and Security** 1.1 Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints. 1.2 Firewall rules shall be defined to block unidentified outbound connections, reverse TCP shells and other potential backdoor connections **2. Secure Configuration** 2.1 Disable remote connections from outside machines to the network hosting critical payment infrastructure (Ex: RTGS/NEFT, ATM Switch, SWIFT Interface). Disable Remote Desktop Protocol (RDP) on all critical systems. 2.2 Enable IP table to restrict access to the clients and servers in SWIFT and ATM Switch environment only to authorised systems. 2.3 Ensure the software integrity of the ATM Switch/SWIFT related applications. 2.4 Disable PowerShell in servers where not required and disable PowerShell in Desktop systems. 2.5 Restrict default shares including IPC$ share (inter-process communication share) **3. Application Security Life Cycle (ASLC)**	This has been inserted to provide more understanding

	3.1 In respect of critical business applications, UCBs may conduct source code audits by professionally competent personnel/service providers or have assurance from application providers/OEMs that the application is free from embedded malicious / fraudulent code. 3.2 Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking and exception handling are required to be clearly specified at the initial and ongoing stages of system development/acquisition/implementation. 3.3 Ensure that software/application development practices adopt principle of defence-in-depth to provide layered security mechanism. 3.4 Ensure that adoption of new technologies is adequately evaluated for existing/evolving security threats and that the IT/security team of the UCB achieve reasonable level of comfort and maturity with such technologies before introducing them for critical systems of the UCB. **4. User Access Control : Implement** 4.1 a centralised authentication and authorisation system through an Identity and Access Management solution for accessing and administering critical applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication, securing privileged accesses following the principle of least privileges and separation of duties. This shall be implemented by the bank either with the in-house team managing the infrastructure or through the service provider if their infrastructure is hosted at a shared location at the service provider's end. 4.2 centralised policies through Active Directory or Endpoint management systems to whitelist/blacklist/ restrict removable media use. **5. Advanced Real-time Threat Defence and Management** 5.1 Build a robust defence against the installation, spread, and execution of malicious code at multiple points in the enterprise. 5.2 Implement whitelisting of internet websites/systems. **6. Maintenance, Monitoring, and Analysis of Audit Logs**	

	6.1 Consult all the stakeholders before finalising the scope, frequency and storage of log collection. 6.2 Manage and analyse audit logs in a systematic manner so as to detect, respond, understand or recover from an attack. 6.3 Implement and periodically validate settings for capturing of appropriate logs/audit trails of each device, system software and application software, ensuring that logs include minimum information to uniquely identify the log for example by including a date, timestamp, source addresses, destination addresses. **7. Incident Response and Management** 7.1 UCB's BCP/DR capabilities shall adequately and effectively support the UCB's cyber resilience objectives and should be so designed to enable the UCB to recover rapidly from cyber-attacks/other incidents and safely resume critical operations aligned with recovery time objectives while ensuring security of processes and data is protected. 7.2 UCBs shall have necessary arrangements, including a documented procedure, with such third party vendors/service providers for such purpose. This shall include, among other things, to get informed about any cyber security incident occurring in respect of the bank on timely basis to early mitigate the risk as well as to meet extant regulatory requirements. 7.3 Have a mechanism to dynamically incorporate lessons learnt to continually improve the response strategies. Response strategies shall consider readiness to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication and co-ordination with stakeholders during response. **8. User / Employee/ Management Awareness** 8.1 Encourage them to report suspicious behaviour incidents to the incident management team. 8.2 Make cyber security awareness programs mandatory for new recruits and web-based quiz and training for lower, middle and upper management every year. 8.3 Board members may be sensitised on various technological developments and cyber security related developments periodically. **9. Risk based transaction monitoring (This control shall be applicable to those banks who are direct**	

