

**“ഭരണഭാഷ മാതൃഭാഷ”**

ഡി.സി.എ/1396/2024/എ.ഡി (2)

സഹകരണ ഓഡിറ്റ് ഡയറക്ടറേറ്റ്,  
തിരുവനന്തപുരം, തീയതി : 19.11.2024

**സർക്കുലർ നം. 04/2024**

**വിഷയം- സഹകരണ വകുപ്പ് - ഓഡിറ്റ് ഡയറക്ടറേറ്റ് - Auditing in IT Environment - special Drive in പ്രൈമറി അഗ്രിക്കൾച്ചറൽ ക്രെഡിറ്റ് കോ-ഓപ്പറേറ്റീവ് സൊസൈറ്റി - സംബന്ധിച്ച്.**

സംസ്ഥാനത്തെ പ്രാഥമിക കാർഷിക വായ്പ സഹകരണ സംഘങ്ങളുടെ ഓഡിറ്റുവേളയിൽ കമ്പ്യൂട്ടർ സോഫ്റ്റ് വെയറുമായി ബന്ധപ്പെട്ട് പല ഗുരുതര ന്യൂനതകളും കണ്ടെത്തിയിട്ടുള്ള സാഹചര്യത്തിൽ പ്രാഥമിക കാർഷിക വായ്പ സംഘങ്ങളിലെ ഇൻഫോർമേഷൻ ടെക്നോളജി സംവിധാനങ്ങളുടെ പരിശോധന നടത്തുന്നതിലേക്കായി Auditing in IT Environment-മായി ബന്ധപ്പെട്ട് ഒരു സ്പെഷ്യൽ ഡ്രൈവ് സംഘടിപ്പിക്കാൻ തീരുമാനിച്ചിരിക്കുന്നു. ആയതിനുള്ള മാർഗ്ഗ നിർദ്ദേശങ്ങൾ ചുവടെ ചേർക്കുന്നു.

1. റെഗുലർ ഓഡിറ്റിന്റെ ഭാഗമായിട്ടായിരിക്കണം സ്പെഷ്യൽ ഡ്രൈവ് നടപ്പിലാക്കേണ്ടത്. അതാത് സംഘങ്ങളുടെ ഓഡിറ്റ് ടീം തന്നെയാണ് ഈ സ്പെഷ്യൽ ഡ്രൈവ് നിർവഹിക്കേണ്ടത്.
2. സ്പെഷ്യൽ ഡ്രൈവിന്റെ ഓഡിറ്റ് മെട്രിക്സ്/ചെക്ക് ലിസ്റ്റ് ഇതിനോടൊപ്പം ചേർത്തിട്ടുണ്ട്. ആയതിൽ ഉൾക്കൊള്ളിക്കാത്ത IT System/Operations സംഘത്തിൽ ഉണ്ടെങ്കിൽ ഓഡിറ്റർമാർ അതു കൂടി ചെക്ക് ചെയ്യേണ്ടതാണ്.
3. ഇത്തരത്തിൽ ചെക്കിംഗ് നടത്തി ന്യൂനതകൾ കണ്ടെത്തുന്ന സാഹചര്യത്തിൽ ഓഡിറ്റർമാർ ടി ന്യൂനതകൾ സർക്കുലർ 01/2023 പ്രകാരം Draft audit Memo ആയി സംഘം അധികാരികൾക്ക് നൽകേണ്ടതാണ്.
4. ടി വിഷയവുമായി ബന്ധപ്പെട്ട് ജില്ലയിൽ ജോയിന്റ് ഡയറക്ടർ ഓഫീസിലെ അസിസ്റ്റന്റ് ഡയറക്ടറെ നോഡൽ ഓഫീസറായി ചുമതലപ്പെടുത്തുന്നു.

5. ജില്ലയിലെ എല്ലാ പ്രാഥമിക കാർഷിക വായ്പ സഹകരണ സംഘങ്ങളിലും സ്പെഷ്യൽ ഡ്രൈവ് പ്രകാരം പരിശോധന സമയബന്ധിതമായി നടക്കുന്നുവെന്ന് നോഡൽ ഓഫീസർ ഉറപ്പ് വരുത്തേണ്ടതാണ്.

6. ഓഡിറ്റർമാർക്ക് സ്പെഷ്യൽ ഡ്രൈവ് വിജയകരമായി പൂർത്തീകരിക്കുന്നതിനാവശ്യമായ എല്ലാ സഹായങ്ങളും ജില്ലയിൽ നിയമിച്ചിട്ടുള്ള IT ഓഡിറ്റ് സപ്പോർട്ട് സെല്ലിലെ ഓഡിറ്റർമാരുമായി ചേർന്ന് നോഡൽ ഓഫീസർ നൽകേണ്ടതാണ്.

7. സ്പെഷ്യൽ ഡ്രൈവ് പ്രകാരം ഓഡിറ്റ് ടീം തയ്യാറാക്കി സമർപ്പിക്കുന്ന ഡ്രാഫ്റ്റ് ഓഡിറ്റ് മെമ്മോയുടെ (DAM) അടിസ്ഥാനത്തിൽ നോഡൽ ഓഫീസർ ചുവടെ പറയുന്ന മാതൃകയിൽ റിപ്പോർട്ട് തയ്യാറാക്കി എല്ലാ ആഴ്ചയും ജില്ല ജോയിന്റ് ഡയറക്ടർക്ക് സമർപ്പിക്കേണ്ടതാണ്.

Name of PACS	Taluk	% of Completion	Audit Team	Date of Issue of DAM	Whether reply to DAM received

8. ജില്ലാ ജോയിന്റ് ഡയറക്ടർമാർ ഓരോ രണ്ടാഴ്ച കൂടുമ്പോഴും ഓഡിറ്റ് ഡയറക്ടർക്ക് പുരോഗതി റിപ്പോർട്ട് സമർപ്പിക്കേണ്ടതാണ്.

9. സ്പെഷ്യൽ ഡ്രൈവുമായി ബന്ധപ്പെട്ട് ഓഡിറ്റർമാർക്കുള്ള സംശയ ദൂരീകരണം നടത്തുന്നതിന് എല്ലാ ജില്ലകളിലും IT ഓഡിറ്റ് സപ്പോർട്ട് സെൽ രൂപീകരിച്ചിട്ടുണ്ട്.

10. ഡിസംബർ 31-നകം ജില്ലയിലെ എല്ലാ പ്രാഥമിക കാർഷിക വായ്പ സഹകരണ സംഘങ്ങളിലും ടി സ്പെഷ്യൽ ഡ്രൈവ് പൂർത്തിയാക്കുന്നതിനുള്ള പ്ലാൻ, ജില്ലാ ജോയിന്റ് ഡയറക്ടർമാർ നിശ്ചയിച്ച് താലൂക്ക് അസിസ്റ്റന്റ് ഡയറക്ടർമാർക്കും, ഓഡിറ്റർമാർക്കും ആവശ്യമായ ഉത്തരവും, നിർദ്ദേശങ്ങളും സഹിതം നൽകേണ്ടതാണ്.

11. ഓഡിറ്റ് ടീം സംഘങ്ങളിലെ IT Audit Special Drive ഡിസംബർ 31-നകം പൂർത്തിയാക്കി കണ്ടെത്തിയ ന്യൂനതകൾക്കുള്ള സംഘത്തിന്റെ മറുപടി രണ്ടാഴ്ചക്കകം സംഘത്തിൽ നിന്നും വാങ്ങേണ്ടതാണ്.

12. സംഘം സമയബന്ധിതമായി മറുപടി നൽകിയില്ലെങ്കിൽ ജോയിന്റ് ഡയറക്ടർ/ അസിസ്റ്റന്റ് ഡയറക്ടർ ആയത് സംബന്ധിച്ച് മീറ്റിംഗ് വിളിച്ചു കൂട്ടി സംഘത്തിന്റെ മറുപടി മിനിറ്റസ് ആക്കി സാക്ഷ്യപ്പെടുത്തലുകളോടെ സൂക്ഷിക്കേണ്ടതാണ്.

