CHAPTER 6

FINDINGS

AND

SUGGESTIONS
CHAPTER 6
FINDINGS AND SUGGESTIONS

6.1 Introduction
This chapter summarises the research work carried out by the researcher on the topic “Information security systems in CORE banking environment of urban cooperative banks of Pune and Mumbai cities”. The findings summarised in this chapter is outcome of what has been attempted in earlier chapters. The findings are drawn from 18 urban cooperative banks with core banking solution deployed. The researcher based on the collected primary data, the findings and conclusions are drawn. Based on the findings and conceptual theory and earlier work in this area, the researcher has proposed conceptual layer framework for information security in CBS solution environment of UCBs. The researcher has further suggested the direction on research leads and future trends.

6.2 Findings and Conclusions
In this section the researcher has made an attempt to list out findings and conclusions based on the objectives of the study. In this study the researcher focused on five objectives as mentioned chapter 3. These objectives focuses on

- Escrow agreement
- Budget provision
- Objectives for CBS implementation
- CBS solution age of implementation
- Information security standards
- Information security domains
- Internet banking security
- ATM security
- Training and awareness program
- Awareness level of end users regarding information security
- Different types of cyber attacks experienced in CBS environment

The researcher has presented these findings into four parts.
Part I: Present findings and conclusions regarding the perception of IT heads and banks managements regarding present overall information security systems status of urban cooperative banks (UCB) in CBS environment

Part II: Present the findings and conclusion regarding the perception of IT heads regarding applicability of information security standards in CBS solution environment.

Part III: Perception of employees (end users) regarding awareness level of the about information security.

Part IV: Findings and conclusion regarding the perception of employees (end users) regarding training and awareness program on information security.

6.2.1 Part I: Perception of IT heads and banks management regarding present overall information security systems status of urban cooperative banks (UCBs) in CBS solution environment

The main objective of this research work is to evaluate information security system of CBS solution environment of urban cooperative banks of Pune and Mumbai cities. The study is carried out to understand present status of overall information security systems of urban cooperative banks (UCBs). This study also aims to evaluate different domains of information security such as:

1. CSB environment
2. Escrow agreement
3. Information security policy, procedure
4. Physical and environmental security
5. Assets management
6. Human resources security
7. Access control
8. Network security
9. Cryptographic controls
10. Data security
11. Business continuity management
12. Information security policy domains
13. Periodic penetration testing
14. Virus protection
15. ATM security
16. Internet banking security
17. Types of cyber attack experienced by UCB’s
18. Regulatory compliance
1. CBS environment

- It has been found that out of the total 18 urban cooperative banks under the study, 12 UCB’s are using fully developed and customized CBS solution which comes to 66.67 percent of total sample. [Ref. Table No. 5.13]

- It is observed that out of total 18 UCB’s under the study, 16 UCB’s have outsourced the CBS solution wherein only 2 UCB’s have In-house developed product solution and in-house IT wings to take care of development and maintenance of the systems [Ref. Table No. 5.14]

- It has been observed that out of total sample under the study i.e.100 percent, 88.89 percent UCB’s CBS solution is based on windows operating system, while 11.11 percent UCB’s have used Linux as an operating system for CBS solution. [Ref. Table No. 5.15]

- It has been observed that out of total 18 urban cooperative banks under the study, 7 UCB’s CBS solution is in place which is about three years old and 6 UCB’s CBS solution is in place for more than three years and less than six years old. Furthermore 2 UCBs solution is more than nine years old and 3 UCBs CBS solution is more than six years and less than nine years old. [Ref. Table No. 5.8]

- It is found that out of the total 18 urban cooperative banks under the study, 3 UCBs have no budget provision for up-gradation of IT infrastructure for CBS solution environment. [Ref. Table No. 5.9]

- It is found that out of the total 18 urban cooperative banks under the study, majority of UCBs i.e. 94.4% agreed with that the implementation of CBS solution improves MIS and standardization of process, improves operational efficiency, better compliance with all regulatory requirements in operations and reporting, increased in business volume, availability of accurate data whenever required, improve profitability of banks and offer wider, more flexible product portfolio to the customers. [Ref. Table No. 5.7]

Conclusion

CBS solution is six years old in the large sized urban cooperative banks. Therefore it may be concluded that urban cooperative banks are young in implementation of CBS solution environment. Many of the UCBs have outsourced their CBS solution software which may have resulted in increased risk to confidentiality of data and also
increases long term maintenance cost. The UCBs have very little control on what happens inside of the system, when the CBS solution is outsourced.

2. Escrow agreement
It was found that, out of the total urban cooperative banks under study, 83.33 percent stated that they do not have escrow agreement in place for access to source code of CBS solution software [Ref Table No. 5.20]

Conclusion
It is concluded from the data analysis that majority of the UCBs i.e. 83.33 percent do not have escrow agreement for source code access. The Escrow agreement may be very useful for urban cooperative banks since the CBS software is very expensive and very important to maintain and is used for longer period. In case of vendor of customized CBS software is unable to provide support for business continuity and maintenance; it increases the risk of banking operations of UCBs. This risk may be minimized if banks have in place escrow agreement for source code access.

3. Information security policy and procedure
It is found that out of total 18 urban cooperative banks under the study; only 6 urban cooperative banks i.e. 33.33 percent have information security policy, procedure in place to protect their information and information systems. From the data analysis it was found that there are 12 urban cooperative banks i.e.66.67 percent do not have information security policy, procedure in place. [Ref. Table No. 5.21]

Conclusion
The international standards reveals that information security policy framework is very first step for implementation of information security program which provide management direction and support for information security. From the data analysis it has been observed that majority of the urban cooperative banks under the study do not have information security policy framework for the management of security across the banks. The lack of a documented information security policy is a message that management of the urban cooperative banks has not taken data security seriously.
4. Physical and environmental security

- It is found that out of total urban cooperative banks (100 percent) under the study, 55.56 percent urban cooperative banks have deployed electronic access controls (access cards/Swipe-card) to restrict access to sensitive area. [Ref. Table No. 5.25]

- It is observed that out of total urban cooperative banks under the study, 77.78 percent urban cooperative banks have installed biometric system to restrict the access to sensitive area and 83.34 percent urban cooperative banks have appointed security guards to protect people, property and prevent crime. [Ref. Table No. 5.25]

- Perimeter wall acts as the outermost layer of security. It has been observed that out of total urban cooperative banks under the study 55.56 percent urban cooperative banks do not have perimeter wall to prevent, or at least delay, attacks. [Ref. Table No. 5.25]

- Banking and finance operations requires a very high level video surveillance solution, with the ability to protect highly secure areas through to recording individual transactions in retail banking operations. To provide safe operation of ATM networks, tackling ATM fraud and branch security CCTV cameras need to be installed by the banks. It was found that out of total urban cooperative banks under the study 50 percent urban cooperative banks have not ensured such CCTV monitoring system. [Ref. Table No. 5.25]

- To handle smart attack attempts, an even smarter security mechanism is needed, which will proactively and intelligently keep an eagle’s eye on the network, and monitor and report incidents quickly. IDSs or IPSs (Intrusion Detection System/Intrusion Prevention System) are the solutions that include these requirements. It was found that out of total urban cooperative banks under the study 55.56 percent urban cooperative banks have not ensured the installation of Intruder Detection System to detect the network attacks. [Ref. Table No. 5.25]

- Additionally, it was observed that out of total urban cooperative banks under the study, 61.11 percent urban cooperative banks installed security locks to restrict access to the sensitive area like server rooms. [Ref. Table No. 5.25]

- It is also observed that out of total urban cooperative banks under the study 61.11 percent urban cooperative banks don’t even implemented basic security
requirement such as registration process for visitor, visitor pass and log book to monitor and recover from incident. [Ref. Table No. 5.25]

- The statistical findings revealed that out of total UCBs under the study, majority of the banks i.e. 94.44% UCBs have adequate procedure to take care of natural disaster like fire, earthquake, and flood, While 5.56% of the banks do not ensured environmental risk.[Ref. Table No. 5.24]

- It is also observed that out of total urban cooperative banks under the study, 72.22% the UCBs stated that physical access controls is ensure to overcome the risk of manmade disasters like theft of information. Furthermore a similar percentage supported for controls such as power cabling and telecommunication cabling laid down with appropriate distance and support like feed power supply, UPS, generator backup are in place. [Ref. Table No. 5.24]

- In addition, it is also observed that out of total urban cooperative banks under the study,88.89% UCBs stated access to sensitive area such as server room, data center; UPS room, backup server room etc. are restricted.[Ref. Table No. 5.24]

Conclusion

It is concluded from the statistical findings that out of total urban cooperative banks under the study majority of urban cooperative banks haven’t recognized the importance of physical and environmental security control in order to minimize environmental and physical risk in CBS solution environment. Therefore, it is concluded from the above findings that physical and environmental security controls are inadequate in CBS solution environment of urban cooperative banks.

5. Assets Management

- It was found that all i.e. 100 percent urban cooperative banks under the study have fully up-to-date, accurate and complete inventory of information assets (computer and communications hardware/systems, application software’s, data & printed information) as per prescribed standards. It is also observed that urban cooperative banks staffs are aware of the corresponding security requirements for handling sensitive resources. [Ref. Table No. 5.27]

- From the statistical data it was found that out of total urban cooperative banks under the study majority of urban cooperative banks i.e. 89.79 percent have
established registration process for new application system, hardware etc. [Ref. Table No. 5.27]

- It was also found that out of total urban cooperative banks under the study, majority of urban cooperative banks i.e. 83.33 percent have power and data cables clearly labeled and wiring diagrams are kept complete and up-to-date, while very few urban cooperative banks i.e. 16.67 percent have not follows such procedure. [Ref. Table No. 5.27]

- It was also observed that out of total urban cooperative banks under the study, majority of the urban cooperative banks i.e.94.45 percent follows appropriate marking scheme on documents, forms, reports, screens, backup media, file transfers etc., while only 5.56 percent urban cooperative banks do not have such marking scheme for documents, forms, reports and backup media etc. [Ref. Table No. 5.27]

- It was also found that out of total urban cooperative banks under the study 61.1 percent urban cooperative banks have maintained detailed inventory of information assets as per ISO standards. [Ref. Table No. 5.28]

**Conclusion**

One of the key success factors in analyzing and measuring the effectiveness of information security is to ensure a thorough understanding of the assets which are most valuable. Asset management is a set of business processes designed to manage the lifecycle and inventory of technology assets. The urban cooperative banks that develop and maintain an effective IT asset management program reduces the risks of information security. From the statistical findings it was concluded that out of total urban cooperative banks under the study, majority of the urban cooperative banks understands the importance of assets management and have implemented proper and predefined asset management procedure and standards for maintaining an accurate inventory, licensing information, and protection of hardware and software asset to reduce IT cost, risk and improving productivity.