	members of CPS as well as having their own ATM Switch interface or SWIFT interface) 9.1 Risk based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all -delivery channels.	
	Baseline Cyber Security and Resilience Requirements (in addition to the requirements given **in Annex I, II & III) - Level IV** **1. Arrangement for continuous surveillance - Setting up of Cyber Security Operation Centre (C-SOC)** UCBs are mandated that a C-SOC (Cyber Security Operations Centre) be set up at the earliest, if not yet done. It is also essential that this Centre ensures continuous surveillance and keeps itself regularly updated on the latest nature of emerging cyber threats. 1.1 Expectations from C-SOC : Ability to i. protect critical business and customer data/information, demonstrate compliance with relevant internal ii. provide real-time/near-real time information on and insight into the security posture of the UCB iii. effectively and efficiently manage security operations by preparing for and responding to cyber risks/threats, facilitate continuity and recovery iv. know who did what, when, how and preservation of evidence v. Integration of various log types and logging options into a Security Information and Event Management (SIEM) system, ticketing/workflow/case management, unstructured data/big data, reporting/dashboard, use cases/rule design (customised based on risk and compliance requirements/drivers, etc.), etc. vi. C-SOC should be able to monitor the logs of various network activities and should have the capability to escalate any abnormal / undesirable activities. vii. Key Responsibilities of C-SOC could include: Monitor, analyse and escalate security incidents; Develop Response - protect, detect, respond, recover; Conduct Incident Management and Forensic Analysis; Co-ordination with relevant stakeholders within the UCB/external agencies 1.2 Steps for setting up C-SOC – Technological Aspects i. First step is to arrive at a suitable and cost effective technology framework designed and implemented to ensure proactive	This has been inserted to provide more understanding .

	monitoring capabilities aligned with the banking technology risk profile and business and regulatory requirements. Clear understanding of the service delivery architecture deployed by the UCB will enable identification of the location for the sensors to collect the logs that are required to carry out the analysis and investigation. SIEM is able to meet this requirement to some extent but a holistic approach to problem identification and solution is required. ii. Second step is to have a security analytics engine which can process the logs within reasonable time frame and come out with possible recommendations with options for further deep dive investigations iii. Third step is to look at deep packet inspection approaches iv. Fourth step is to have tools and technologies for malware detection and analysis as well as imaging solutions for data to address the forensics requirements v. It is to be noted that the solution architecture deployed for the above has to address performance and scalability requirements in addition to high availability requirements. Some of the aspects to be considered are : • Staffing of C-SOC - is it required to be 24x7x365, in shifts, business hours only, etc. • Model used - Finding staff with required skills /managed security service provider with required skill set • Metrics to measure performance of C-SOC • Ensuring scalability and continuity of staff through appropriate capacity planning initiatives. **2. Participation in Cyber Drills : 2.1. UCB s shall participate in cyber drills conducted under the aegis of** **Cert-IN , IDRB T etc.** **3. Incident Response and Management** 3.1 UCBs shall ensure incident response capabilities in all interconnected systems and networks including those of vendors and partners and readiness demonstrated through collaborative and co-ordinated resilience testing that meet the UCB's recovery time objectives. 3.2. Implement a policy & framework for aligning Security Operation Centre, Incident Response and Digital forensics to reduce the business downtime/ to bounce back to normalcy.	

	4. Forensics and Metrics 4.1 Develop a comprehensive set of metrics that provides for prospective and retrospective measures, like key performance indicators and key risk indicators. Some illustrative metrics include coverage of anti-malware software and their updation percentage, patch latency, extent of user awareness training, vulnerability related metrics, number of open vulnerabilities, IS/security audit observations, etc. 4.2 Have support/ arrangement for network forensics/forensic investigation/distributed denial-of-service (DDOS) mitigation services on stand-by. **5. IT Strategy and Policy** 5.1 The UCB shall have a Board approved IT-related strategy and policies covering areas such as: Existing and proposed hardware and networking architecture for the UCB and its rationale; Standards for hardware or software prescribed by the proposed architecture; Strategy for outsourcing, in-sourcing, procuring off-the-shelf software, and in-house development; IT Department's Organisational Structure; Desired number and level of IT expertise or ; Strategy for independent assessment, evaluation and monitoring of IT risks, findings of IT/IS/Cyber security related audits. **6. IT and IS Governance Framework** 6.1 Cyber Security Team/Function : UCBs shall form a separate cyber security function/group to focus exclusively on cyber security management. The organisation of the cyber security function should be commensurate with the nature and size of activities of the UCB including factors such as technologies adopted, delivery channels, digital products being offered, internal and external threats, etc. The cyber security function should be adequately resourced in terms of the number of staff, level of skills and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. **6.2 IT Strategy Committee** UCBs may consider setting up a Board level IT Strategy Committee with a minimum of two directors as members, one of whom should be a professional director. At least two members of the IT Strategy Committee would need to be technically competent4 while at least one member would need to have substantial expertise in managing/guiding technology initiatives.	