13. മേൽ നിർദ്ദേശപ്രകാരം ഓഡിറ്റർമാർ സമർപ്പിക്കുന്ന ന്യൂനതകളും ആയതിന് സംഘം നൽകിയ മറുപടിയും അതാത് ജില്ലയിലെ IT audit support cell പരിശോധിച്ച് ആഡിറ്റ് കണ്ടെത്തലുകളിൽ ഏറ്റവും ഗുരുതര സ്വഭാവമുള്ള 5 എണ്ണം Para 1, Para 2, Para 3, Para 4, Para 5 എന്ന് ഓരോ ഓരോ Para-യും അടയാളപ്പെടുത്തി താഴെപ്പറയുന്ന format ൽ തയ്യാറാക്കി ജില്ല ജോയിന്റ് ഡയറക്ടർക്ക് സമർപ്പിക്കേണ്ടതാണ്.

1. Audit Criteria
2. Audit Observation
3. Audit Findings
4. The findings observed in ..... PACS out of .....PACS in the District.
5. A table or chart to summarize the findings if required.
6. Causes And effects
7. Reply by the society.
8. Whether it is acceptable in audit? If not, why?
9. Audit conclusion
10. Audit recommendation

14. മേൽ പരാമർശിച്ചിട്ടുള്ള ഓരോ ഓഡിറ്റ് Para-കളും ജില്ലാ ജോയിന്റ് ഡയറക്ടർമാർ വിശദമായി രേഖകളുടെ (Audit Evidence) അടിസ്ഥാനത്തിൽ പരിശോധിച്ച് ഓരോ Para-കളിലും ജോയിന്റ് ഡയറക്ടറുടെ അഭിപ്രായം രേഖപ്പെടുത്തി ഓഡിറ്റ് ഡയറക്ടർക്ക് ജനുവരി 31-നകം സമർപ്പിക്കേണ്ടത്.


15. ധനാപഹരണമോ, മറ്റ് സാമ്പത്തിക ക്രമക്കേടുകളോ ടി ഓഡിറ്റിൽ കണ്ടെത്തുന്ന പക്ഷം സ്പെഷ്യൽ റിപ്പോർട്ട് തയ്യാറാക്കുന്നതുൾപ്പടെയുള്ള നിയമപ്രകാരമുള്ള തുടർ നടപടി സ്വീകരിക്കേണ്ടതാണ്.

ഒപ്പ്  
ഷെറിൻ എം.എസ് ഐഎ&എഎസ്  
ഡയറക്ടർ (സഹകരണ ഓഡിറ്റ്)

പകർപ്പ് -

1. സഹകരണ സംഘം രജിസ്ട്രാർ, തിരുവനന്തപുരം.
2. എല്ലാ ജില്ലാ ജോയിന്റ് രജിസ്ട്രാർമാർക്കും
3. എല്ലാ ജില്ലാ ജോയിന്റ് ഡയറക്ടർമാർക്കും
4. പ്രസിഡന്റ് / സെക്രട്ടറി എല്ലാ സഹകരണ സംഘങ്ങൾക്കും
5. എല്ലാ ജില്ലാ ജോയിന്റ് ഡയറക്ടർ/കൺകറന്റ് ഓഡിറ്റർമാർക്കും
6. എല്ലാ അപ്പക്സ് ഓഡിറ്റർമാർക്കും
7. എല്ലാ കൺകറന്റ് ഓഡിറ്റർമാർക്കും
8. എല്ലാ താലൂക്ക് അസിസ്റ്റന്റ് രജിസ്ട്രാർമാർക്കും ഇൻസ്പെക്ടർമാർക്കും (ജോയിന്റ് രജിസ്ട്രാർ മുഖേന)
9. എല്ലാ താലൂക്ക് അസിസ്റ്റന്റ് ഡയറക്ടർമാർക്കും ഓഡിറ്റർമാർക്കും (ജോയിന്റ് ഡയറക്ടർമാർ മുഖേന)
10. സ്റ്റോക്ക് ഫയൽ
11. വെബ് സൈറ്റ്

//ആജ്ഞാനുസരണം//

  
ഡെപ്യൂട്ടി ഡയറക്ടർ

**Comprehensive Matrix for Audit in IT Environment of Credit  
Co-operatives**

<b>General Information</b>			
1	Name of Co-operative society :		
2	Taluk :		
3	District :		
4	No of branches :		
	<b>Audit Questions</b>	<b>Yes/No to Audit Questions</b>	<b>In case of Audit defect mention the Audit Para</b>
1	Whether the Co-operative society is computerized or not		
2	No of non credit activity units using software		
3	Does the society have ATM Services: Withdraw cash, check balances, and sometimes make deposits or transfers at ATMs.		
4	Does the society have Online societying: Access to accounts, transactions, and financial management via a web browser.		
5	Does the society have Mobile societying Apps: Manage accounts, transfer funds, pay bills, and more through a smartphone app.		
6	Does the society have Electronic Funds Transfer (EFT): Transfer money between accounts or to other people electronically.		
7	Does the society have eStatements: Access and download society statements electronically rather than receiving paper copies.		
8	Does the society have Automatic Bill Payment: Set up recurring payments for regular expenses.		
9	Does the society have SMS Alert : is a feature that keeps customers informed about their account activities and transactions through real-time notifications sent via SMS		
10	Has the society appointed a System Administrator? Please verify their qualifications and assess the extent of their liability and accountability in managing the society's IT systems and ensuring compliance with security protocols.		
<b>1</b>	<b><i>IT Policy</i></b>		
	Does the society have a comprehensive IT policy that covers key areas such as data		

1.1	security, access control, cybersecurity measures, disaster recovery, and compliance with legal regulations, and how is its effectiveness monitored and audited regularly?		
<b>2 Agreement with Vendor</b>			
2.1	Are specific terms outlined in the Master Services Agreement (MSA) that address intellectual property rights and liability?		
2.2	Does the Service Level Agreement (SLA) include specific metrics for performance expectations and uptime guarantees?		
2.3	Are specific deliverables and timelines outlined in the Statement of Work (SOW) for ongoing projects?		
2.4	Does the Software License Agreement state restrictions and compliance requirements, particularly regarding duration of license, user limits and usage restrictions?		
2.5	Does the Data Processing Agreement (DPA) ensure compliance with privacy laws, such as GDPR, and include data protection measures?		
2.6	Does the Services Level Agreement define a range of services that align with the society's operational needs?		
2.7	Does the society's Service Level Agreement (SLA) address transaction processing times and customer support responsiveness?		
2.8	Are security measures specified in the Security and Compliance Agreement to meet financial regulations, including anti-money laundering (AML) and Know Your Customer (KYC) protocols?		
2.9	Are key terms in the Fee Schedule outlined, including the structure for transaction fees, service charges, and penalties for non-compliance?		
2.10	Are procedures established in the Dispute Resolution Mechanism for handling disputes, including preferred methods such as mediation or arbitration?		
2.11	Is the AMC, hosting charges, and assistance of a service engineer mentioned in the agreement?		
2.12	Does the agreement include a beneficial exit Policy?		
2.13	Are there any unfavorable clauses in the exit policy regarding migration or termination of the Agreement?		
	Deos the society conducted Migration audit		

2.14	and old software and back up maintained properly?		
<b>3</b>	<b><i>CORE societying / Client - Server Network</i></b>		
3.1	<b>If Client - Server Network</b>		
3.2	Server Room: Is there a dedicated room within the society for housing servers and other IT equipment?		
3.3	<b>Access Control:</b> Are access control measures implemented to restrict entry to the room to authorized personnel only, such as biometric scanners, key card readers, and PIN codes?		
3.4	<b>Physical Locks:</b> Are high-quality, tamper-resistant physical locks installed on doors and entry points to enhance the security of sensitive areas?		
3.5	<b>Climate Control:</b> Are climate control measures, including cooling systems and monitoring protocols, in place to maintain optimal temperature and humidity levels in critical areas?		
3.6	<b>Power Management:</b> Are power management systems, such as uninterruptible power supplies (UPS) and backup generators, implemented to ensure uninterrupted operations and prevent downtime during power outages?		
3.7	<b>Surveillance:</b> Are measures in place to ensure that continuous video surveillance (CCTV) effectively monitors all access points and internal areas, and is the recorded footage securely stored for future review?		
	<b>IF Cloud/CORE societying</b>		
3.8	Does the society has a Cloud Service Provider (AWS, Azure, Google Cloud, Others)		
3.9	Is the society's data stored in a specific geographic region / in multiple regions?		
3.10	Is data backed up frequently, and are the backups automated?		
3.11	Are encryption methods and access protocols used to protect data at rest and in transit?		
3.12	Is access to cloud systems restricted through multi-factor authentication (MFA) and role-based access control (RBAC)?		
3.13	Does the cloud provider offer disaster recovery services, and is there a disaster recovery plan in place for the society?		
3.14	Does the society conduct DC/DR drills regularly, and can you check the last date of the drill conducted?		
3.15	Is the guaranteed uptime specified in the Service Level Agreement (SLA)?		