**6. Human Resources Security**

- From the statistical data it was found that out of total urban cooperative banks under the study77.80 percent urban cooperative banks have defined roles and
responsibilities of personnel. Whereas 22 percent urban cooperative banks have not defined roles and responsibilities of personnel. [Ref. Table No. 5.29]

- The statistical finding shows that out of the total urban cooperative banks under the study 72 percent urban cooperative banks have maintained the documentation for roles and responsibility of personnel. [Ref. Table No. 5.30]

- It was found that all the urban cooperative banks under the study i.e. 100 percent follow the screening process for staff/managers for sensitive roles. [Ref. Table No. 5.31]

- It was observed that out of total urban cooperative banks under the study, 72.30 percent urban cooperative banks have appropriate HR policies and procedures in place e.g. disciplinary actions for staff and contractors that violate the IT security rules. [Ref. Table No. 5.31]

- It was observed from statistical analysis that out of total urban cooperative banks under the study 66.70 percent urban cooperative banks have appropriate policies, procedure and standards for termination or change of employment. Similar percentage was supported for review of policies, standards, procedures and guidelines relating to information security elements of the termination process e.g. retrieving information assets (papers, data, and systems), keys, removal of access rights etc. [Ref. Table No. 5.31]

Conclusion

It is concluded from statistical findings that out of total urban cooperative banks under the study several of the UCBs have made significant improvement in human resource security but still there is gap that some of the urban cooperative banks are lagging in implementing the human resource security control.

7. Access control

- It was found that out of total urban cooperative banks under the study, all the urban cooperative banks i.e. 100 percent stated that they have implemented successfully unique login ID and passwords on end user’s computers for authorized access to information and information system. A similar percentage is supported for access control policy that addresses the rules and rights for each user or a group of users [Ref. Table No. 5.32]
- It has been also observed that out of total urban cooperative banks under the study 94.40 percent urban cooperative banks followed the segregation of duties to avoid the conflict and minimize the fraud. [Ref. Table No. 5.32]

- It has been revealed from the statistical data that out of total urban cooperative banks under the study 83.3 percent urban cooperative banks have defined business requirements for logical access control security. [Ref. Table No. 5.32]

- It has been found that out of total urban cooperative banks under the study 83.30 percent urban cooperative banks stated that they creates user ID created based on roles and responsibilities, while 16.7 percent urban cooperative banks stated that they do not implement such security control measure in CBS solution environment. [Ref. Table No. 5.33]

- It has been also observed that out of total urban cooperative banks under the study all the urban cooperative banks i.e. 100 percent provide individual password for accountability. [Ref. Table No. 5.34]

- It has been found that out of total urban cooperative banks under the study all the urban cooperative banks i.e.100 percent stated that password is changed on regular basis to avoid unauthorized access to information system. [Ref. Table No.5.34]

- It was found that out of total urban cooperative banks under the study all the urban cooperative banks i.e. 100 percent stated that they have stored the passwords in encrypted form and password is not displayed on screen. [Ref. Table No.5.34]

- It has been found that out of total urban cooperative banks under the study, 94.50 percent urban cooperative banks indicated that access to operating system was controlled by secure log-on procedure. [Ref. Table No.5.35]

- It was observed from the statistical analysis that out of total urban cooperative banks under the study all the 18 urban cooperative banks i.e. 100 percent stated that system logout and screen logout facility is activated. [Ref. Table No.5.35]

- It was found that out of total urban cooperative banks under the study 88.90 percent urban cooperative banks indicated that inactive terminals are shut down/log off automatically after a defined period of inactivity. [Ref. Table No.5.35]
It has been found that out of total urban cooperative banks under the study 94.50 percent urban cooperative banks have carried out review of monitoring activity on regular basis. [Ref. Table No.5.35]

It was also found that out of total urban cooperative banks under the study 44.50 percent urban cooperative banks stated that controls are in place to restrict access to program source libraries. [Ref. Table No.5.32]

**Conclusion**

Access control refers to the process of controlling access to systems, networks, and information based on business and security requirements. The objective is to prevent unauthorized disclosure of the information assets. The key components include **Identification, Authentication, and Authorization** which are applied to people, process, and technology devices. From the above findings it has been concluded that out of total UCBs under the study still there are some urban cooperative banks have not implemented required access control measures to safeguard their information and information system. Therefore it is concluded that access control system in some of the UCBs are still in infancy stage.

8. **Network security**

- The statistical findings revealed that out of total urban cooperative banks under the study 77.80 percent urban cooperative banks stated that they have implemented users logging from remote locations are identifiable by terminal IDs / IP addresses. [Ref. Table No. 5.36]
- Out of total urban cooperative banks under the study 66.70 percent urban cooperative banks stated that physical and logical access to diagnostic ports are securely controlled i.e. protected by a security mechanism. [Ref. Table No. 5.36]
- Out of total urban cooperative banks under the study, 66.70 percent urban cooperative banks stated that firewall is in use as per ISO standard. [Ref. Table No. 5.36]
- It has been also observed that out of total urban cooperative banks under the study 90 percent urban cooperative banks stated that all internet connections are routed through a firewall and also maintain a comprehensive list of what should be allowed or disallowed through the firewall. [Ref. Table No. 5.36]
Out of total urban cooperative banks under the study, 50 percent urban cooperative banks stated that they network prevent entry or exit through any network port that is not required by banks. [Ref. Table No. 5.36]

Out of total urban cooperative banks under the study 61.10 percent urban cooperative banks stated that filtering process is in place for email attachment to reduce the risk of systems. [Ref. Table No. 5.36]

It has been also observed that out of total urban cooperative banks under the study 72.2 percent urban cooperative banks stated that remote login is enabled to access the system. [Ref. Table No. 5.37]

It was observed from the statistical data that out of total urban cooperative banks under the study 38.9 percent indicated that they never update the firewall, while 22.2 percent updates the firewall once in month. [Ref. Table No. 5.38]

To evaluate the frequency of automated vulnerability scanning tools for all systems on network the respondents view was recorded. It has been found from the statistical data that out of total urban cooperative banks under the study 55.6 percent urban cooperative banks stated that they have automated vulnerability scanning tools for all systems on network, while 44.40 percent respondents replied that their urban cooperative banks do not have such facility. [Ref. Table No. 5.39]

**Conclusion**

The purpose of network security is essential to prevent loss, through misuse of data. Network security refers to any activities designed to protect network. In particular, these activities protect the usability, reliability, integrity, and safety of UCB’s network and data. Effective network security targets a variety of threats and stops them from entering or spreading on the network. From the above finding it was concluded that out of total urban cooperative banks under the study many of the urban cooperative banks have not implemented network security adequately. Since the network security is not implemented properly there are number of potential pitfalls that may arise in UCB’s network and lead to information loss. Therefore it was concluded that network security of UCB is in infancy stage.
9. Cryptographic Controls

- A cryptographic control is an important tool for protecting information. Cryptography is traditionally associated only with keeping data secret. It has been found that out of total urban cooperative banks under the study 72.2 percent urban cooperative banks stated that cryptography key management is not in place to support the use of cryptographic techniques for the UCBs. [Ref. Table No. 5.40]

- It has been also found that out of total urban cooperative banks under the study 72.2 percent urban cooperative banks recorded that cryptographic keys have not protected against modification, loss, and destruction. [Ref. Table No. 5.40]

- It has been found that out of total urban cooperative banks under the study 72.20 percent urban cooperative banks stated that secret keys and private keys have not protected against unauthorized disclosure and equipments used to generate, store keys have not physically protected. [Ref. Table No. 5.40]

- From the statistical data it was also found that out of total urban cooperative banks under the study 72.2 percent urban cooperative banks revealed that key management system is not based on agreed set of standards, procedures and secure methods. [Ref. Table No. 5.40]

Conclusion

The cryptography control addresses the security measures used to ensure that information transmitted is readable only by the authorized individual. This is commonly referred to as encryption. Encryption is the transformation of plain text into an unreadable cipher text and is the basic technology used to protect the confidentiality and integrity of data. Cryptography can introduce security problems when it is not implemented accurately. Cryptographic solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. From above findings it is concluded that out of total urban cooperative banks under the study majority of the urban cooperative banks have not implemented adequate cryptography controls to ensure confidentiality and integrity of data.
10. Data Security:

- It was found that out of total urban cooperative banks under the study, 61.10 percent urban cooperative banks stated that they have their own data centre, while 38.90 percent urban cooperative banks stated that such facility is not available at their urban cooperative banks. [Ref. Table No. 5.41]

- It was also found that out of total urban cooperative banks under the study, 94.40 percent urban cooperative banks stated that have documented and tested data backup strategies and procedures. [Ref. Table No. 5.41]

- From the statistical data it has been observed that out of total urban cooperative banks under the study, 83.30 percent urban cooperative banks stated that data backup strategies cover data, programs, system files, parameter files etc. for all systems including servers, desktops, phone/network systems, system/network management systems, standalone/portable systems, control systems. [Ref. Table No. 5.41]

- It has been found that out of total urban cooperative banks under the study, 94.50 percent urban cooperative banks stated that the backup media protected against loss, theft, damage, fire (fire safes BS-certified) including both on-site and off-site/remote storage and are normally locked up. [Ref. Table No. 5.41]

- It has been observed that out of total urban cooperative banks under the study, 72.30 percent urban cooperative banks stated that data backup is scheduled automatically. [Ref. Table No. 5.41]

- It has been also observed that out of total urban cooperative banks under the study, 88.90 percent recorded that they have maintained physical and environmental security at data centre and disaster site. A similar percentage is supported for accountability of backup data is ensured by UCBs [Ref. Table No. 5.41]

- It has been found that out of total urban cooperative banks under the study, 44.50 percent urban cooperative banks depends on disaster site for back up data, While over 55.50 percent urban cooperative banks does not have disaster site for data backup. [Ref. Table No. 5.41]

- It has been also observed that out of total urban cooperative banks under the study, 94.40 percent urban cooperative banks scheduled a data backup once a day, while
5.60 percent urban cooperative banks scheduled data backup twice a day. [Ref. Table No. 5.42]

Conclusion
An effective backup strategy is essential for safe business from the effects of data loss. The UCBs need better and more consistent strategies for backing up data and archiving data to support compliance, reduce risk and deliver expected benefits of technology-driven environment.