	Some of the roles and responsibilities that the IT Strategy Committee/Board should have are: (i) Approving IT strategy and policy documents (ii) ensuring that the management has put an effective strategic planning process in place (iii) ensuring that the IT organizational structure complements the business model and its direction (iv) ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable (v) Reviewing IT performance measurement and contribution of IT to businesses **6.3 IT Steering Committee:** An IT Steering Committee shall be formed with representatives from the IT, HR, legal and business sectors. Its role is to assist the Executive Management in implementing IT strategy that has been approved by the Board. It includes prioritization of IT-enabled investment, reviewing the status of projects (including, resource conflict), monitoring service levels and improvements, IT service delivery and projects. The IT Steering committee/Board should appraise/report to the IT strategy Committee periodically. The committee should focus on implementation. Its functions, inter-alia, include: (i) Defining project priorities and assessing strategic fit for IT proposals (ii) Reviewing, approving and funding initiatives, after assessing value-addition to business process (iii) Ensuring that all critical projects have a component for "project risk management" (iv) ponsoring or assisting in governance, risk and control framework, and also directing and monitoring key IT Governance processes (v) Defining project success measures and following up progress on IT projects (vi) Provide direction relating to technology standards and practices (vii) Ensure that vulnerability assessments of new technology is performed (viii) Verify compliance with technology standards and guidelines (ix) Ensure compliance to regulatory and statutory requirements (x) Provide direction to IT architecture design and ensure that the IT architecture reflects the need for legal and regulatory compliance, the ethical use of information and business continuity **6.4 Chief Information Security Officer (CISO)**	

	A sufficiently senior level official should be designated as Chief Information Security Officer (CISO), responsible for articulating and enforcing the policies that the UCB uses to protect its information assets apart from coordinating the cyber security related issues / implementation within the organisation as well as relevant external agencies. The CISO shall be primarily responsible for ensuring compliance to various instructions issued on information/cyber security by RBI. The following may be noted in this regard: The CISO should: (i) report directly to the top executive overseeing the risk management function or in his absence to the CEO directly. (ii) have the requisite technical background and expertise. (iii) have a reasonable minimum term. (iv) place a separate review of cyber security arrangements/ preparedness of the UCB before the Board on a quarterly basis. (v) The UCB's Board should be able to objectively measure steps to assess the effectiveness of the CISO's office. (vi) The CISO will be responsible for bringing to the notice of the Board about the vulnerabilities and cyber security risks that the UCB is exposed to. The CISO: (vii) by virtue of his role as member secretary of information security and/or related committees(s), if any, may ensure, inter alia, current/ emerging cyber threats to banking (including payment systems) sector and the UCB's preparedness in these aspects are invariably discussed in such committee(s). (viii) office shall manage and monitor the C-SOC and drive cyber security related projects. It can have a dotted relation with Chief Information Officer (CIO)/ Chief Technology Officer (CTO) for driving such projects. (ix) shall be an invitee to the IT Strategy committee and IT Steering Committee. The CISO may also be a member of (or invited to) committees on operational risk where IT/ IS risk is also discussed. (x) office shall be adequately staffed with technically competent people, if necessary, through recruitment of specialist officers, commensurate with the business volume, extent of technology adoption and complexity. (xi) shall not have any direct reporting relationship with the CIO/CTO and shall not be given any business targets.	