3.16	Is the cloud provider compliant with financial industry standards (e.g., PCI DSS:Payment card industry data security, GDPR: General data protection regulation)?		
3.17	Does the society have a strategy to avoid vendor lock-in, ensuring that data is easily transferable to another provider if needed?		
3.18	Is the cloud infrastructure easily scalable up or down to meet business demands?		
3.19	Are security monitoring tools or services in place to detect suspicious activity in the cloud environment?		
3.20	Does the cloud provider maintain detailed audit logs of all activities within the cloud environment?		
3.21	Is customer support provided by the cloud provider at a 24/7 level?		
3.22	Is there clarity in the contract about who owns the data hosted in the cloud and the associated data ownership rights?		
3.23	Is there a clearly defined incident response plan in collaboration with the cloud provider for handling security incidents?		
3.24	Is the Unified Customer Identification Number (UCIN) implemented in the society's software, and does it contribute to improving customer data management, KYC processes, and compliance with regulatory requirements like GST and TDS?		
3.25	Is role-based access control (RBAC) implemented in the society's software systems to ensure that users have the minimum necessary permissions for their roles, and are there measures in place to monitor and manage these access rights effectively?		
3.26	Is authorization granted to more than one employee within any branch, and does this practice align with the society's internal controls and security policies?		
<b>4</b>	<b><i>Password Management</i></b>		
4.1	<b>Maker-Checker Policy:</b> Is the Maker-Checker Policy implemented in the software to ensure secure transaction processing, and are there measures in place to maintain accountability and compliance within this framework?		
4.2	<b>System Logs Review.</b> Are system logs reviewed frequently to ensure that staff are updating their passwords in accordance with the society's policy, and have there been any		



	instances of non-compliance?		
4.3	<b>Password Complexity:</b> Do all staff members' passwords meet the required complexity standards (e.g., length, special characters, and numbers), and are there systems in place to enforce this?		
4.4	<b>Multi-Factor Authentication:</b> Is multi-factor authentication (MFA) enabled and consistently used by all staff for accessing sensitive systems, and is its effectiveness monitored?		
4.5	<b>Password Change History:</b> Are staff required to change their passwords regularly, and does the system prevent the reuse of old passwords?		
4.6	<b>Compliance Audits:</b> Are random compliance audits conducted frequently to ensure the password policy is enforced, and are measures taken when non-compliance is identified?		
4.7	<b>Criteria for Reports:</b> Are there specific criteria or thresholds set within the Core Banking System (CBS) to generate Exceptional Reports for unusual transactions?		
4.8	<b>Monitoring Frequency:</b> Are Exceptional Reports reviewed frequently by the society's management or compliance team to detect irregularities?		
4.9	<b>Unusual Transactions:</b> Are unusual transactions, such as those exceeding predefined limits, identified and investigated through Exceptional Reports?		
4.10	<b>Failed Transactions:</b> Are failed transactions flagged by Exceptional Reports handled and investigated by the society, and are follow-up actions taken?		
4.11	<b>Unauthorized Access:</b> Are there processes in place to detect and respond to unauthorized access attempts highlighted in Exceptional Reports?		
4.12	<b>High-Risk Activity:</b> Does the society manage and investigate high-risk activities flagged in Exceptional Reports, such as sudden spikes in cross-border transactions or account activity?		
4.13	<b>Account Irregularities:</b> Does the society take specific steps when account irregularities, such as unusual activity in dormant accounts, are detected in Exceptional Reports?		
4.14	<b>Risk Management:</b> Are Exceptional Reports integrated into the society's overall risk management strategy to prevent fraud and		

	ensure compliance?		
4.15	<b>Response Time:</b> Is there a standard response time for investigating and addressing anomalies identified in Exceptional Reports?		
4.16	<b>Audit and Review:</b> Are Exceptional Reports utilized during internal audits to ensure that transactions and activities comply with the society's internal controls and regulatory standards?		
<b>5</b>	<b><i>Application Control</i></b>		
5.1	Whether the society done day start, day end, year end and back up procedures in time?		
5.2	Whether the Parameter/ Master File/Master Settings accessible to the operators should only be in read-only format?		
5.3	Is there proper authorization policy implemented for creating and modifying account heads, users and customers through super password or double password?		
5.4	Is there dual authentication is applied in software for gold rate settings and interest rate settings?		
<b>6</b>	<b><i>Automated Teller Mechine (ATM)</i></b>		
6.1	<b>Physical Security:</b> Does the society ensure that ATMs are placed in secure locations with proper surveillance cameras and anti-skimming devices installed?		
6.2	<b>Software and Updates:</b> Is the ATM software regularly updated with the latest security patches, and is its connection to the core societying system monitored for real-time processing?		
6.3	<b>Transaction Integrity:</b> Does the society ensure that all ATM transaction logs are accurate and properly reconciled with customer receipts to detect discrepancies?		
6.4	<b>Cash Management:</b> Are processes in place to monitor ATM cash levels and cash replenishment and audits conducted frequently to prevent theft or shortages?		
6.5	<b>Disaster Recovery:</b> Does the ATM have a backup power system in place to ensure continuous operation during power outages, and is there a disaster recovery plan for system failures?		
6.6	<b>Compliance and Security:</b> Does the society ensure that its ATMs comply with PCI DSS standards, and customer transactions are encrypted for security?		

6.7	<b>User Interface:</b> Is the ATM's user interface regularly reviewed for ease of use, and are necessary accessibility features, such as braille or audio assistance, available for customers with disabilities?		
6.8	<b>Maintenance and Servicing:</b> Are maintenance checks on ATMs performed frequently, and does the society address technical issues or hardware failures promptly?		
6.9	<b>Fraud Detection:</b> Are fraud detection systems in place to monitor and prevent card skimming, and does the society respond to alerts for suspicious or fraudulent transactions?		
6.10	<b>Error Monitoring and Downtime:</b> Does the society monitor error rates and downtime for ATMs, and are steps taken to minimize service interruptions?		
<b>7</b>	<b>NEFT/RTGS</b>		
7.1	Is the society currently offering NEFT and RTGS services to its customers?		
7.2	Does the society follow specific procedures to process NEFT and RTGS transactions?		
7.3	Are there security measures in place to protect NEFT and RTGS transactions from fraud and unauthorized access?		
7.4	Does the society educate its employees and customers about using NEFT and RTGS services effectively and securely?		
<b>8</b>	<b>Third Party Software requirements</b>		
8.1	Is third-party payment gateway software used to securely route NEFT/RTGS transactions between the cooperative society, sponsor society, and NPCI, and is it monitored for efficiency?		
8.2	Is third-party fraud detection software implemented to monitor NEFT/RTGS transactions for suspicious activities, and does it offer features for real-time alerts?		
8.3	Are network solutions employed to ensure reliable connectivity between the CBS and the NEFT/RTGS network, and are they maintained to prevent disruptions?		
<b>9</b>	<b>Firewall</b>		
9.1	Is a firewall currently used in the society's network, is it regularly updated with the latest security patches, and is its performance monitored to ensure continuous protection		

	against threats?		
9.2	Is there a designated team responsible for managing and implementing firewall updates in the society's network, and is there oversight for monitoring the firewall to ensure it functions effectively and remains up to date?		
9.3	Are specific services included in the firewall AMC, and are maintenance activities conducted frequently?		
9.4	Is there a designated individual or team responsible for overseeing the performance and compliance of the firewall under the AMC?		
9.5	Does the society have measures in place to ensure that firewall updates and patches are implemented on time according to the AMC agreement?		
9.6	Are the response times for technical support outlined in the AMC for issues related to the firewall?		
9.7	Is there a provision in the AMC for training to staff on firewall management and security practices?		
<b>10</b>	<b><i>Load Balancer</i></b>		
10.1	Is a load balancer implemented in the society's infrastructure to manage high volumes of transactions and ensure service availability?		
<b>11</b>	<b><i>Fraud Mitigation Strategies</i></b>		
11.1	<b>Cybersecurity Training:</b> Does the society provide training programs to employees to raise awareness about cybersecurity threats and prevent insider threats?		
11.2	<b>Multi-Factor Authentication (MFA):</b> Is multi-factor authentication implemented for both customer accounts and internal systems? How is it enforced?		
11.3	<b>fraud detection and prevention systems:</b> Are there fraud detection and prevention systems in place, and do they monitor transactions for suspicious activities?		
11.4	<b>Data Encryption:</b> Does the society ensure that sensitive customer data is encrypted both in transit and at rest?		
11.5	<b>Incident Response Plan:</b> Does the society have a documented incident response plan, and is it tested and updated regularly?		
	<b>Regular Security Audits:</b> Does the society conduct security audits and vulnerability		