- It has been found that out of total urban cooperative banks under the study, 50 percent urban cooperative banks review policies, procedures, standards and guidelines regularly for business community. [Ref. Table No. 5.44]
- It was also found that out of total urban cooperative banks under the study 61.10 percent urban cooperative employed high availability designs for IT systems, networks etc. to support critical business processes. [Ref. Table No. 5.44]
- Evaluation of business continuity plans, continuity exercises/tests etc. is carried out by sampling and reviewing process documentation and reports confirmed by 61.10 percent of urban cooperative banks out of total urban cooperative banks under the study. [Ref. Table No. 5.44]
- It has been also observed that out of total urban cooperative banks under the study, 50 percent urban cooperative banks members of the crisis/incident management and recovery teams and other relevant staff are aware of the plans and are clear on their personal roles and responsibilities. [Ref. Table No. 5.44]
- It was observed that out of total urban cooperative banks under the study, 55.60 percent urban cooperative banks have no single rational framework for business continuity planning in their urban cooperative banks,[Ref. Table No. 5.44]
- It has been found from the statistical data that out of total urban cooperative banks under the study 61.10 percent urban cooperative banks follow adequate business continuity plans and the planning process to satisfy the identified information security requirements. [Ref. Table No. 5.44]
- It has been observed that out of total urban cooperative banks under the study, 61.10 percent urban cooperative bank’s business continuity plans are regularly
exercised/tested to ensure that they are remaining up to date and effective. [Ref. Table No. 5.44]

Conclusion

Business Continuity Management and Information Security are achieved by applying best practices and controls, which require a combination of policies, procedures and physical or hardware / software measures to be implemented. An effective business continuity management is implemented by urban cooperative banks to reduce operational risk, limit the financial losses and handled emergencies and restores the operations. The ability of urban cooperative banks to recover from a disaster is directly related to the degree of BCM [Business Continuity Management] that has taken place before the disaster. With increasing pressure on businesses to run 24 X 7, continuous availability of all critical functions has become an important for UCBs. The ability of banks to recover from a disaster is directly related to the degree of BCP [Business Continuity Planning] that has taken place before the disaster. From the above findings it was concluded that many of the UCBs does not realized the importance of BCM and therefore their CBS environment have not ensured the continuous availability of all the critical functions in case of disaster.

12. Information security policy domains

- It was observed that out of total urban cooperative banks under the study, 44.4 percent urban cooperative banks implemented patch management, while 22.2 percent urban cooperative banks have not implemented such measure and 33.3 percent urban cooperative banks were unable to answer. [Ref. Table No. 5.45]

- Configuration management is responsible for identifying, controlling, and tracking all versions of hardware, software, documentation, processes, procedures, and all other components of the IT environment. It has been found that out of total urban cooperative banks under the study, 55.60 percent urban cooperative banks follow the best practice for configuration management, while 11.1 percent urban cooperative bank have not implemented such security controls and 33.3 percent urban cooperative banks were unable to answer. [Ref. Table No. 5.45]

- It has been also found that out of total urban cooperative banks under the study 38.9 percent urban cooperative banks have implemented the best practices for
change control management, while 16.5 percent urban cooperative banks have no such measures in place in CBS and 44.4 percent urban cooperative banks were unable to answer. [Ref. Table No. 5.45]

- From the statistical data, it has been found that out of total urban cooperative banks under the study 22.2 percent urban cooperative banks revealed that they have adopted computer forensics techniques to capture and maintain forensic evidence, while 44.4 percent urban cooperative banks have no such security control in place in CBS solution environment and 33.3 percent urban cooperative banks were not able to answer. [Ref. Table No. 5.45]

Conclusion
Therefore, it is concluded that information security domain controls are fundamental component of CBS solution environment of all urban cooperative banks information-security system. Still, these domain control process to identify, acquire, install and verify security updates and capture forensic evidence for applications and systems isn't consistently applied by several urban cooperative banks in their CBS solution environment.

13. Periodic Penetration Testing
Penetration testing is the process of attempting to gain access to the system. A successful penetration would lead to obtaining sensitive information (violation of confidentiality), modifying information (violation of integrity), or rendering the systems inoperable (violation of availability). It has been found that out of total urban cooperative banks under the study, 55.6 percent urban cooperative banks do not conduct penetration testing on regular basis to identify the gap in information security architecture, while 44.4 percent urban cooperative banks conduct penetration testing to maintain system confidentiality, integrity, availability. [Ref. Table No. 5.46]

Conclusion
Therefore, it is concluded that the higher number of urban cooperative banks i.e. 55.6 percent do not conduct penetration test therefore their CBS solution environment is vulnerable and lead to obtaining sensitive information (violation of confidentiality),
modifying information (violation of integrity), or rendering the systems inoperable (violation of availability).

14. Viruses protection

- It has been found that out of total urban cooperative banks under the study, 94.4 percent urban cooperative banks have policy procedure is in place for virus protection, while only 5.6 percent urban cooperative banks does not have such policy, procedure in place. [Ref. Table No. 5.47]
- It has been also observed that all the urban cooperative banks under the study update antivirus software regularly. [Ref. Table No. 5.48]
- Furthermore, it has been also found that out of total urban cooperative banks under the study, 94.4 percent urban cooperative bank’s computers external device is checked for viruses, worms and malwares. [Ref. Table No. 5.48]
- It has been found that out of total urban cooperative banks under the study, 83.3 percent urban cooperative banks have ensured end user computer’s USB ports are locked. [Ref. Table No. 5.48]

15. ATM Security

- It has been found that out of total urban cooperative banks under the study, 66.7 percent urban cooperative banks stated that to operate ATM, dual control is set up and similar number of urban cooperative banks ATM cash dispenser and depository shaft designed to prevent “fishing” and “trapping. [Ref. Table No. 5.50]
- Furthermore, it has been also observed that out of total urban cooperative banks under the study, 72.20 percent urban cooperative bank’s ATM is equipped with surveillance camera to record criminal activity at and around the ATM and 61.1 percent urban cooperative bank’s remote ATM is not equipped with a silent robbery alarm, telephone, or other means of communication with law enforcement official. [Ref. Table No. 5.50]
- In addition, it has been found that out of total urban cooperative banks under study, 44.40 percent urban cooperative bank’s ATM service entrance is equipped with a viewing port or CCTV system that allows personnel inside the service room to view activity outside. [Ref. Table No. 5.50]
It has been also observed that out of total urban cooperative banks under the study, 50 percent urban cooperative bank’s ATM provides customers with adequate privacy to prevent bystanders from observing details of their transactions (e.g. entry of their pin numbers).[Ref. Table No. 5.50]

It was also observed that out of total urban cooperative banks under the study, 72.20 percent urban cooperative banks revealed that security guard is appointed at the ATM centre.[Ref. Table No. 5.50]

**Conclusion**

Therefore, it is concluded that although ATMs are the primary source of cash withdrawals, very few urban cooperative banks have taken few, if any, measures to protect customers from criminal’s activity. Majority of urban cooperative banks have not installed surveillance camera to record criminal activity at and around the ATM, remote ATM is not equipped with a silent robbery alarm, telephone, or other means of communication with law enforcement official and the service entrance is not equipped with a viewing port or CCTV system that allows personnel inside the service room to view activity outside. Only 50 percent of the urban cooperative bank’s ATM provides customers with adequate privacy to prevent viewer from observing details of their transactions (e.g. entry of their pin numbers). Therefore it is concluded that ATM security of UCBs is in infancy stage.

**16. Internet Banking Security**

- It has been observed out of total urban cooperative banks under the study, 50 percent urban cooperative banks provided internet banking facility to their customer, while rest of the 50 percent urban cooperative banks provide no such facility in their CBS solution environment.[Ref. Table No. 5.51]

- It has been also observed out of total urban cooperative banks under the study, 33.33 percent urban cooperative banks indicated that a security policy for internet banking was duly approved by the board of directors. Similar percentage was supported for two-factor authentication for fund transfers through internet banking. [Ref. Table No. 5.52]
From the statistical data it has been found that out of total urban cooperative banks under the study 33.33 percent urban cooperative bank’s software locks the user-id if it is used for X unsuccessful times to logon to the system. [Ref. Table No. 5.52]

It has been also found that out of total urban cooperative banks under the study majority of the urban cooperative banks i.e. 88.89 percent stated that the software does not allow creation of user-IDs in the same name more than once and a similar percentage is supported for software forces the user to change the password at set periodical intervals.[Ref. Table No. 5.52]

Furthermore, it has been also observed that out of total urban cooperative banks under the study, 88.89 percent urban cooperative bank’s CBS system application software maintains password length minimum 6 or 8 characters or as the case may be with combinations of alpha, numeric and special characters.[Ref. Table No. 5.52]

Conclusion
From the above finding it is concluded that out of total urban cooperative banks under the study only 50 percent of the urban cooperative banks provided internet banking facility to their customer. The urban cooperative banks those are having the internet banking facilities in CBS environment also lacking on standardization in internet banking security.