	(xii) The budget for IT security/ CISO's office may be determined keeping in view the current/ emerging cyber threat landscape. 6.5 Information Security Committee Since IT/ cyber security affects all aspects of an organisation, in order to consider IT/ cyber security from a UCB-wide perspective a steering committee of executives should be formed with formal terms of reference. The CISO would be the member secretary of the Committee. The Information Security Committee may include, among others, the Chief Executive Officer (CEO) or designee and two senior management officials well versed in the subject. The Committee shall meet atleast on a quarterly basis. Major responsibilities of the Information Security Committee, inter-alia, include: (i) Developing and facilitating the implementation of information security policies, standards and procedures to ensure that all identified risks are managed within a UCB's risk appetite. (ii) Approving and monitoring major cyber security projects and the status of cyber security plans and budgets, establishing priorities, approving standards and procedures. (iii) Supporting the development and implementation of a UCB-wide information security management programme. (iv) Reviewing the position of security incidents and various information security assessments and monitoring activities across the UCB. (v) Reviewing the status of security awareness programmes. (vi) Assessing new developments or issues relating to information/ cyber security. (vii) Reporting to the Board of Directors on cyber security activities. (viii) Minutes of the Information Security Committee meetings should be maintained to document the committee's activities and decisions and a review on information/cyber security needs to be escalated to the Board on a quarterly basis. **6.6 Audit Committee of Board (ACB)** Vide DCBR.CO.BPD.(PCB).MC.No.3/12.05.001/2015-16 Master circular dated July 1, 2015 all UCBs have been advised to set up an Audit Committee (ACB) at the Board level. In addition to its prescribed	

	role as per extant instructions, the ACB shall also be responsible for the following: (i) Performance of IS Audit and Evaluation of significant IS Audit issues – The ACB should devote appropriate and sufficient time to IS Audit findings identified and members of ACB need to review critical issues highlighted and provide appropriate guidance to the UCB's management. (ii) Monitor the compliance in respect of the information security reviews/VA-PT audits under various scope conducted by internal as well as external auditors/consultants to ensure that open issues are closed on a timely basis and sustenance of the compliance is adhered to.	
Lesson 7 Payment and Collection of Cheques and other Negotiable Instruments	**Judicial Pronouncement** **1. Rajeshbhai Muljibhai Patel and Ors vs. State of Gujarat and Ors (dated 10.02.2020)** Court had the power to quash the criminal complaint filed under Section 138 of the N.I. Act on the legal issues like limitation, etc. The Validity of - Sections 114, 406, 420, 465, 467, 468 and 471 of Indian Penal Code, 1860 and Sections 138 and 139 of Negotiable Instruments Act, 1881 was in question. Hence, present appeal - Whether High Court erred in quash criminal case against Accused under Section 138 of Act and declining to quash FIR against Appellants under Sections 114, 406, 420, 465, 467, 468 and 471 of Code. Supreme Court held, while allowing the appeals that though, the Court had the power to quash the criminal complaint filed under Section 138 of the N.I. Act, 1881 on the legal issues like limitation, etc. Criminal complaint filed under Section 138 of the N.I. Act, 1881 against accused ought not to have been quashed merely on the ground that there are inter se dispute between Appellant No. 3 and Respondent No. 2. Without keeping in view the statutory presumption raised under Section 139 of the N.I. Act,1881 the High Court, committed a serious error in quashing the criminal complaint filed under Section 138 of N.I. Act, 1881. **2. Pareshbhai Amrutlal Patel and Ors. vs. The State of Gujarat and Ors.(dated 28.02.2020)** ***Since the issue in both the cases revolves around the same cheque, therefore, instead of quashing the FIR, the ends of justice would meet if proceedings arising out of FIR were transferred to the Court of Judicial Magistrate*** Quashing of proceedings - Denial of - Sections 114, 120-B, 379, 406, 419, 420, 465, 467, 468 and 475 of Indian Penal Code, 1860	Case laws has been added for more clarity.