11.6	assessments regularly to identify and mitigate potential risks?		
11.7	<b>Access Control Policies:</b> Are access control measures in place to restrict access to sensitive systems and data, and is user access managed and monitored?		
11.8	<b>Customer Awareness Programs:</b> Does the society have initiatives to educate customers about phishing attacks and safe online societal practices?		
11.9	<b>Monitoring and Logging:</b> Does the society monitor system logs for unusual activities or unauthorized access attempts, and are tools used for this purpose?		
11.10	<b>Third-Party Risk Management:</b> Does the society assess and manage risks associated with third-party vendors that have access to its systems or customer data?		
11.11	<b>Backup and Recovery:</b> Are backup and disaster recovery strategies in place to ensure business continuity in case of a cyber incident?		
11.12	<b>Regulatory Compliance:</b> Does the society ensure compliance with relevant regulations and standards related to data protection and cybersecurity, such as PCI DSS or GDPR?		
11.13	<b>Penetration Testing:</b> Does the society conduct regular penetration testing to identify vulnerabilities in its systems? How are the findings addressed?		
11.14	<b>User Behavior Analytics:</b> Does the society utilize user behavior analytics to detect anomalies in user activity that may indicate fraud or unauthorized access?		
11.15	<b>Reporting Mechanisms:</b> Are there mechanisms in place for employees and customers to report suspicious activities or potential security breaches?		
11.16	<b>IS Audit:</b> Whether the society conducted Information System Audit and was done by the certified IS Auditor?		
<b>12</b>	<b><i>Hardware Used</i></b>		
12.1	Are the society utilized all types of hardware and other IT infrastructure effectively (e.g., servers, workstations, networking equipment)?		
12.2	Is the hardware updated or replaced/disposed regularly to ensure optimal performance and security?		
	Are security measures in place to protect		

12.3	physical hardware from theft, damage, or unauthorized access?		
12.4	Are there any specific hardware security modules (HSMs) used for managing encryption keys?		
<b>13</b>	<b><i>Operating System Licensing</i></b>		
13.1	Genuine and licensed versions of operating systems are in use across the society's systems (e.g., Windows, Linux, etc.)?		
13.2	Whether the society ensure compliance with licensing agreements for its operating systems?		
13.3	Are there regular audits conducted to verify the legitimacy of operating system licenses?		
13.4	Is there any processes to manage and update operating system licenses?		
13.5	Are there regular updating of anti virus softwares?		
13.6	Whether the society handle vulnerabilities associated with operating systems in use?		
<b>14</b>	<b><i>Remote Desktop Viewer</i></b>		
14.1	Is there any remote desktop viewer solutions are implemented within the society (e.g., Microsoft Remote Desktop, TeamViewer, Any desk etc.)?		
14.2	Are there any policy regarding the access of remote desktop protocols for employees?		
14.3	Are there specific policies regarding the use of remote desktop viewers for accessing sensitive information?		
14.4	Whether society follows the security protocols in remote desktop sessions (e.g., encryption, session timeouts, instant password)?		
14.5	Whether the society monitor remote desktop access to detect any unauthorized usage?		
14.6	Are there specific measures taken to ensure the security of data transmitted during remote desktop sessions?		
14.7	Whether the remote desktop sessions authenticated and authorized?		
14.8	Are there any restrictions on the devices that can connect to the society's systems via remote desktop?		
14.9	Whether incident response procedures are in place in case of a security breach involving remote desktop access?		
14.10	Whether the society educate employees about the secure use of remote desktop viewers?		

**15** ***Other Observations***

15.1	What is your overall opinion on the society's information technology environment, including its infrastructure, security measures, and operational efficiency? Additionally, what specific measures would you recommend to enhance the effectiveness and resilience of this IT setup?		
------	---	--	--

# *Comprehensive Matrix for Audit in IT Environment for Credit Co-operatives*

---

## **Introduction**

### **Overview of Information Technology Audit (IT Audit) Scope**

The IT audit of a credit co-operative society involves a comprehensive review of its information technology infrastructure, including hardware, software, networks, and security systems. The audit assesses the effectiveness of the Core Banking System (CBS), online financial services, and other digital platforms in ensuring operational efficiency, security, and compliance with regulatory standards. The scope covers key areas such as:

- Data security and privacy measures for safeguarding sensitive financial and personal information.
- Network security, including firewalls, load balancers, and threat detection systems.
- Compliance with legal and regulatory frameworks, including RBI, PCI DSS, and data protection laws.
- Disaster recovery (DR) and business continuity planning to ensure resilience during crises.
- Software and hardware management, including third-party vendor agreements and system maintenance.
- Access control mechanisms, ensuring that only authorized personnel can access sensitive data and systems.

-

-

### **Objectives and Importance of Audit in IT Environment**

The primary objective of an audit in I T environment is to ensure that the society's IT infrastructure is secure, efficient, and compliant with regulatory standards. The importance of audit in IT environment includes:



- Risk Mitigation: Identifying vulnerabilities in the society's IT systems that could lead to data breaches, fraud, or operational failures.
- Operational Efficiency: Ensuring that the society's IT systems are running smoothly, allowing for optimal performance and customer satisfaction.
- Compliance: Verifying that the society complies with all relevant regulations, such as RBI guidelines, anti-money laundering (AML), and know your customer (KYC) norms.
- Data Integrity and Security: Protecting customer data and ensuring the integrity of financial transactions through proper system controls.
- Disaster Preparedness: Assessing the society's disaster recovery and business continuity plans to ensure minimal disruption in case of system failures or cyber attacks.

## **Table of Contents**

- **General Information**
  - Name of Co-operative Society
  - Taluk and District
  - Number of Branches
  - Computerization Status
  - Non-Credit Units Using Software
- **Financial Services**
  - ATM Services
  - Online and Mobile Apps
  - Electronic Funds Transfer (EFT)
  - E Statements
  - Automatic Bill Payments
  - SMS Alerts
- **IT Personnel**
  - Appointment of System Administrator
  - Qualifications and Responsibilities
- **Information Technology (IT) Policy**
  - Data Security and Privacy
  - Access Control
  - Cyber Security Measures
  - Software and Hardware Management
  - Disaster Recovery and Business Continuity
  - Compliance with Legal Obligations

- Monitoring and Auditing Procedures
- **Agreements with Software Vendors**
- Master Services Agreement (MSA)
- Service Level Agreement (SLA)
- Statement of Work (SOW)
- Software License Agreement
- Data Processing Agreement (DPA)
- Non-Disclosure Agreement (NDA)
- Payment Terms and Invoicing
- Maintenance and Support Agreement
- **Cloud Solutions**
- Cloud Service Providers (AWS, Azure, etc.)
- Data Storage Solutions
- Data Backup and Recovery
- Data Security and Encryption
- Access Control and Compliance
- **Network Security**
- Firewall Management
- Load Balancer Setup and Maintenance
- Fraud Detection Systems
- Threat Detection and Response
- **NEFT/RTGS Integration**
- Membership with RBI Payment Systems
- Security Protocols for Transactions
- Staff and Customer Training
- Regulatory Compliance
- **Physical Security**
- Server Room Access Control
- CCTV Surveillance and Power Management
- Climate Control Systems
- Final Remarks and Recommendations
- Overall IT Infrastructure Review
- Suggested Improvements for IT Security and Operations