17. Types of cyber attacks experienced by UCB’s

It has been found that out total bank under the study 22.2 percent urban cooperative banks computer system was infected by malware, while 11.1 percent urban cooperative banks revealed that their systems were experienced phishing attacks. [Ref. Table No. 5.53]

Further, out of total urban cooperative banks under the study 16.70 percent urban cooperative bank’s computer systems were experienced password sniffing and financial fraud. [Ref. Table No. 5.53]

Denial of service, exploit of wireless network, system penetration, laptop or mobile, hardware theft or loss and exploit of client web browser was experienced by their CBS solution environment confirmed by 11.10 percent urban cooperative banks out of total urban cooperative banks under the study.[Ref. Table No. 5.53]
In addition out of total urban cooperative banks under the study, 5.6 percent urban cooperative banks agreed upon insider abuse of internet access or e-mail, Exploit of DNS server and instant messaging abuse. [Ref. Table No. 5.53]

It is also observed that out of total urban cooperative banks under the study 16.70 percent urban cooperative banks stated that unauthorized access to the system by insider was taken place. [Ref. Table No. 5.53]

**Conclusion**

Therefore it is concluded that most of the UCBs fall for victim to cybercrime, but to different degrees. The above finding shows that the cyber attacks on CBS environment faced by urban cooperative banks are likely to continue over the next few years. The most cyber crimes are those caused by denial of services, malicious code (Malware), password sniffing and financial fraud and unauthorized access. UCBs may minimize the frequency of such crimes by conducting training and awareness program.

**18. Regulatory Compliance**

- It has been found that out of total urban cooperative banks under the study, 72.2 percent urban cooperative banks have carried out implementation audit for CBS solution. [Ref. Table No. 5.54]

- Furthermore, it has been also observed that out of total urban cooperative banks under the study 66.7 percent urban cooperative banks have carried out compliance audit for implementation audit, while 33.3 percent urban cooperative banks revealed that no such audit is carried out for CBS solution [Ref. Table No. 5.54]

**Conclusion**

For effective regulatory and supervisory compliance the urban cooperative banks need to use IT in their operations. CBS helps to integrate range of services that can be offered by all the bank’s branches from centralized data centers. The applicability of various government mandatory regulation and banking practices in CBS are still evolving.
19. Monitoring features of CBS solution

- It is found that out of total urban cooperative banks under the study 61.1 percent urban cooperative bank’s CBS is featured with comprehensive application logs with options for information, warning and critical message and administrative alerts. [Ref. Table No. 5.56]

- Furthermore, it is also observed that out of total urban cooperative banks under the study, 77.8 percent urban cooperative bank’s CBS solution is featured with monitoring of full usage statistics i.e. user access logs and detailed information on sessions, time, duration, services used. [Ref. Table No. 5.56]

20. Overall security level of CBS solution

- When the respondents were requested to rate their security level of CBS solution, it has been found that out of total urban cooperative banks under the study 55 percent urban cooperative banks have their CBS is somewhat secure. A compilation of the result shows that 28 percent of the urban cooperative banks indicated the system is fully secure. [Ref. Table No. 5.57]

6.2.2 Part II: Perception of IT heads regarding applicability of information security standards

- It was found that out of total urban cooperative banks under the study, very few urban cooperative banks i.e. 16.7 percent have followed ISO/IEC 27002: 2005 (code of practice for information security management) benchmark in CBS solution environment, while 44.4 percent do not followed such benchmarks information security management and 38.9 percent urban cooperative banks were unable to answer. [Ref. Table No. 5.55]

- It has been also observed that out of total urban cooperative banks under the study 61.1 percent urban cooperative banks stated that ISO/IEC 15408 (Evaluation Criteria for IT Security) and ISO/IEC 13335 (IT Security Management) benchmark are not supported for CBS environment, while 38.9 percent urban cooperative banks have not answered. [Ref. Table No. 5.55]

- It is also found that out of total urban cooperative banks under the study, COBIT (IT Governance) standard is followed by 11.1 percent urban cooperative banks. [Ref. Table No. 5.55]
Furthermore out of total urban cooperative banks under the study, only 5.6 percent urban cooperative banks stated that Information Technology Infrastructure Library (ITIL) (OR ISO/IEC 20000 SERIES) standards and ISACA standards and ISO 17799 for creating, documenting and implementing security policies are implemented for CBS environment.[Ref. Table No. 5.55]

Conclusion

The above finding shows that majority of UCBs information security system solutions are not as per adequate information security standard. Since they are not following the information security standard they CBS solution environment is at high risk.

6.2.3 Part III: Perception of employees (end users) regarding awareness about information security

- The statistical findings shows that out of total respondents under the study, majority of the respondents i.e. 93.3 percent has positive approach towards password protects system, service or programs. [Ref. Table No. 5.63]

- Furthermore, it is also found that out of total respondents under the study, 80.9 percent respondents agreed upon that longer password is more secure, on the other hands, 66.4 percent of the respondents reported they are aware of use of combination of uppercase, lowercase letters, including special characters difficult to crack the password. [Ref. Table No. 5.63]

- It has been also observed that out of total respondents under the study, 74.2 percent of the respondents stated that password should be updated regularly so that a probability of password being cracked is less. On password security awareness, 68.8 percent of the respondents agreed that hacker may take a very long time to crack a long, complex password. [Ref. Table No. 5.63]

- Out of total respondent under the study, 79.9 percent of the respondents are aware that to prevent unauthorized access never record password anywhere. In addition, 55.9 percent of the respondents agreed on not to open attachments send by a stranger. [Ref. Table No. 5.63]

- It has been observed that out of total respondents under the study, 99.4 percent respondents stated that they change their password regularly and frequency of duration of password updation is between 14 to 21days replied by 36.7 percent
respondents.[Ref. Table No. 5.65 and Table No. 5.64]

- It has been observed that out of total respondents almost 43 percent respondents stated that it is difficult to remember the password if changed regularly. [Ref. Table No. 5.66]

- It has been revealed that out of total respondents under the study 90.7 percent of the respondents stated that they log off the system when they leave the room or terminal. Furthermore 51.5 percent of the respondents said that they lock the office or room when they leave the terminal. Majority of the respondents i.e. 94.9 percent stated that each computer was provided with a screen saver locked with a password. According to 69.5 percent of the respondents, they shut down the system while they were not around or not using the CBS solution. [Ref. Table No. 5.67]

- It was observed that out of total respondents under the study, 37.1 percent respondents stated that they do have access to transfer the data to external storage device and 1.9 percent of the respondents were unable to answer. [Ref. Table No. 5.68]

**Conclusion**
From the statistical findings it is concluded that the awareness level of employee’s regarding password management is high.

**6.2.4 Part IV: Perception of employees regarding training and awareness program on information security**

- It was observed that out of total respondents under the study, 72.5 percent respondents have positive approach towards management of UCBs conduct training and awareness program on information security. However, 27.5% stated that their bank’s management does not conduct training and awareness program.[Ref. Table 5.58]

- On assessing the frequency of duration of training and awareness program, it was found that out of total respondents under the study 55.1 percent respondents stated that the training program duration is one to seven days, while 0.4 percent respondents stated that it is between 8 to 21 days. [Ref. Table 5.59]

- It was found that out of total respondents under the study, 58.77 percent of the respondents stated that policies/procedures included as part of training program,
while 66.67 percent of the respondents stated usage of IT assets. Furthermore 73.39 percent of the respondents indicated that a standard relating to passwords and authentication topic was also part of training and awareness program. 71.05 percent respondents stated that Procedures of email and internet usage is also a part of training program, while 71.35 percent of the respondents indicated Physical protection. Furthermore 55.56 percent of the respondents revealed that training and awareness program also focuses on remote computing, likewise 72.51 percent of the respondents indicated Safe handling of sensitive data/information. 69.30 percent of the respondents rated for Network security and 75.15 percent respondents stated that training is also given on how to report security incidents occurs.[Ref. Table 5.60]

- From statistical analysis it has been observed that out of total respondents under the study, 99.12 percent respondents stated that the training program gives the better idea of information security, while 0.88 percent respondents stated negative response [Ref. Table 5.61]

- It has been observed that out of total respondents under the study, 45.91 percent of the respondents were highly satisfied, whereas 22.80 percent of the were Highly Dissatisfied with training and awareness program, 19 percent of the respondents were somewhat satisfied and 12.28 percent respondent were not answered.[Ref. Table 5.62]

**Conclusion**

The finding of the study shows that the respondents were satisfied in general with training and awareness program conducted by UCBs as the percentage of respondents is high. Also it is observed that most of the important topics are covered as a part of Information security training and awareness program.

**6.2.5 Summary of Findings**

The researcher has summarized the information security status in core banking environment of 18 urban cooperative banks under the study as shown in the following Table No. 6.1. Figures indicated that the percentage of domain controls is in place in UCB’s core banking environment.
Table No. 6.1: Summary of findings