	and Section 138 of the Negotiable Instrument Act, 1881 was in question. Hence, in present appeal - Whether impugned proceedings initiated against Appellants liable to be quashed. It is held, while disposing off the appeal: (i) The issue in both the complaints pertains to cheque which was said to be from the cheque book of the Company of which Respondent No. 2 was the officer. (ii) Since the issue in both the cases revolves around the same cheque, therefore, instead of quashing the FIR, the ends of justice would meet if proceedings arising out of FIR were transferred to the Court of Judicial Magistrate, where the proceedings of other complaint under Section 138 of the NI Act were pending so that the complaint filed by the Appellants and the proceedings arising out of FIR alleged by Respondent No. 2 were decided together to avoid contradictory judgments and to facilitate the issues which were common in both.	
Lesson 11 Consumer Protection	**Judicial Pronouncement** **1. Punjab and Sind Bank and Ors. vs. Durgesh Kuwar (25.02.2020 -Supreme Court)** Considering the period which has elapsed, it would be necessary for the Court to issue a direction, which, while sub-serving the interest of the bank, is also consistent with the need to preserve the dignity of a woman employee who, we hold, has been unfairly treated. The Honorable Court is of the view that the High Court cannot be faulted in coming to the conclusion that the transfer of the respondent, who was holding the office of Chief Manager in the Scale IV in Indore branch to the branch at Sarsawa in the district of Jabalpur was required to be interfered with. At the same time, a period of nearly four years has since elapsed. Despite the order of stay, the respondent was not assigned an office at Indore and had to suffer the indignity of being asked to sit away from the place assigned to a Branch Manager. Considering the period which has elapsed, it would be necessary for the Court to issue a direction, which, while sub-serving the interest of the bank, is also consistent with the need to preserve the dignity of a woman employee who, we hold, has been unfairly treated. We accordingly direct that Ms. Durgesh Kuwar, the respondent officer, shall be reposted at the Indore branch as a Scale IV officer for a period of one year from today. While affirming the decision of the High Court, the appeal is disposed of in terms of the above directions. The respondent	Case laws has been added for more clarity.

	would be entitled to costs quantified at Rs 50,000 which shall be paid over within one month. **2. Canara Bank vs. United India Insurance Co. Ltd. (06.02.2020 Supreme Court)** Beneficiaries of the policies taken out by the insured are also 'consumers' under the Consumer Protection Act. In the above case, some farmers had stored their agricultural produce in the cold storage run by a partnership firm and took loan from the Canara Bank against the agricultural produce stored in the cold storage. The cold store was insured with United India Insurance Co. Ltd. A fire took place in cold store, the entire building with agricultural produce was destroyed. The cold store owners had taken out a comprehensive insurance policy and raised claim with the insurance company but the claim was repudiated on the ground that the fire was not an accidental fire. The farmers also issued notice to insurance company in respect of the plant, machinery and building but this claim was also repudiated by the insurance company on additional ground that the farmers had no locus standi to make the claim and there was no privity between the farmers and insurance company. The farmers filed a claim against cold store, Canara Bank and the Insurance Company. It was found that in the tripartite agreement among the farmers, Canara Bank and Cold store, it was mandatory to insure the agricultural produce hypothecated with the Canara Bank. The Honorable Supreme Court held that the beneficiaries of the policies taken out by the insured are also 'consumers' under the Consumer Protection Act, even though they are not parties to the contract of insurance.	
Lesson 12 Loans and Advances	**Electronic Cards for Overdraft Accounts:** It has been decided to permit banks to issue electronic cards to natural persons having overdraft accounts that are only in the nature of personal loan without any specific end-use restrictions. The card shall be issued for a period not exceeding the validity of the facility and shall also be subject to the usual rights of the banks as lenders. The card shall be allowed to be used for domestic transactions only. Adequate check and balances shall be put in place to ensure that the usage of such cards is restricted to facilitate online / non-cash transactions. The restriction on cash transaction will not apply to overdraft facility provided. Prior to launching the product, the banks shall frame a Board approval policy on issuance of electronic cards to above mentioned overdraft accounts, encompassing appropriate risk management, periodic review procedures, grievance redressal mechanism, etc., which will be subject to supervisory review.	Regulatory updates.