### **List of Abbreviations and Full Forms**

AWS - Amazon Web Services

IaaS - Infrastructure as a Service  
PaaS - Platform as a Service  
SaaS - Software as a Service  
GDPR - General Data Protection Regulation  
PCI DSS - Payment Card Industry Data Security Standard  
ATM - Automated Teller Machine  
CBS - Core Banking System  
RBI - Reserve Bank of India  
NEFT - National Electronic Funds Transfer  
RTGS - Real-Time Gross Settlement  
NPCI - National Payments Corporation of India  
MFA - Multi-Factor Authentication  
UPS - Uninterruptible Power Supply  
AML - Anti-Money Laundering  
KYC - Know Your Customer  
DR - Disaster Recovery  
DC - Data Center  
AMC - Annual Maintenance Contract  
SLA - Service Level Agreement  
DPA - Data Processing Agreement  
NDA - Non-Disclosure Agreement  
SOW - Statement of Work

### **Information Technology (IT) Policy**

An Information Technology (IT) Policy of a society is a structured document that outlines the rules and guidelines for the secure and efficient use of the society's IT resources. It is designed to protect the society's data and systems while ensuring compliance with legal, regulatory, and operational standards. The IT policy typically

comprises the following components:

- **Data Security and Privacy:** Guidelines on protecting sensitive customer and financial data, including encryption, data access controls, and privacy compliance (e.g., GDPR, PCI DSS).
- **Access Control:** Rules for user authentication, authorization, and management of access levels to ensure only authorized personnel can access critical systems.
- **Cyber security Measures:** Policies on threat detection, incident response, firewall configurations, antivirus protections, and regular security audits.
- **Software and Hardware Management:** Procedures for the procurement, use, maintenance, and updating of IT assets, including software licenses and hardware systems.
- **Disaster Recovery and Business Continuity:** Protocols for ensuring the society's operations can quickly recover from incidents like system failures or cyber attacks.
- **Compliance and Legal Obligations:** Guidelines to ensure adherence to national and international regulations regarding data protection, anti-money laundering (AML), and financial transactions.
- **Monitoring and Auditing:** Procedures for regular monitoring, logging, and auditing of system activity to ensure security and compliance.

The IT policy serves as a blueprint for safeguarding technology and data while supporting efficient credit operations.

### **1. Agreement with a Software Vendor**

When entering into an agreement with a software vendor and a society, comprehensive documentation is essential to ensure that all terms, obligations, and expectations are clearly defined and agreed upon. Here are the typical requirements and best practices for documentation and agreements with both software vendors and societies:

Key Documentation:

- **Master Services Agreement (MSA):** Outlines the overall terms of the partnership, including general terms of service, intellectual property rights, liability, confidentiality, termination clauses, and dispute resolution.
- **Service Level Agreement (SLA):** Defines the level of service expected, including performance metrics, uptime guarantees, response times for support, and remedies if service levels are not met.

- **Statement of Work (SOW):** Details specific deliverables, timelines, and responsibilities for individual projects or tasks.
- **Software License Agreement:** Specifies the terms of software usage, including user limits, restrictions on usage, licensing fees, and compliance requirements.
- **Data Processing Agreement (DPA):** Required if the software vendor processes personal data on your behalf, detailing data protection measures, compliance with privacy laws (e.g., GDPR), and responsibilities regarding data breaches.
- **Non-Disclosure Agreement (NDA):** Protects sensitive information shared between parties during negotiations or ongoing engagements.
- **Payment Terms and Invoicing:** Outlines how and when payments will be made, including penalties for late payments and acceptable methods of payment.
- **Maintenance and Support Agreement:** Specifies ongoing support services, including bug fixes, software updates, and customer support channels.

### **Important Clauses:**

- **Intellectual Property Rights:** Define ownership of developed software, modifications, and customizations.
- **Warranty and Liability:** Details of warranties provided by the vendor and limitations of liability in case of software failures.
- **Termination and Exit Strategy:** Include conditions under which the agreement can be terminated and procedures for transitioning services, including data handover.

## **2. Agreement with a Society**

### Key Documentation:

- **Master Services Agreement:** Defines the range of services provided, such as cash management, payment processing, loan services, and account management.
- **Service Level Agreement (SLA):** Details the society's obligations regarding transaction processing times, account access, and customer support responsiveness.
- **Security and Compliance Agreement:** Specifies the security measures and compliance requirements the society must adhere to, particularly concerning financial regulations, anti-money laundering (AML), and know your customer (KYC) protocols.
- **Fee Schedule:** Outlines all costs associated with the services, including

transaction fees, service charges, and penalties for overdrafts or non-compliance.

- **Confidentiality Agreement:** Ensures that both parties will keep sensitive information secure, particularly regarding account details, transaction history, and personal data.
- **Data Protection Agreement:** Details how the society handles and protects client data, especially if personal or sensitive information is involved.
- **Risk Management and Fraud Prevention Clauses:** Define the procedures for monitoring transactions, detecting fraud, and managing financial risks.
- **Dispute Resolution Mechanism:** Establishes how disputes will be handled, including mediation, arbitration, or legal proceedings.

### **Important Clauses:**

- **Account Access and Control:** Clarifies who has access to the accounts, including authorization levels and procedures for adding or removing access.
- **Indemnification and Liability:** Specifies the society's liability in cases of errors, fraud, or breaches and the indemnity provisions to protect both parties.
- **Termination Conditions:** Outlines how either party can terminate the agreement and the consequences of termination, including account closures and the transfer of funds.

### **General Best Practices:**

- **Legal Review:** Have legal counsel review all agreements to ensure compliance with applicable laws and regulations.
- **Clear Definitions:** Define all key terms clearly to avoid ambiguity and potential disputes.
- **Documentation Management:** Keep all agreements, amendments, and related documentation well-organized and accessible for future reference.
- **Regular Updates:** Periodically review and update agreements to reflect changes in services, regulations, or business needs.

These documents ensure transparency, protect both parties' interests, and help manage risks associated with the software and financial services involved.

## **Core Banking / Cloud Banking and Client-Server Protocols in Credit Cooperatives**

## **Core Banking by using Client-Server Protocol**

- **Definition:**
- Core Banking refers to the centralized system used by society to manage its core functions, such as account management, transaction processing, and customer data management. It is the backbone of a society's operations.
  
- **Infrastructure:**
- Traditionally, core banking systems are hosted on physical servers and data centers owned by the society or its technology partners.
- **Features:**
- **Centralized Data:** Core banking systems ensure that data is consistent across all branches and channels.
- **Real-Time Transactions:** Supports real-time processing of transactions and updates.
- **Integration:** Connects various functions like loans, deposits, and account management.
- **Security:** Usually involves robust security measures to protect sensitive financial data.
- **Scalability and Maintenance:**
- Scaling up may involve significant investment in hardware and infrastructure.
- Maintenance and upgrades are managed internally or through third-party vendors, requiring dedicated IT resources.

## **Cloud Banking technology in Credit Cooperatives**

- **Definition:**
- Cloud banking refers to the use of cloud computing technologies to deliver banking services and manage operations. It can encompass various aspects of banking, including core banking functions, but utilizes cloud-based infrastructure.
- **Infrastructure:**
- Cloud banking relies on remote servers and storage provided by cloud service providers (e.g., AWS, Azure, Google Cloud). The society accesses these resources over the internet.
- **Features:**
- **Flexibility and Scalability:** Easily scalable to handle varying workloads and

customer demands without significant upfront investment.

- **Cost Efficiency:** Reduces costs related to hardware, data centers, and maintenance as the cloud provider manages these resources.
- **Accessibility:** Provides access to banking services from anywhere with an internet connection, enhancing digital and mobile banking capabilities.
- **Disaster Recovery:** Often includes built-in disaster recovery and backup solutions provided by the cloud provider.
- **Security and Compliance:**
  - Cloud banking requires rigorous security measures to protect data in transit and at rest. Society must ensure that their cloud providers comply with relevant regulations and standards.
  - Data privacy and regulatory compliance are managed through agreements and certifications provided by the cloud service provider.

### **Key Differences**

- **Deployment:** Core banking is typically hosted on-premises or in private data centers, while cloud banking uses cloud infrastructure provided by third-party vendors.
- **Scalability:** Cloud banking offers greater scalability and flexibility compared to traditional core banking systems.
- **Cost Structure:** Cloud banking can reduce capital expenditures by shifting to an operational expenditure model, whereas core banking often involves significant upfront investment in hardware and infrastructure.
- **Maintenance:** Cloud banking offloads maintenance and upgrades to the cloud provider, while core banking requires internal or vendor-based maintenance.