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bank 1</td>
<td>0</td>
<td>100</td>
<td>100</td>
<td>87.5</td>
<td>66.33</td>
<td>109</td>
<td>100</td>
<td>100</td>
<td>63.63</td>
<td>90.9</td>
<td>80</td>
<td>100</td>
<td>60</td>
<td>75</td>
<td>100</td>
<td>100</td>
<td>7.14</td>
<td>80</td>
<td>50</td>
<td>0</td>
<td>85.71</td>
<td>74.83</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Bank 2</td>
<td>0</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>66.33</td>
<td>109</td>
<td>100</td>
<td>100</td>
<td>81.81</td>
<td>90.9</td>
<td>0</td>
<td>50</td>
<td>100</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50</td>
<td>100</td>
<td>85.71</td>
<td>72.49</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Bank 3</td>
<td>0</td>
<td>100</td>
<td>100</td>
<td>87.5</td>
<td>83.33</td>
<td>109</td>
<td>69</td>
<td>100</td>
<td>45.46</td>
<td>100</td>
<td>0</td>
<td>70</td>
<td>25</td>
<td>100</td>
<td>100</td>
<td>0</td>
<td>60</td>
<td>100</td>
<td>7.14</td>
<td>0</td>
<td>100</td>
<td>71.43</td>
<td>69.90</td>
</tr>
<tr>
<td>4</td>
<td>Bank 4</td>
<td>0</td>
<td>100</td>
<td>100</td>
<td>75.0</td>
<td>83.33</td>
<td>42.85</td>
<td>19</td>
<td>100</td>
<td>190</td>
<td>72.72</td>
<td>100</td>
<td>70</td>
<td>90</td>
<td>100</td>
<td>100</td>
<td>85.71</td>
<td>71.43</td>
<td>60</td>
<td>100</td>
<td>0</td>
<td>100.00</td>
<td>70.96</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Bank 5</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>100</td>
<td>50.0</td>
<td>16.66</td>
<td>28.57</td>
<td>90</td>
<td>100</td>
<td>36.36</td>
<td>72.72</td>
<td>100</td>
<td>80</td>
<td>15</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>7.14</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>0.00</td>
<td>45.29</td>
</tr>
<tr>
<td>6</td>
<td>Bank 6</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>87.5</td>
<td>100</td>
<td>109</td>
<td>100</td>
<td>100</td>
<td>63.63</td>
<td>100</td>
<td>20</td>
<td>100</td>
<td>85</td>
<td>20</td>
<td>100</td>
<td>100</td>
<td>7.14</td>
<td>100</td>
<td>100</td>
<td>0</td>
<td>85.71</td>
<td>90.32</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Bank 7</td>
<td>0</td>
<td>100</td>
<td>100</td>
<td>50.0</td>
<td>83.33</td>
<td>42.85</td>
<td>20</td>
<td>100</td>
<td>81.81</td>
<td>81.81</td>
<td>0</td>
<td>100</td>
<td>65</td>
<td>50</td>
<td>100</td>
<td>57.14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>40.91</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Bank 8</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>50.0</td>
<td>83.33</td>
<td>42.85</td>
<td>20</td>
<td>100</td>
<td>81.81</td>
<td>81.81</td>
<td>0</td>
<td>100</td>
<td>65</td>
<td>50</td>
<td>100</td>
<td>57.14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>40.91</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Bank 9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50.0</td>
<td>33.33</td>
<td>57.14</td>
<td>100</td>
<td>100</td>
<td>36.36</td>
<td>90.9</td>
<td>0</td>
<td>80</td>
<td>25</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>100</td>
<td>71.43</td>
<td>38.37</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Bank 10</td>
<td>0</td>
<td>100</td>
<td>100</td>
<td>25.0</td>
<td>33.33</td>
<td>42.85</td>
<td>69</td>
<td>60</td>
<td>72.72</td>
<td>72.72</td>
<td>0</td>
<td>70</td>
<td>15</td>
<td>0</td>
<td>50</td>
<td>85.71</td>
<td>7.14</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>57.14</td>
<td>47.80</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Bank 11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50.0</td>
<td>33.33</td>
<td>57.14</td>
<td>100</td>
<td>100</td>
<td>36.36</td>
<td>90.9</td>
<td>0</td>
<td>80</td>
<td>25</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>100</td>
<td>71.48</td>
<td>88.87</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Bank 12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>75.0</td>
<td>100</td>
<td>42.5</td>
<td>0</td>
<td>100</td>
<td>43.95</td>
<td>72.72</td>
<td>0</td>
<td>50</td>
<td>15</td>
<td>0</td>
<td>50</td>
<td>85.71</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>0.00</td>
<td>44.16</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Bank 13</td>
<td>0</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>109</td>
<td>100</td>
<td>100</td>
<td>190</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>0</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100.00</td>
<td>90.91</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Bank 14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50.0</td>
<td>33.33</td>
<td>57.14</td>
<td>100</td>
<td>100</td>
<td>36.36</td>
<td>90.9</td>
<td>0</td>
<td>80</td>
<td>25</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>71.43</td>
<td>38.37</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Bank 15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50.0</td>
<td>33.33</td>
<td>57.14</td>
<td>100</td>
<td>100</td>
<td>36.36</td>
<td>90.9</td>
<td>0</td>
<td>80</td>
<td>25</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>100</td>
<td>71.43</td>
<td>38.37</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Bank 16</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>50.0</td>
<td>83.33</td>
<td>81.81</td>
<td>100</td>
<td>100</td>
<td>90</td>
<td>85.71</td>
<td>100</td>
<td>90</td>
<td>80</td>
<td>100</td>
<td>100</td>
<td>0</td>
<td>100</td>
<td>100</td>
<td>85.71</td>
<td>81.48</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Bank 17</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>62.5</td>
<td>33.33</td>
<td>50</td>
<td>100</td>
<td>80</td>
<td>81.81</td>
<td>90.9</td>
<td>0</td>
<td>60</td>
<td>40</td>
<td>0</td>
<td>100</td>
<td>14.29</td>
<td>7.14</td>
<td>40</td>
<td>100</td>
<td>100.00</td>
<td>57.27</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Bank 18</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>100</td>
<td>50.0</td>
<td>42.85</td>
<td>70</td>
<td>80</td>
<td>90.9</td>
<td>100</td>
<td>0</td>
<td>20</td>
<td>75</td>
<td>75</td>
<td>100</td>
<td>0</td>
<td>92.86</td>
<td>80</td>
<td>50</td>
<td>100</td>
<td>0.00</td>
<td>60.30</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>16.67</strong></td>
<td><strong>33.33</strong></td>
<td><strong>61.11</strong></td>
<td><strong>69.44</strong></td>
<td><strong>60.15</strong></td>
<td><strong>64.66</strong></td>
<td><strong>73.89</strong></td>
<td><strong>95.56</strong></td>
<td><strong>65.15</strong></td>
<td><strong>88.38</strong></td>
<td><strong>27.78</strong></td>
<td><strong>81.11</strong></td>
<td><strong>51.39</strong></td>
<td><strong>40.28</strong></td>
<td><strong>69.44</strong></td>
<td><strong>54.76</strong></td>
<td><strong>11.11</strong></td>
<td><strong>34.44</strong></td>
<td><strong>69.44</strong></td>
<td><strong>55.56</strong></td>
<td><strong>58.73</strong></td>
<td><strong>58.29</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
6.3 Conclusion of the study

This section presents the conclusion of the study. The domain wise summarised information security findings are shown in below Table No. 6.2.

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Information Security Domains</th>
<th>UCBs %</th>
<th>Sr. No.</th>
<th>Information Security Domains</th>
<th>UCBs %</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Escrow agreement</td>
<td>16.67</td>
<td>12</td>
<td>Data security</td>
<td>58.89</td>
</tr>
<tr>
<td>2</td>
<td>Information security Policy</td>
<td>33.33</td>
<td>13</td>
<td>Security technologies</td>
<td>51.39</td>
</tr>
<tr>
<td>3</td>
<td>Supervision of security solutions</td>
<td>61.11</td>
<td>14</td>
<td>IS policy domain</td>
<td>40.28</td>
</tr>
<tr>
<td>4</td>
<td>Physical access control</td>
<td>69.44</td>
<td>15</td>
<td>Application logs</td>
<td>69.44</td>
</tr>
<tr>
<td>5</td>
<td>Environmental security</td>
<td>60.15</td>
<td>16</td>
<td>Business continuity management</td>
<td>54.76</td>
</tr>
<tr>
<td>6</td>
<td>Asset management</td>
<td>64.66</td>
<td>17</td>
<td>Cyber attacks experienced</td>
<td>11.11</td>
</tr>
<tr>
<td>7</td>
<td>HR Security</td>
<td>73.89</td>
<td>18</td>
<td>Penetration testing</td>
<td>34.44</td>
</tr>
<tr>
<td>8</td>
<td>Logical access control</td>
<td>95.56</td>
<td>19</td>
<td>IS audit</td>
<td>69.44</td>
</tr>
<tr>
<td>9</td>
<td>Network security</td>
<td>65.15</td>
<td>20</td>
<td>Security standards</td>
<td>55.56</td>
</tr>
<tr>
<td>10</td>
<td>OS access control</td>
<td>88.38</td>
<td>21</td>
<td>ATM security</td>
<td>58.73</td>
</tr>
<tr>
<td>11</td>
<td>Cryptographic controls</td>
<td>27.78</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

From the Table No. 6.2, it was observed that 16.67% UCBs are having escrow agreement in place for source code access. 33.33% UCBs have well documented information security policy and duly approved by management. Furthermore 61.11% UCBs have deployed information security solution for supervision and monitoring of the system usage. The adequate controls for environmental and physical security are implemented by 60.15% and 69.44% of UCBs respectively. In addition, 64.66% of UCBs have appropriate assets management procedure is included in CBS solution. Majority of the banks i.e. 95.56 % have high level of logical access controls in CBS solution. Majority of the banks i.e. 88.38% have adequate operating system level access controls in place to ensure confidentiality, integrity and availability of data and
information. Only 27.78% banks have cryptography controls in place for secured communication. The adequate data security controls are implemented by 58.89% of the banks.

Additionally 51.39% of the banks have appropriate information security technologies to prevent, detect and monitor the security breached. Furthermore 40.28% banks have appropriate procedure for IS policy domain i.e. patch management, configuration management and version management. The facility of application log in CBS solution to monitor and review the usage of data and system is seen in 69.44% of the banks under the study.

The adequate procedure for business continuity management to recover from disaster is observed in 54.76% of the banks. Furthermore 34.44% of the banks conduct penetration test to find out the gaps in existing CBS solution software. Whereas 69.44% of the banks conduct information security implementation audit and compliance audit for implementation audit for the application software.

Moreover 55.56% banks CBS solution is implemented based on the information security standards. Furthermore 58.73% of the banks follow adequate controls and practices for ATM security. The cyber attacks were experienced by 11.11% of the banks.

**6.3.1 Domain wise overall information security level of UCBs**

The UCBs must determine the appropriate security levels based on the UCBs confidentiality, integrity and availability needs for the information as well as for business operations. These requirements are covered in the legal, regulatory and policy frameworks. This focuses the basis for assessing the risks to business operations and assets and in selecting appropriate security controls and techniques.