	The card shall be issued subject to instructions on terms and conditions, security, grievance redressal, confidentiality of customer information as applicable for debit cards and all other relevant instructions on card operations issued by RBI.	
	Judicial Pronouncements 1. In the matter of **Bank of India Vs. M/s. Brindavan Agro Industries Pvt. Ltd**. [Civil Appeal No. 1720 of 2020 arising out of SLP. (Civil) No. 2007 of 2019], Honorable Supreme Court set aside the orders passed by the NCDRC and SCDRC. It was found that though, the Bank agreed to refund Rs.9.16 lakhs from the processing charges through email dated 29th June 2012 but the Consumer had not accepted such proposal in its e-mail dated 24th July, 2012. Therefore, the Court held that the Consumer is entitled to refund of Rs.9.16 lakhs only in terms of the decision of the Bank communicated to the Consumer rather than waiver of TEV charges in its entirety. The request was to give concession of 50% of all charges, therefore, it is the cumulative amount of charges which is to be taken into consideration and not the charges under a particular head. ***2. Vicky vs. State (Govt . of NC T of Delhi) (13.01.2020 Supreme Court)*** The substantive sentences in first two groups and that in respect of the case in the third group would run consecutively The Honorable court has referred the case of V.K. Bansal, wherein the appellant-accused was facing fifteen cases and the Supreme Court has grouped fifteen cases into three different groups:- (i) the first having twelve cases relating to advancement of 8 loan/banking facility to M/s Arawali Tubes Ltd. acting through the appellant thereon as Director; (ii) the second having two cases relating to advancement of loan to the appellant M/s Arawali Alloys Ltd. acting through the appellant as its Director; and (iii) the third having a single case qua the criminal complaint by the State Bank of Patiala. The Court directed that the substantive sentences within first two groups would run inter-se concurrently. The Supreme Court directed that the substantive sentences in first two groups and that in respect of the case in the third group would run consecutively. 3. **Bank of Baroda vs. Kotak Mahindra Bank Ltd**. (17.03.2020 Supreme Court) The period of limitation shall be governed by the Act and not by Section 44A of the CPC, since the latter provides only for the	Case laws has been added for more clarity.

	procedure to be followed for executing a foreign decree Kotak Mahindra Bank Ltd., issued a Letter of Credit for US $1,794,258 on behalf of its customer M/s. Aditya Steel Industries Limited in favour of M/s. Granada Worldwide Investment Company, London. The appellant Bank of Baroda was the confirming bank to the said letter of credit. The Vysya Bank issued instructions to the London branch of the appellant on 12.10.1992 to honour the Letter of Credit. Acting on this instruction the London branch of the appellant discounted the Letter of Credit for a sum of US $ 1,742,376.41 and payment of this amount was made to M/s Granada Worldwide Investment Company on 13.10.1992. Later in 2009, Bank of Baroda filed an Execution Petition against Kotak Mahindra Bank under Section 44A read with Order 21 Rule 3 of the CPC for recovery of Rs.16,43,88,187.86. The Execution Petition was filed in view of the decree passed by the High Court of Justice, Queens Bench, Divisional Commercial Court of London (UK Court) on 20 February 1995 for US$ 1,267,909.26 in favour of Bank of Baroda. The maintainability of the Execution Petition was challenged primarily on the ground of limitation. One major Issue in the case for the court to decide 'What is the limitation for filing an application for execution of a foreign decree of a reciprocating country in India?' For this major issue of the case that related to the limitation period , the Supreme Court had rejected the argument that there is no limitation period for execution of foreign decree in India while observing that the term "application" in Section 3 of the Act shall be deemed to include execution petitions The period of limitation shall be governed by the Act and not by Section 44A of the CPC, since the latter provides only for the procedure to be followed for executing a foreign decree.	
Lesson 13 Securities for Banker's Loan	**Judicial Pronouncements** 1. In the matter of ***Aarifaben Yunusbhai Patel and Ors. vs. Mukul Thakorebhai Amin and Ors (2020),*** the court has come to the conclusion that the auction of both the properties were vitiated on account of lack of notice to the judgment-debtor, and that being an error fatal to the validity of auction sale, in light of the decision of the Supreme Court the auction sale cannot be permitted to remain and they have to be quashed. Other submissions of the counsel for the auction purchasers therefore need not be elaborately dealt with, but suffice it to say that the Court is quashing the auction sale on ground of non-compliance with the mandatory provision of notice to the judgment-debtor." The court was constrained to observe that the High Court totally ignored the order of this Court quoted hereinabove. This Court had specifically directed the executing court to decide both, the issue of limitation and objections on merits. This was obviously	Case laws has been added for more clarity.