In summary, while core banking focuses on the central systems that manage banking operations, cloud banking leverages cloud technology to deliver and manage these services more flexibly and cost-effectively.

### **Cloud Provider**

A cloud provider is a company that offers cloud computing services, enabling organizations to store, manage, and process data over the internet rather than relying on local servers or hardware. These services typically include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), catering to a wide range of IT needs. Leading cloud providers, such as Amazon Web



Services (AWS), Microsoft Azure, and Google Cloud, provide scalable and flexible resources that can be accessed on-demand. By leveraging cloud providers, businesses can reduce IT costs, enhance operational efficiency, and easily scale their infrastructure as needed. Overall, cloud providers play a crucial role in facilitating digital transformation and supporting modern business operations.

### **Data Storage**

Data storage in cloud computing refers to the practice of storing digital information on remote servers managed by cloud service providers, rather than on local physical devices. This approach allows users and organizations to access their data from anywhere with an internet connection, offering greater flexibility and convenience. Cloud storage solutions typically provide scalability, enabling users to easily increase or decrease their storage capacity as needed. Security measures, such as encryption and access controls, are implemented to protect sensitive data stored in the cloud. Overall, cloud data storage enhances collaboration, reduces costs associated with physical storage, and simplifies data management.

### **Data Backup**

Data backup is the process of copying and storing data to ensure its availability in case of data loss, corruption, or system failure. Backups create a duplicate of important files, databases, or entire systems, which can be restored if the original data is compromised. Regular data backups are essential for business continuity, protecting against threats like hardware failure, accidental deletion, or cyber attacks such as ransom ware. In cloud computing, backups are often automated and stored on remote servers, providing an additional layer of security and convenience. Effective data backup strategies include full, incremental, or differential backups to optimize storage and recovery times.

### **Data Security**

Data security involves the protection of digital data from unauthorized access, corruption, or theft throughout its lifecycle. It includes measures like encryption, access control, and authentication to safeguard sensitive information from breaches, cyber attacks, and internal threats. Data security is critical for maintaining privacy, ensuring compliance with regulations (e.g., GDPR: General Data Protection Regulation), and protecting intellectual property. In cloud computing, data security

extends to securing data both at rest and in transit through advanced encryption and secure access protocols. Effective data security strategies help mitigate risks, ensuring business continuity and trust in digital systems.

### **Access Control**

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It ensures that only authorized individuals or systems have the ability to access sensitive data or perform specific actions. There are various types of access control, such as role-based access control (RBAC), where permissions are assigned based on a user's role, and multi-factor authentication (MFA), which adds layers of security. In cloud computing, access control is crucial for safeguarding data, applications, and networks from unauthorized access. Properly implemented access control helps prevent data breaches, ensuring compliance and protecting system integrity.

### **Disaster Recovery**

Disaster recovery (DR) is the process of restoring critical IT systems and data after a disaster, such as a cyber attack, hardware failure, or natural disaster. It involves a predefined plan that enables businesses to recover quickly and minimize downtime, ensuring continuity of operations. DR typically includes data backups, failover systems, and cloud-based solutions to restore functionality. In cloud computing, disaster recovery is often more efficient and cost-effective, as cloud providers offer automated backup and recovery services. A well-designed disaster recovery plan helps organizations mitigate risks, protect sensitive data, and reduce financial losses.

### **DC/DR DRILL**

A DC/DR drill (Data Center/Disaster Recovery drill) is a simulated exercise designed to test an organization's ability to recover from a disaster and restore critical IT systems. It involves replicating a disaster scenario, such as a data center outage or cyber attack, to evaluate the effectiveness of the disaster recovery plan. The drill measures response times, team coordination, and the functionality of backup systems and procedures. Regularly conducting DC/DR drills helps identify weaknesses and ensures readiness for real-world disruptions. Ultimately, these drills are vital for minimizing downtime and ensuring business continuity. Societies typically conduct DC/DR drills at least once or twice a year to ensure that their disaster recovery plans are effective and up to date.

### **Uptime and Availability**

Uptime refers to the amount of time a system, service, or network is operational and accessible to users, while availability is the measure of how consistently a system performs as expected over a specific period. High uptime is crucial for businesses, especially in credit cooperatives, where uninterrupted access to services like online credit/non credit services, ATMs, and payment systems is essential. Availability is often defined in Service Level Agreements (SLA), with many providers offering 99.9% or higher uptime guarantees, commonly known as "three nines" or "four nines" availability. Cloud providers and IT teams implement redundancy, failover mechanisms, and backups to ensure maximum uptime. Achieving high availability ~~minimizes downtime, ensuring business continuity and customer satisfaction.~~

### **Compliance**

Compliance refers to the adherence to laws, regulations, and industry standards that govern the operations of an organization. In banking and finance, compliance ensures that institutions meet legal requirements related to data protection, financial transparency, anti-money laundering (AML), and Know Your Customer (KYC) regulations. Failure to comply can result in legal penalties, fines, and reputational damage. Organizations must regularly audit their processes and implement compliance frameworks to ensure they meet both local and international regulations. Effective compliance helps maintain trust, security, and operational integrity in a regulated industry.

### **Vendor Lock-In**

Vendor lock-in occurs when a company becomes overly dependent on a single vendor for products or services, making it difficult to switch providers without facing significant costs or disruption. In cloud computing, this can happen when proprietary systems, data formats, or technologies limit the ease of migration to another cloud provider. Vendor lock-in can result in reduced flexibility, higher costs, and reliance on the vendor's terms for future services. To avoid lock-in, businesses often adopt strategies like using open standards, multi-cloud solutions, or negotiating favorable exit clauses. Mitigating vendor lock-in risk is crucial for maintaining control over business operations and future scalability.

### **Scalability**

Scalability refers to a system's ability to handle increased workload or expand its capacity as demand grows, without compromising performance. In cloud computing, scalability allows organizations to adjust resources like storage, processing power, and bandwidth easily, depending on current needs. This is especially beneficial for businesses with fluctuating demand, as they can scale up during peak times and scale down when less capacity is required. Scalability ensures cost-efficiency, as companies only pay for the resources they use. It also supports business growth, ensuring that IT infrastructure can seamlessly expand alongside the organization.

### **Security Monitoring**

Security monitoring involves the continuous observation of an organization's IT environment to detect, analyze, and respond to potential security threats and vulnerabilities. This process utilizes tools and techniques such as intrusion detection systems (IDS), security information and event management (SIEM) solutions, and automated alerts to identify suspicious activities in real-time. Effective security monitoring helps organizations maintain compliance with regulations and standards by ensuring that security policies are enforced consistently. It enables rapid incident response, minimizing the impact of security breaches and protecting sensitive data. By continuously assessing security posture, organizations can proactively address weaknesses and enhance their overall cyber security strategies.

### **Audit Trails**

Audit trails are records that document all activities and transactions within an IT system, providing a comprehensive history of user actions, changes made, and access to sensitive information. These trails are crucial for ensuring accountability and transparency, as they help organizations track who accessed data, when, and what actions were taken. In the context of compliance, audit trails are essential for demonstrating adherence to regulatory requirements and internal policies. They facilitate forensic investigations by providing a detailed account of events leading up to a security incident or data breach. Regularly reviewing and analyzing audit trails helps organizations identify anomalies, enhance security measures, and improve operational processes.

### **Service Support**

Service support refers to the assistance and resources provided to users to ensure the smooth operation and maintenance of IT services and systems. This can include help

desk services, technical support, and troubleshooting for software and hardware issues. Effective service support aims to resolve incidents quickly, minimize downtime, and enhance user satisfaction by addressing queries and concerns promptly. It often involves a structured approach, such as ITIL (Information Technology Infrastructure Library) frameworks, to ensure consistent service delivery and continuous improvement. By maintaining robust service support, organizations can optimize productivity and ensure that users can efficiently utilize IT resources.

### **Data Ownership**

Data ownership refers to the legal and ethical rights that an individual or organization has over their data, including how it is collected, stored, accessed, and utilized. Owners of data are responsible for ensuring its accuracy, security, and compliance with relevant regulations, such as data protection laws. In a business context, data ownership often involves defining who has the authority to make decisions regarding data usage and sharing. Clear data ownership policies help prevent unauthorized access, misuse, and breaches, while also facilitating accountability and governance. Establishing data ownership is essential for maintaining trust and transparency in data management practices.