The Table No. 6.3 defines the groups and their associated risk level. To assess the information security level and the risk level of various controls of CBS solution in UCBs under study, the researcher has defined the level of information security based on three groups namely Group A, Group B and Group C. The following Table No. 6.3 shows the groups, their grouping percentage and associated level of information security and risk level.
Table No. 6.3 : Groups and their associated risk level

<table>
<thead>
<tr>
<th>Group</th>
<th>Grouping Range (%)</th>
<th>Level of Information Security</th>
<th>Risk Level</th>
<th>Impact of risk on UCBs CBS environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A</td>
<td>&gt;75% and &lt;=100%</td>
<td>High</td>
<td>Low</td>
<td>Pose with the likely for limited impact on the confidentiality, integrity, availability and efficiency.</td>
</tr>
<tr>
<td>Group B</td>
<td>&gt;50% and &lt;=75%</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Pose with the potential for moderate to serious impact on the integrity, availability and efficiency.</td>
</tr>
<tr>
<td>Group C</td>
<td>&gt;0% and &lt;=50%</td>
<td>Low</td>
<td>High</td>
<td>Pose with the potential for extremely serious impact on the integrity, availability and efficiency.</td>
</tr>
</tbody>
</table>

The information security domains are grouped under Group A, whose UCBs percentile is more than 75 percent and less than or equal to 100 percent. The security level of Group A is defined as high level since the percentile is high and therefore the security domains under this group is at low risk.

Similarly, the information security domains are grouped under Group B, whose UCBs percentile is more than 50 percent and less than or equal to 75 percent. The security level of Group B is defined as moderate level since the percentile of UCBs for security domains is moderate and therefore the security domains under this group is at moderate risk.

Furthermore, the information security domains are grouped under Group C, whose UCBs percentile is more than 0 percent and less than or equal to 50 percent. The security level of Group C is defined as low level since the percentile of UCBs for security domains is low and therefore the security domains that belongs to this group is at high risk.
The Table No. 6.4 shows the grouping of information security domains across the three groups and their associated risk level.

**Table No. 6.4: Group wise information security controls and their risk level in CBS solution of UCBs**

<table>
<thead>
<tr>
<th>Group No.</th>
<th>Sr. No</th>
<th>Information security domain</th>
<th>UCBs %</th>
<th>Level of Security</th>
<th>Level of Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A</td>
<td>1</td>
<td>Logical access</td>
<td>95.56</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>OS access control</td>
<td>88.38</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>HR security</td>
<td>73.89</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group B</td>
<td>1</td>
<td>Physical access control</td>
<td>69.44</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Application logs</td>
<td>69.44</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>IS audit</td>
<td>69.44</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Network security</td>
<td>65.15</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Asset management</td>
<td>64.66</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Monitoring features of Security solution</td>
<td>61.11</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>Environmental security</td>
<td>60.15</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>Data security</td>
<td>58.89</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>ATM security</td>
<td>58.73</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>Security standards</td>
<td>55.56</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>Business continuity management</td>
<td>54.76</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>Security technologies</td>
<td>51.39</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group C</td>
<td>1</td>
<td>IS policy domain</td>
<td>40.28</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Penetration testing</td>
<td>34.44</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Information security policy</td>
<td>33.33</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Cryptographic controls</td>
<td>27.78</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Escrow agreement</td>
<td>22.22</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
From the Table No. 6.4, it was observed that three domain control areas namely logical access, operating system access control and human resource security are grouped under Group A.

Group B consists of 12 domain areas such as physical access control, environmental security, asset management, network security, data security, ATM security, security standards, business continuity management, application logs, IS audit, security technologies and monitoring features of security solution whose implementation level of security is moderate.

Group C consists of security domain areas namely escrow agreement, information security policy, cryptographic controls, IS policy domains and penetration testing.

From the Table No. 6.4, it was observed that urban cooperative banks have adequately implemented three domain controls namely logical access, operating system access control and human resource security in CBS solution. These controls provide high level of security and therefore minimise the risk of information security breaches in CBS solution environment of UCBs.

Furthermore, urban cooperative banks have reasonably implemented physical access control, environmental security, asset management, network security, data security, ATM security, security standards, business continuity management, application logs, IS audit, security technologies and monitoring features of security solution in CBS solution. This type of implementation increases the risk to UCBs information in CBS solution and may lead to data loss. This type of implementation may impact on UCBs operations, functions, or reputation. A breach of this security level would result in a negative effect, or would result in damage, to an asset or IT resources.

In addition, urban cooperative banks have overlooked for escrow agreement, information security policy, cryptographic controls, IS policy domains and penetration testing resulting into security breaches. In such scenario risk to information security in CBS solution is very high. It may result in complete loss of major assets or resources.
The majority of security controls are not implemented in CBS solution environment of UCBs. Therefore it is concluded that the information security level in CBS solution environment is in infancy stage.

### 6.3.2 Grouping of UCBs based on information security level

To calculate information security level wise percentage of UCBs, the researcher has selected the variables such as escrow agreement, information security policy, physical access control, environmental security, asset management, HR security, logical access control, network security, OS access control, cryptographic controls, data security, IS policy domains, BCM, penetration testing, security standards, ATM security, training and awareness, IS audit, and monitoring features. The Table No. 6.5 shows the risk level wise grouping of UCBs and their percentage along with the impact of risk on UCBs for CBS solution environment and business.

<table>
<thead>
<tr>
<th>Group No.</th>
<th>Grouping Range (%)</th>
<th>Level of information Security</th>
<th>Risk Level</th>
<th>Number of banks</th>
<th>Impact of risk on UCBs CBS environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group A</td>
<td>&gt;75% and &lt;=100%</td>
<td>High</td>
<td>Low</td>
<td>2 (11%)</td>
<td>Pose with likely for limited impact on the confidentiality, integrity, availability and efficiency.</td>
</tr>
<tr>
<td>Group B</td>
<td>&gt;50% and &lt;=75%</td>
<td>Moderate</td>
<td>Moderate</td>
<td>5 (21%)</td>
<td>Pose with the potential for moderate to serious impact on the integrity, availability and efficiency.</td>
</tr>
<tr>
<td>Group C</td>
<td>&gt;0% and &lt;=50%</td>
<td>Low</td>
<td>High</td>
<td>11 (61%)</td>
<td>Pose with the potential for extremely serious impact on the integrity, availability and efficiency.</td>
</tr>
</tbody>
</table>
From the Table No. 6.5, it has been observed that out of total urban cooperative banks under the study only 2 UCBs i.e. 11% are implemented adequate security controls measures to mitigate risk and prevent the data loss. The overall percentage of security for the above selected variable is 81.75%. These UCBs implemented the security controls as per the standards. These two UCBs have information security policy in place, existence of escrow agreement for source code access, physical and environmental security controls as per industry recommended standards, adequate security controls are in place for asset management, Human resource security, logical access control, network security, Operating system access control, cryptographic controls, data security, monitoring features and ATM Security. These UCBs have documented policy, procedures and practices for IS policy domain such as configuration management, patch management, version maintenance and virus protection. UCBs implemented adequate procedure for business continuity management to recover from disaster. They also conduct the regular penetration testing to find the gaps or to ensure integrity of system. Their information security in CBS solution environment is designed and developed as per industry recommended information security standards. These two UCBs conduct training and awareness program on information security on regular basis to minimise the errors and risk of information system. The impact of such information security controls is that till date these UCBs CBS solution environment is not experienced or victim of any cyber crime. Therefore their CBS solution environment is at very low risk level. This may cause limited impact on the confidentiality, integrity, availability and efficiency.

Furthermore from the data analysis it has been found that out total urban cooperative banks under the study, 5 UCBs i.e. 21% are having moderate level of information security controls in place. The overall information security level of these banks is 57.68%. In addition to this it is found that these banks are the victim of cyber attacks to some extent. The cumulative percentage of various cyber attacks experienced by UCBs is 11.11%. If information security is not planned and implemented adequately in CBS solution there are chances to increase cyber attacks by hackers or insider to gain access to sensitive and confidential data. The domain controls that are highly important and need to be adequately implemented by UCBs are IS policy, data security, escrow agreement, penetration testing, IS audit Therefore their CBS solution
environment is at moderate risk level. This may cause moderate to serious impact on the confidentiality, integrity, availability and efficiency of information security.

Also from the data analysis, it has been found that out total urban cooperative banks under the study, majority i.e. 11 UCBs(61%) are having low level of information security controls in place. In addition to this it is found that these banks are the victim of cyber attacks at some extends. The cumulative percentage of various cyber attacks experienced by UCBs is 11.11%. If information security is not planned and implemented adequately in CBS solution then probability of increase in cyber attacks by hackers or insider to gain access to sensitive and confidential data is very high. The overall information security level of these banks is 40%. These banks even don’t have basic information security controls in place to minimise the data loss or to minimise the risk of information security. Therefore their CBS solution environment is at high risk. This may cause serious impact on the confidentiality, integrity, availability and efficiency of information security.

It is concluded from the findings and observation that majority of UCBs are required to plan, design, implement and assess information security in CBS solution environment to mitigate the reputational, operational risk and to comply with regulatory compliance. The key challenging issues in information security in CBS solution environment of UCBs are:

- View security as of little importance
- Lack of Information Security Standard
- Budget constraints
- Non existence of escrow agreement
- Lack of information security policies and procedures in place
- Inadequate physical and environmental security controls
- Inadequate access control procedure
- Weakness in Network Security
- Absence of adequate cryptography controls
- Data security controls with non compliance to recommended standards
- Poor implementation of security policies
- Poor implementation of information Security controls
Therefore it is concluded that majority of the UCBs are not serious about the information security. This may adversely affects on the functioning of UCBs CBS solution. This may cause potential extreme serious impact on the confidentiality, integrity, availability and efficiency of information security. Therefore it is concluded that the information security in UCBs CBS solution environment is in infancy stage.