	done with the purpose that in case later if the issue of limitation is decided in favour of the objectors, R-1 and R-3, then the matter again should not be remanded for decision on merits of the case. The issue of limitation could not have been ignored and should have been decided by the High Court. 2. In the matter of Appeal in ***Connectwell Industries Pvt . Ltd . vs . Union of India (UOI) and Ors . (06. 03. 2020 - SC) . (17. 03. 2020 - Supreme Court),*** *t*he Honorable Supreme Court held that there is no dispute regarding the facts of this case. The property in dispute was mortgaged by BPIL to the Union Bank of India in 2000 and the DRT passed an order of recovery against the BPIL in 2002. The recovery certificate was issued immediately, pursuant to which an attachment order was passed prior to the date on which notice was issued by the Tax Recovery Officer- Respondent No.4 under Rule 2 of Schedule II to the Act. It is true that the sale was conducted after the issuance of the notice as well as the attachment order passed by Respondent No.4 in 2003, but the fact remains that a charge over the property was created much prior to the notice issued by Respondent No.4 on 16.11.2003. The High Court held that Rule 16(2) is applicable to this case on the ground that the actual sale took place after the order of attachment was passed by Respondent No.4. The High Court failed to take into account the fact that the sale of the property was pursuant to the order passed by the DRT with regard to the property over which a charge was already created prior to the issuance of notice on 11.02.2003. As the charge over the property was created much prior to the issuance of notice under Rule 2 of Schedule II to the Act by Respondent No.4, we find force in the submissions made on behalf of the Appellant. The judgment of the High Court is set aside and the Appeal is allowed. The MIDC is directed to issue a 'No Objection" certificate to the Appellant. 3. In ***Anuj Jain vs. Axis Bank Limited and Ors. (26. 02. 2020 - Supreme Court)***, the honorable Supreme Court on the issue as to whether lenders of JAL could be treated as financial creditors, hold that such lenders of JAL, on the strength of the mortgages in question, may fall in the category of secured creditors, but such mortgages being neither towards any loan, facility or advance to the corporate debtor nor towards protecting any facility or security of the corporate debtor, it cannot be said that the corporate debtor owes them any 'financial debt' within the meaning of Section 5(8) of the Code; and hence, such lenders of JAL do not fall in the category of the 'financial creditors' of the corporate debtor JIL. 4. In ***K. Virupaksha and Ors. vs . The State of Karnataka and Ors. (03.03.2020 -Supreme Court)***	