### **Incident Response**

Incident response refers to the systematic approach an organization takes to prepare for, detect, and manage cyber security incidents or breaches. The process typically involves several phases, including preparation, identification, containment, eradication, recovery, and post-incident analysis. A well-defined incident response plan helps minimize the impact of security incidents, ensuring that critical systems and data are quickly restored to normal operation. Effective incident response also involves communication among stakeholders and documenting the incident for future reference and compliance. By regularly testing and updating their incident response plans, organizations can improve their resilience against cyber threats and enhance overall security posture.

### **Unified Customer Identification Number (UCIN)**

A Unified Customer Identification Number (UCIN) is a unique identifier assigned to a customer by a society to consolidate and manage all of their accounts under one ID. In software, the relevance of UCIN is significant as it facilitates better customer management, enabling society to track and analyze customer activity across multiple touch points. It also enhances the accuracy of KYC (Know Your Customer)

processes, improves risk management, and ensures compliance with regulatory requirements. Additionally, UCIN allows for a more personalized banking experience by enabling targeted product offerings and improved customer support.

### **Role-based access control (RBAC)**

Role-based access control (RBAC) is a security model that restricts system access based on a user's role within an organization. In RBAC, roles are assigned to users according to their job functions, and each role is granted specific permissions to access certain software features, data, or resources. This ensures that users only have access to the information and tools necessary for their duties, reducing the risk of unauthorized access or misuse of sensitive data.

RBAC enhances security by enforcing the principle of least privilege, where users are granted the minimum permissions needed to perform their tasks. It also simplifies access management, as roles can be easily modified or revoked without individually adjusting user permissions. In software, RBAC is critical for safeguarding customer information and ensuring compliance with data protection regulations, while streamlining the management of user access across various systems.

### **The Maker-Checker Policy**

The Maker-Checker Policy is an internal control mechanism designed to enhance the security and integrity of financial transactions. It requires two distinct roles—the "maker," who initiates a transaction, and the "checker," who reviews and approves it. This segregation of duties minimizes the risk of fraud or errors by ensuring that no single individual has complete control over a transaction from initiation to approval.

Once the maker submits a transaction, it cannot be executed until the checker verifies that all details are accurate and compliant with internal policies. The system maintains a record of both the maker and checker for each transaction, creating a reliable audit trail for compliance and accountability. By enforcing dual control, the Maker-Checker Policy helps protect the society from fraudulent activities while ensuring adherence to regulatory requirements. Ultimately, this policy is crucial for maintaining trust and security in its operations.

### **Password policies**

Password policies in a society are crucial security measures designed to protect

sensitive information and prevent unauthorized access to systems and accounts. These policies outline the requirements for creating, maintaining, and managing passwords used by employees and customers.

**Key components of a robust password policy typically include:**

- **Complexity Requirements:** Passwords must include a mix of upper and lower-case letters, numbers, and special characters to enhance security and make them harder to guess.
- **Minimum Length:** Passwords should meet a minimum length requirement, often set at eight characters or more, to increase the difficulty of brute-force attacks.
- **Regular Changes:** Users may be required to change their passwords regularly, such as every 60 to 90 days, to reduce the risk of compromised passwords being used over time.
- **Prohibited Passwords:** The policy may specify certain commonly used or easily guessable passwords (e.g., "123456," "password") that are prohibited from use.
- **Account Lockout Mechanisms:** After a certain number of unsuccessful login attempts, accounts may be temporarily locked to prevent unauthorized access through brute-force attacks.
- **Multi-Factor Authentication (MFA):** The use of MFA is encouraged, where users must provide additional verification (e.g., a one-time code sent to their mobile device) along with their password for enhanced security.
- **Education and Awareness:** Society often provide training and resources to educate employees and customers about the importance of strong passwords and best practices for password management.

**Check whether the password policy is strictly followed by the staff**

To check whether the password policy is strictly followed by the staff in a society, you can follow these steps:

**1. Review System Logs:** Access system logs to review whether passwords are being changed regularly according to the society's password policy (e.g., every 60-90 days). Ensure that the system enforces password expiration and prompts users to update passwords within the required time frame.

**2. Audit User Accounts:** Perform an audit of user accounts to verify that all

passwords meet the society's complexity requirements (e.g., minimum length, inclusion of uppercase letters, numbers, and special characters). Check if the system rejects weak or prohibited passwords.

**3. Check for Multi-Factor Authentication (MFA):** Verify if multi-factor authentication (MFA) is enabled and being used by staff, especially for accessing sensitive systems or data. Confirm that MFA is applied consistently across all staff members.

**4. User Password Change History:** Review password change history for each user to confirm compliance with password update frequency. Ensure that users are not reusing old passwords and that the system enforces a password history to prevent reuse.

**5. Access Control Reports:** Check access control reports to identify any instances of unauthorized access or potential breaches that may indicate weak or shared passwords.

**6. Staff Interviews:** Conduct interviews or surveys with staff to ensure they understand the password policy and follow best practices for password management (e.g., not sharing passwords, creating strong passwords).

**7. Enforcement of Lockout Mechanisms:** Verify if lockout mechanisms are in place after a defined number of failed login attempts. Check whether users who are locked out follow the correct procedures to reset their passwords securely.

**8. Policy Compliance Audits:** Conduct random compliance audits to ensure that password policies are enforced at the system level and adhered to by the staff. Review the compliance rate and identify any policy violations.

**9. Use of Password Managers:** Check whether the branch is using approved password management tools (if applicable) and if staffs are properly utilizing these tools to store and manage complex passwords.

### **Exceptional Reports obtained from the Core Banking System (CBS)**

Exceptional Reports obtained from the Core Banking System (CBS) are critical tools used to highlight transactions or activities that deviate from predefined norms or expected patterns. These reports help in identifying unusual, suspicious, or potentially



fraudulent activities within the banking system.

### **Key Aspects of Exceptional Reports:**

- **Unusual Transactions:** The report flags transactions that exceed normal thresholds, such as large withdrawals, deposits, or transfers that are significantly higher than typical customer activity.
- **Failed Transactions:** Lists transactions that were attempted but failed due to issues like insufficient funds, incorrect account details, or system errors.
- **Unauthorized Access Attempts:** Identifies any unauthorized or suspicious login attempts, especially those outside normal working hours or from unusual locations.
- **High-Risk Activities:** Highlights activities like multiple accounts being opened within a short time, unusual cross-border transactions, or sudden spikes in account activity.
- **Account Irregularities:** Alerts management to accounts that exhibit irregular patterns, such as dormant accounts with sudden high-volume activity.

Exceptional Reports provide vital insights for risk management, fraud detection, and ensuring compliance with internal controls and regulatory standards. They enable timely investigation and corrective actions to maintain the integrity of banking operations.

### **If the society is using ATM**

#### ATM

An Automated Teller Machine (ATM) is an electronic banking device that allows customers to perform basic financial transactions such as cash withdrawals, balance inquiries, fund transfers, and deposits without the need for a human teller. ATMs are connected to the society's core systems and can operate 24/7, providing convenience for users.

Critical Matters to be Checked Regarding ATMs:

- **Physical Security:**

- Ensure the ATM is placed in a secure location with surveillance cameras and proper lighting.
- Verify that anti-skimming devices are installed to prevent card data theft.
- Check that the ATM housing is tamper-resistant and that physical locks are secure.

- **Software and Connectivity:**

- Confirm that the ATM's software is up to date and has the latest security patches to prevent cyber attacks.
- Ensure that the ATM is connected to the core banking system and that real-time transaction processing is functioning properly.

- **Transaction Integrity:**

- Verify that transaction logs are maintained accurately for all activities, including withdrawals, deposits, and transfers.
- Check that customer receipts accurately reflect the transactions performed, and any discrepancies are flagged.

- **Cash Management:**

- Review cash replenishment procedures to ensure that cash levels are monitored, and that the ATM is regularly stocked to meet demand.
- Conduct regular audits of cash levels and reconciliations to prevent discrepancies or theft.

- **Disaster Recovery and Backup:**

- Ensure that there are backup power systems (e.g., UPS) to maintain ATM functionality during power outages.
- Verify that the society has a disaster recovery plan in case of system failures or network issues.

- **Compliance and Security Standards:**

- Check that the ATM complies with PCI DSS (Payment Card Industry Data Security Standard) requirements.
- Ensure that the ATM is equipped with encryption protocols to protect customer data during transactions.