6.5 Suggestions

It has been found from the data analysis that, urban cooperative banks have experienced a number of security breaches. These incidents have raised uncertainties on the environment of information security and security controls. India is home of large number of urban cooperative banks. These urban cooperative banks are facing challenges in many aspects and one of the important aspects is information security, and is pushing themselves in a complex business environment. With the growth of mobile banking and internet banking customers are becoming more and more technology savvy and expecting for secure and extended services. The tough competition is also facing urban cooperative banks under pressure to become more competent and responsive. At the same time, urban cooperative banks are hunting for different solution to reduce operating costs. In short, urban cooperative banks need to scale up their IT and improve operational efficiency in order to deliver reliable, continuous services in a cost effective and secured manner. The adoption of common policy, standards, guidelines and processes for information security including data classification and management enables the UCB’s to reduce the risk of inappropriate information access.

To address the situation, RBI has set up benchmarks, standards and legal regulations on information security to help UCBs to ensure an adequate level of security is maintained, resources are used in the appropriate manner, and the best information security practices are adopted.

The researcher has made certain suggestions based on findings and conclusion of the study for effective management of information security in CBS solution environment of UCBs to mitigate the risk and maximise the Return on Investment (ROI). The
suggestions offered by researcher would definitely enhance the information security of CBS environment of UCBs.

The findings and conclusion of the study provides the decision makers of UCBs the insights of present status of information security in CBS environment. The real time banking or core banking is useful to the customers as well as to the bankers. Therefore, UCBs are required to ensure the high availability of data integrity and transaction integrity in centralised environment to retain the customer and maximise the return on investment. This would also allow the UCBs for effective implementation and management of information security as per their business requirements. Based on the findings and conclusion of the study the following suggestions are offered by the researcher:

With reference to explanation at para 6.3 only two UCBs have implemented adequate information security controls based on industry recommended standards for efficient and effective management of information security in CBS solution environment. The all other UCBs need to adopt and implement information security controls as per their business requirements which were implemented by two UCBs under study as mentioned below so that breaches to information security pose likely to have limited impact on the confidentiality, integrity, availability and efficiency.

1. **Management of UCBs would provide support for design, develop and implementation of information security program:** The findings of the study suggest that top management support is the necessary for an effective and success of information security. The management has to provide a support for establishment of organization structure for information security, managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the controls. Before implementation of information security program the management of UCBs have to define the business objectives. Based on the business goals, risk assessments have to be carried out. The documentation of information security plan would enable in securing information assets and to comply with the objectives of business.
2. **Organization structure for information security management**: A Chief Information Security Officer (CISO) or equivalent may be appointed at executive management level, with overall responsibility for the UCBs information security programme. A CISO is responsible for developing and maintaining an information security strategy and policy that supports the security governance framework.

3. **Preventative measure for outsourced software**: It has been suggested that urban cooperative banks need to sign the contract with the service provider for outsourced CBS solution software. The urban cooperative banks need to establish clear metrics and service level agreement surrounding application security with their outsourcing partners as part of the procurement and contract processes. The urban cooperative banks have to ensure that the service provider signs nondisclosure agreements. It is also suggested that application security testing should be mandatory for all outsourced development and maintenance.

4. **Budget provision for up-gradation of IT infrastructure**: The urban cooperative banks, both large and small, include the information security budget in the overall IT budget. If enough budget provision is not allocated for information security, risk of losses, intrusions, viruses and security breaches increases. Therefore, information security budget provision may be the first component in an overall IT budget. The board of directors/management of each UCB has the responsibility for ensuring appropriate budget provision for information security. The information security budget may ensure appropriate resources to support the banking business. The information security budget provision may be provided for operational functioning of information security e.g. staff, infrastructure, hardware and software, training and awareness program, incident response planning.

5. **Escrow agreement for outsourced software**: A well-drafted escrow agreement is an important component of the risk mitigation plan. The key to an effective escrow arrangement is to ensure that the licensee is able to access and use source code and other relevant resources, on the occurrence of certain events such as maintenance services or a refusal by the software vendor to support the software, to obtain ongoing support for software. Therefore it is suggested for the urban
cooperative banks who have adopted the teller made or outsourced CBS solution need to sign escrow agreement for business continuity and mitigate the risk. This would help UCBs to assure that exiting CBS solution software would support for new technology.

6. **Well documented information security policy and procedure:** The urban cooperative banks should develop information security policy document which addresses management support, commitment, and direction to achieve information security goals. An information security policy document shall be approved by management and published and communicated to all employees and relevant external parties. The information security policy may clearly define the user’s roles and responsibilities towards the information they collect, use, access or process. As per the UCBs business requirement the policy need to address domain or control wise detailed procedure for information security. The management of UCBs may ensure that the information policy would be review at regular intervals for adequacy and effectiveness. The information policy may follow penal measures for violation of policies and the process in the event of violation.

7. **Adequate physical and environmental security:** In majority of UCBs physical and environmental protections are ignored. Effective physical security measures help to protect against unauthorized access, damage, or interference in the areas where critical or sensitive information is prepared or located, or where information processing services supporting key business processes are hosted. In today's ever-growing regulatory compliance landscape, urban cooperative banks may significantly benefit from implementing workable and verified physical security best practices as per their business needs.

- Ensure the physical security system such as electronic access controls (access cards/swipe-card), alarms, security locks, biometric access control system, and perimeter walls, security guards, CCTV /Web Camera, intruder detection system, identification badges for highly sensitive areas for authorized access effective availability of confidentiality and integrity of data and system.
- Ensure the process of registration, visitors pass, logbook for check in and checkout for the visitors, vendors or third party service provide to monitor or to recover from the security incident.
- Ensure for natural disasters (like fire, earthquake, flood etc.) risks are covered.
- Ensure for the power and telecommunications cabling are laid down with appropriate distance as per standard.
- Ensure the facilities like feed power supply, UPS, generator backups are in place for continuous availability of data and system.
- Maintains a network diagram that includes IP addresses, room numbers/location and asset owners or responsible personnel.
- Ensure for access to sensitive area such as server room, datacenter, UPS room is restricted through access control system.

8. Procedure for maintaining inventory of information assets: The goal of information security is to appropriately protect assets in order to ensure business continuity, minimize business damage, and maximize return on investments. The urban cooperative banks may ensure the detailed procedure for maintaining inventory of information assets and classification of assets.
   - An inventory of information assets such as computer and communications hardware/systems, application software, data and document is to be maintained as per ISO standards.
   - Ensure for the inventory of information assets is fully up-to-date, accurate and complete despite equipment or staff moves or new equipment or software is procured.
   - Ensure the appropriate registration process for new software and hardware etc.
   - Put appropriate asset tags on all PCs, network equipment.
   - Make sure that the power and data cables are clearly labelled.
   - Appropriate marking scheme is used for all documents, reports and backup media etc.
   - Conduct of training for staff designed for handling sensitive resources safely.
   - Ensure for detailed inventory of information assets should define asset location, risk to assets, and grouping of assets.
• Designate asset owner and custodian for overall management of information asset.

9. **Control systems to protect the computer network from intrusion**: There are already many individuals who have actually learned how to break into the systems and manipulate or destroy systems or network. Due to such threats, it has become important to build a system that is meant to protect the network from intrusion. UCBs may ensure the following minimum practices for availability and integrity of network.

• If remote login is enabled then make sure that users logging on from remote locations are identifiable by terminal IDs or IP addresses.
• Ensure for the firewall is in place and all internet connections are routed through a firewall.
• Ensure for the administrators monitor any attempts to violate the security policy using the audit logs generated by the application level firewall.
• Maintain a comprehensive list of what may be allowed or disallowed through the firewall.
• Ensure for the network is featured with entry or exit point to prevent through any network port that is not required by UCBs.
• For internal communication make use of intranet.
• Ensure for email attachment filtering process is in place.
• Ensure for all systems on network are featured with automated vulnerability scanning software to prevent and detect the intrusion.
• Ensure for the latest patches and updates relating to firewall product is tested and installed. If patches and updates are automatically downloaded from the vendor's websites, ensure that the update is received from a trusted site.
• Maintain a server list that details all the servers on network. At a minimum it may include name, purpose, IP address, date of service, service tag (if physical), rack location or default host, operating system, and responsible person.
• Ensure for all servers run antivirus software and report to the central management.
10. **Data center for high availability and integrity of data:** IT operations are a critical aspect of most UCBs. One of the main concerns is business continuity. If a system becomes unavailable, then UCBs operations may be interrupted. Therefore it is necessary to provide a reliable infrastructure for IT operations, in order to minimize any chance of disruption. Information security is also a concern. A data center is one of the most reliable, effective and efficient methods for high availability and integrity of data. In today's ever-growing regulatory compliance landscape, UCBs would greatly benefit from implementing possible and proven data center security best practices as listed below:

- UCBs need to build their own data center and DR site for business continuity and integrity of data and transactions.
- While selecting a location for data center and DR site UCBs need to limit the risk of exposure from internal and external threats. The selection process may include a review of the surrounding area to determine if it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards.
- Ensure physical and environmental security at data centre and disaster site as mentioned in Para 7.
- All security systems need to be monitored 24 X 7 and activities logged both onsite and at a remote location.
- It is suggested for those UCBs functioning without their own data center and depends on backup media for data backup may ensure that regardless of format data are stored securely and backed up or copied regularly. It is suggested to keep at least 3 copies of data, for example, original, external/local, and external/remote, and have a policy for maintaining regular backups.
- Make sure data backup is scheduled automatically twice a day.
- Ensure the accountability of data backup.
- The traditional data center design can be a time-consuming and difficult process for small size UCBs. As compared to a traditional data center, the small server room can be one of the options for data backup for small size UCBs. Small server room occupies fifty percent less floor space, thus provide cost efficiencies. It is also easy to relocate such type of data center.
whenever required.

- Cloud service as an option for data center: Cloud computing is an emerging option for cost effective and flexible solution for computing needs of UCBs. Many large urban cooperative banks offering cloud based services on private cloud environment. The UCBs who cannot afford the establishment and maintenance cost of their own data center may hire cloud based data center service from such UCBs. As cloud computing is an emerging technology standards, technology management processes are still evolving the UCBs need to take at most precaution while adopting cloud services.