	Criminal proceeding would not be sustainable in a matter of the present nature, exposing the appellants even on that count to the proceedings before the Investigating Officer or the criminal court would not be justified. The appellants herein had also referred to the provision as contained in Section 32 of the SARFAESI Act which provides for the immunity from prosecution since protection is provided thereunder for the action taken in good faith. The learned senior counsel for the Complainant has in that regard referred to the decision of this Court in the case of ***General Officer Commanding, Rashtriya Rifles vs. Central Bureau of Investigation & Anr. (2012) 6 SCC 228*** to contend that the defence relating to good faith and public good are questions of fact and they are required to be proved by adducing evidence. Though on the proposition of law as enunciated therein there could be no cavil, which aspect of the matter is also an aspect which can be examined in the proceedings provided under the SARFAESI Act, 2002. In a circumstance where we have already indicated that a criminal proceeding would not be sustainable in a matter of the present nature, exposing the appellants even on that count to the proceedings before the Investigating Officer or the criminal court would not be justified. 5. ***Pandurang Ganpati Chaugule vs. Vishwasrao Patil Murgud Sahakari Bank Limited (05.05.2020 Supreme Court)*** Recovery is an essential part of banking; as such, the recovery procedure prescribed under section 13 of the SARFAESI Act, is applicable to Co-operative banks The question in this matter for the determination was 'Whether the 'SARFAESI Act' is applicable to Cooperative Banks? The Honorable Supreme held that the cooperative banks established under the State Legislation and MultiState Cooperative Banks are 'banks' under section 2(1)(c) of Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002 (SARFAESI Act). It was held that the recovery is an essential part of banking; as such, the recovery procedure prescribed under section 13 of the SARFAESI Act, legislation relatable to Entry 45 List I of the Seventh Schedule to the Constitution of India, is applicable. It was further held that the Parliament has legislative competence under Entry 45 of List I of the Seventh Schedule of the Constitution of India to provide additional procedures for recovery under section 13 of the SARFAESI Act with respect to cooperative banks. A It was concluded that the provisions of Section 2(1)(c)(iva), of SARFESI Act, adding "ex abundanticautela", 'a multistate cooperative bank' is not ultra vires as well as the notification dated 28.1.2003 issued with	

	respect to the cooperative banks registered under the State legislation.	
Lesson 18 Non Performing Assets	**Prudential Norms on Income Recognition, Asset Classification and provisioning pertaining to Advances – Projects under Implementation.** Circular RBI/2019-20/158 DOR.No.BP.BC.33/ 21.04.048/2019-20 dated February 07, 2020 The revised guidelines for deferment of date of commencement of commercial operations (DCCO) for projects in non-infrastructure and commercial real estate (CRE) sectors projects are as under: i) revisions of the date of DCCO and consequential shift in repayment schedule for equal or shorter duration will not be treated as restructuring provided – the revised DCCO falls within the period of one year from the original DCCO stipulated at the time of financial closure of CRE projects and other terms and conditions of the loan remain unchanged. ii) In case of CRE projects delayed for reasons beyond the control of promotor(s), banks may restructure them by way of revision of DCCO up to another one year and retain the 'standard asset' classification. In such CRE projects loans bank will have to ensure that the revised repayment schedule is extended only by a period equal to or shorter than the extension in DCCO iii) Banks may fund cost overruns that arise on account of extension of DCCO iv) a loan for a project may be classified as NPA during any time before commencement of commercial operations as per record of recovery. v) At the time of extending DCCO, banks should satisfy themselves about the viability of the project and the restructuring plan. (It is decided to extend the above guidelines issued to banks, mutatis mutandis, to NBFCs as well)	Regulatory Updates.
	One Time Restructuring of existing loans to MSMEs. RBI/2019-20/ 160 DOR..No.BP.BC.34/21.04.048./2019-20 February 11, 2020 It has been decided to extend the one time restructuring of MSME advances permitted in terms of the circular DBR.No.BP.BC.18/21.04048/2018-19 dated January 1, 2019 accordingly, a one time restructuring of existing loans to	Regulatory updates.

	MSMEs classified as 'standard' without a downgrade in the asset classification is permitted subject to: i) the aggregate exposure , including non-fund based facilities, of a bank and NBFCs to the borrower does not exceed Rs. 25 crore as on January 1, 2020. ii) the borrower's account was a 'standard asset' as on 01/01/2020 and continues to be so till the date of implementation of restructuring. iii) the restructuring is implemented on or before 31/12/2020 iv) The borrowing entity is GST-registered on the date of implementation of restructuring.	