- **User Interface and Accessibility:**

- Confirm that the ATM is user-friendly, with clear instructions and intuitive functionality.
- Ensure that accessibility features, such as braille keypads or audio assistance, are available for customers with disabilities.

- **Maintenance and Servicing:**

- Ensure regular maintenance checks are performed to prevent hardware failures or technical issues.
- Monitor error rates and downtime to address any recurring problems with the machine.

- **Fraud Detection:**

- Check for alerts on fraudulent activities, such as card skimming or account tampering, and ensure the ATM's fraud detection systems are functioning effectively.
- Verify that any fraudulent transactions are flagged for immediate investigation.

Regularly auditing and checking these critical areas ensures that ATMs function reliably, securely, and in compliance with banking and regulatory standards.

### **NEFT/RTGS**

Integrating NEFT/RTGS services in co-operative society with nationalized bank involves several key steps. First, the co-operative society needs to become a member of the RBI's payment systems, which often requires partnering with a sponsor bank—usually a nationalized banks—that can route transactions on the banks's behalf through NEFT/RTGS networks. The co-operative society must upgrade its Core Banking System (CBS) to ensure compatibility with NEFT/RTGS modules and the National Payments Corporation of India (NPCI) platform, which manages these services.

The society must also implement robust security protocols, including data encryption, multi-factor authentication, and firewalls, to protect transactions and ensure regulatory compliance. After integrating the NEFT/RTGS modules into the CBS, the system undergoes thorough testing with dummy transactions to verify functionality. The society must then obtain approvals from both the RBI and NPCI before going live.

### **Staff training**

Staff training is essential to familiarize employees with the NEFT/RTGS process, and customer education is required to inform them about using these services. Once live, the society must monitor transactions closely, using real-time alerts to detect fraud and ensure smooth operations. Regular compliance reporting to RBI and NPCI is critical to maintain regulatory standards and operational efficiency, enabling co-

operative society to offer national-level fund transfer services.

### **Key Third-Party Software Requirements:**

To integrate NEFT/RTGS services into a co-operative society's Core Banking System (CBS), specific third-party software is required to ensure smooth operation, security, and compliance.

Payment gateway or transaction processing software is essential for securely routing NEFT/RTGS transactions between the bank, sponsor bank, and NPCI/RBI. Encryption tools like SSL certificates and VPNs safeguard sensitive data, while fraud detection software monitors transactions for suspicious activity. CBS integration modules, offered by third-party providers, help seamlessly connect NEFT/RTGS functionality with the existing CBS infrastructure.

For enhanced security, multi-factor authentication (MFA) tools are needed to protect user access, especially for high-value transactions. Compliance reporting software assists in meeting RBI regulatory requirements and generating necessary reports. Finally, reliable network solutions ensure stable connectivity between the society and the NEFT/RTGS network.

These third-party tools help ensure secure, efficient, and compliant integration of NEFT/RTGS services in a co-operative society.

### **Firewall**

A firewall is a critical component of a society's network security infrastructure, serving as the first line of defense against cyber threats. Its primary function is to monitor and control incoming and outgoing network traffic based on predefined security rules. In a financial environment, where sensitive customer data and financial transactions are handled, firewalls play a vital role in protecting against unauthorized access, malware, and cyber attacks.

### **Importance of Firewalls in Society:**

- **Data Protection:** Firewalls prevent unauthorized access to confidential customer data, safeguarding sensitive information from cybercriminals.
- **Network Segmentation:** They help in segmenting the society's internal network, ensuring that different departments and systems are isolated, which reduces the risk of lateral movement in case of a breach.
- **Compliance:** Firewalls help society comply with regulatory requirements such as PCI DSS and RBI guidelines, ensuring secure data transmission.
- **Threat Detection:** Firewalls can detect and block malicious traffic, preventing

attacks such as DDoS, phishing, or ransomware.

- **Access Control:** They control access to the society's network, ensuring only authorized users and systems can communicate, protecting critical systems from external threats.

In essence, firewalls are essential for maintaining the integrity, confidentiality, and availability of banking operations.

### **Load balancer**

A load balancer is a critical component in network architecture that distributes incoming traffic across multiple servers to ensure optimal resource utilization, improve application responsiveness, and enhance overall system reliability. By balancing the load, it prevents any single server from becoming overwhelmed with too much traffic, which can lead to performance degradation or downtime.

Key Functions of a Load Balancer:

- **Traffic Distribution:** Load balancers use various algorithms (such as round-robin, least connections, or IP hash) to intelligently route requests to different servers based on their current load and capacity.
- **High Availability:** By distributing traffic across multiple servers, load balancers ensure that if one server fails, traffic can be rerouted to operational servers, thus maintaining service availability.
- **Scalability:** Load balancers facilitate horizontal scaling by allowing additional servers to be added to the pool without disrupting service. This capability helps accommodate increased traffic loads efficiently.
- **Health Monitoring:** Load balancers regularly check the health of servers in the pool and only route traffic to those that are functioning properly, ensuring reliability and performance.
- **SSL Termination:** Many load balancers can offload SSL decryption tasks from backend servers, reducing their computational burden and improving overall performance.

### **Importance in Financial/Credit Services:**

In financial/credit services, load balancers are essential for handling high volumes of transactions and ensuring that online services, such as internet banking and payment processing, remain available and responsive at all times. By improving performance and reliability, load balancers play a crucial role in enhancing customer experience

and maintaining operational efficiency.

### **Main Threats &frauds**

In a computerized banking environment, several threats and types of fraud can compromise the security of financial systems and customer data. Here are some of the main threats and frauds:

#### **Main Threats**

- **Malware Attacks:** Malicious software such as viruses, worms, and ransomware can infect banking systems, leading to data breaches, system downtime, and financial loss.
- **Phishing Attacks:** Cybercriminals use deceptive emails or messages to trick customers into providing sensitive information, such as login credentials or credit card numbers.
- **Denial of Service (DoS) Attacks:** Attackers overwhelm banking servers with traffic, causing service outages and preventing legitimate users from accessing banking services.
- **Data Breaches:** Unauthorized access to banking systems can lead to the theft of sensitive customer information, including personal identification and financial data.
- **Insider Threats:** Employees with access to sensitive systems may intentionally or unintentionally compromise security, leading to data leaks or fraud.
- **Credential Stuffing:** Attackers use stolen usernames and passwords from one breach to gain access to accounts on other platforms, exploiting users who reuse credentials.
- **Man-in-the-Middle (MitM) Attacks:** Attackers intercept communications between customers and society, allowing them to steal sensitive information or manipulate transactions.
- **Social Engineering:** Manipulating individuals into divulging confidential information or performing actions that compromise security, often through impersonation or deception.

#### **Types of Fraud**

Account Takeover Fraud: Cybercriminals gain unauthorized access to customer

accounts, often using stolen credentials, and perform fraudulent transactions.

- **Credit Card Fraud:** Fraudsters use stolen credit card information to make unauthorized purchases or withdraw funds.
- **Loan Fraud:** Individuals may submit false information to obtain loans or credit, resulting in financial loss for the society.
- **Cheque Fraud:** This includes alterations to cheques, forgery, or using counterfeit cheques to withdraw funds illegally.
- **Wire Transfer Fraud:** Fraudsters trick individuals or businesses into transferring funds to accounts controlled by the criminals, often using phishing or social engineering tactics.
- **Identity Theft:** Criminals steal personal information to impersonate individuals and access their society accounts or open new accounts in their names.
- **Mobile Banking Fraud:** Exploiting vulnerabilities in mobile banking applications or using phishing tactics to gain access to users' mobile banking credentials.
- **Crypto currency Fraud:** Scams involving fake initial coin offerings (ICOs), Ponzi schemes, or fraudulent exchanges targeting users interested in crypto currency investments.

### **Mitigation Strategies**

To combat these threats and frauds, society should implement robust security measures, including:

- Multi-factor authentication (MFA)
- Regular security audits and vulnerability assessments
- Employee training on security awareness and phishing detection
- Advanced threat detection systems and fraud monitoring tools
- Encryption of sensitive data in transit and at rest
- Incident response plans to address breaches and fraud attempts promptly

By understanding these threats and implementing effective security measures, society can better protect their systems and customers from fraud and cyber attacks.