11. Appropriate procedure and practices for business continuity management:

Business continuity management is one of the most critical components of any recovery strategy. The UCBs need to design and develop a procedure for business continuity management (BCM) to ensure that critical business functions can be maintained or restored as quickly as possible in the event of internal or external incidents. UCBs have to implement BCM to minimize the financial, legal and reputational risk. The business continuity plans must cover perquisites for IT, data and communications as well as for essential personnel and offsite locations.

- UCB may define critical business processes and resources and also define the impact of the failure of one or more critical resources on business.
- UCBs may employ high availability designs for IT systems, networks etc. supporting critical business processes.
- Regular reviews of business continuity plans may be conducted to ensure that they are up-to-date, implementable and effective.
- Make sure that members of the crisis or incident management and recovery teams and other relevant staff are aware of the plans and are clear on their personal roles and responsibilities.
- Carry out regular exercise or test to ensure that business continuity plans are remaining up to date and effective and are able to recover the business process in event of disaster.
12. **Cryptographic controls for high level of security in business process:** On-line transaction always needs a high end security to maintain the privacy of the transaction on internet. Cryptographic is one of the methods used to ensure that all business or customer’s transactions are processed securely. Information related to banks and customers is exchanged over networks. Without effective encryption techniques, transaction may be vulnerable to hackers or attackers. The security of electronic transactions can be achieved effectively with cryptographic techniques through digital signature based on public key cryptography. It is suggested that UCBs on priority may go for implementation of cryptography techniques through digital signature to secure online business transactions as well as customer’s banking transaction such as withdrawal, deposit payments and also SMS based mobile banking.

13. **Penetration test to identify security vulnerabilities:** UCBs may conduct periodic penetration test to identify security vulnerabilities and then take countermeasures before a real attack takes place. Both automated tools and manual techniques are used to simulate an attack and find existing vulnerabilities. For automated testing industry standards vulnerability scanning tools are available and UCBs may make use of these tools to identify vulnerabilities. After completion of a penetration testing a detailed report of a vulnerability assessment has to be prepared. UCBs may make use of following method for penetration testing:

   - Attempting to guess passwords using password-cracking tools.
   - Search for back door traps in the programs.
   - Attempt to overload the system using Distributed Denial of Service (DDoS) & Denial of Service (DoS) attacks.

14. **Security controls at remote ATM center:** Crime at ATM’s has become a nationwide issue that is faced not only by customers, but also bank’s operators. The urban cooperative banks needs to meet certain standards in order to ensure a safe and secured banking environment for their customers.

   - Ensure for ATM has dual control.
   - Ensure for surveillance camera positioned to record criminal activity at
and around the ATM.

- If a remote ATM, guarantee that the service equipped with a silent robbery alarm, telephone, or other means of communication with law enforcement official.
- Make sure that the service entrance is equipped with a viewing port or closed-circuit television system that allows personnel inside the service room to view activity outside.
- Provide customers with adequate privacy to prevent bystanders from observing details of their transactions (e.g. entry of their pin numbers)
- Appoint security guard at the ATM.
- Deploy an alarm system in ATM center in case of emergency.
- Ensure for the entrance door of ATM center is closed down only by authorized person.
- Create awareness amongst customers regarding the security at ATM and how to respond in case of attacks at ATM centers.

15. **Update the patches:** Patch management procedures needs to be followed by UCBs to assure the integrity and security of the computer network. Patches often repair security vulnerabilities through which attackers may gain access to systems running the affected software. Not applying patches leaves systems gets exposed. Therefore UCBs installed patch management software or vulnerability assessment tools to repair the vulnerability and regularly update the patches for effective execution of CBS solution.

16. **Best practices for information security management:** To fulfill the regulatory compliance urban cooperative banks may implement information security system as recommended by industry recommended standards to mitigate the risk and to ensure the effective availability and integrity of data and transaction. The urban cooperative banks may implement ISO 27001 based information security management system (ISMS) best practices for CBS environment. The UCBs may implement ISO/IEC 27002:2005 Code of Practice for Information Security Management. Additionally, other industry recommended security/IT control
frameworks such as COBIT (Information Technology management and IT governance) may also be considered by urban cooperative banks.

6.6 Designed and suggested proposed information security framework

In the past two years, urban cooperative banks have experienced a number of security breaches. These incidents have raised uncertainties on the environment of information security and security controls. India is home of large number of urban cooperative banks. These urban cooperative banks are facing challenges in many aspects such as information security, and they are trying to transform themselves in a complex business environment. With the growth of mobile banking and internet banking customers are becoming more and more technology savvy and looking for secure and extended services. Tough competition is also putting urban cooperative banks under pressure to become more competent and responsive. At the same time, urban cooperative banks are looking for different solution to reduce operating costs. In short, urban cooperative banks need to scale up their IT and improve operational efficiency in order to deliver reliable, continuous services in a cost effective and secure manner. The government-wide adoption of common policy, standards, guidelines and processes for information security including data classification and management enables the UCB’s to reduce the risk of inappropriate information access.

To address the situation, RBI has set up benchmarks, standards and legal regulations on information security to help UCBs to ensure an adequate level of security is maintained, resources are used in the appropriate manner, and the best information security practices are adopted.

6.6.1 “Comprehensive layered information security framework for CBS solution environment of UCBs:

An information security framework is a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment. These frameworks are basically a "blueprint" for building an information security programmes to manage risk and reduce vulnerabilities. Information security
framework may to define and prioritize the tasks required to build security into a UCBs. The frameworks are often customized to solve specific information security problems.

A comprehensive information security framework makes use three basic components: people, process and technology. When these three basic components are appropriately managed to secure the environment and then the information security remain consistent with business objectives. A comprehensive security framework based on these three components and may also ensure policy definition, enforcement, measurement, monitoring, and reporting for each one of the components. However, because defining and implementing policies alone cannot ensure security, the framework may also:

1. Identify risks to confidentiality, integrity, and availability for different business functions,
2. Reduce, transfer, or accept those risks.

The researcher had designed comprehensive layer information security framework that UCBs may use either as a starting point for a new security program or as a blueprint for assessing UCBs current security program.

The goal of designing information security framework is to ensure Confidentiality, Integrity and Availability (CIA) of information and information system and minimise the business operational as well as reputation risk. An effort was therefore made by the researcher to design such framework which will ensure CIA.

An effective information security framework cannot be implemented in isolation. It is essential that all resources which make potential information security program have to be sufficiently provided by the management. These resources include personnel, effective and efficient IT systems, good vendor management policies, and quality IT audit mechanisms. Costs are associated with these but the benefits enlarge on account of reduced IT security breaches.

Based on the suggestions, the researcher has designed proposed layered framework for Information security in CBS solution environment of UCBs. While designing the
proposed framework, the researcher has also considered the key standards in ISO 27001, whose main objective is to help the UCBs to establish and maintain an effective information security management system. The standard covers all the main security issues from a manager’s viewpoint and goes into significant depth in explaining good practice. The standard is divided into ten main information security domains. Each of which is key for maintaining security. These are:

1. Security policy
2. Organizational security
3. Asset management
4. Human resource security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. System development and maintenance
9. Business continuity management
10. Regulatory Compliance
11. Incident Management

An information security framework is designed based on the above information security domains and including people, process and technology to form comprehensive layer information security framework. The information security framework is designed to help UCBs to meet the challenge of information security that corresponds to the threats, risks and business demands they face, at the same time suggesting procedure for improving security levels. The researcher therefore has presented “Comprehensive layered information security framework” for CBS solution environment of UCBs. In this proposed framework researcher defines three layers Management Layer, Operational Layer and Technical Layer. The Figure 6.1 presents the comprehensive layered information security framework.

This layered framework suggests is - Plan, Do, Check, Act cycle (PDCA cycle) (ISO, 2005) cycle within the UCB’s:

1. **Plan (Deign):** Establish information security management system (ISMS) policy, objectives, processes and procedures relevant to managing risk and improving
information security to deliver results in accordance with an UCB’s overall policies and objectives.

2. Do (Implement and operate): Implement and operate the ISMS policy, controls, processes and procedures.

3. Checks (Monitors and Review): Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.

4. Act (Maintain and Improve): Take corrective and preventive actions, based on the results of the internal audit and management review or other relevant information, to achieve continual improvement of the ISMS.

The three layers countermeasures are some of the basic methods used to maintain the Confidentiality, Integrity, and Availability information and data. Each of these layer of the framework focuses on defining adequate levels of information protection strategies and designing and implementing the appropriate controls to transform the UCB’s from its current state of information security to the desired state. This transformation includes controls that concern to the people, process and technology dimensions to ensure that a holistic approach to information security is achieved. The Figure 6.1 shows the comprehensive layered information security framework for CBS solution environment of UCBs. This proposed framework is divided into three different layers for effective management of information security to ensure Confidentiality, Integrity and Availability.

1. Management Layer
2. Operation Layer
3. Technical Layer

The first layer deals with the management layer, which contains factors determining the business drivers of security. These include Technology Strategy and Usage, Business Initiatives and Processes and Threats, Vulnerabilities and Risk and Security policy. All these combined forms a unique Security plan of the UCBs. The plan needs to be reflected in the operational and Technical layer with operational and technical controls. The second is operational layer and the last layer is technical layer.
Figure 6.1: Comprehensive layered information security framework for CBS solution environment of UCBs
Layer 1: Management Layer

Management support is most important criteria for the successful implementation of information security program. The primary concerns of UCB’s decision makers are to increase profitability, control the new plan and minimise the risk. To achieve this in core banking environment management of UCBs needs to plan for information security as information is an important asset. Therefore information security is a basic requirement for the success of core banking in UCBs. Therefore the responsibility for managing information security is born by top level management, which provide the resources and sets the requirements which IT security manager support and control the information security activities. In management layer management controls for information security are defined. These management controls are the backbone of information security program. The management controls provides a support and continuing phase of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the controls. The information security program must be in-line with the business objectives and requirements. Therefore before implementation of information security program the management of UCBs have to define the business objectives. Based on the business objectives risk assessments have to be conducted. They may document an information security plan that show proper concern in securing their assets by meeting the objectives of policy statement. The management may form information security committee and the committee is responsible for the overall control of information security program and is responsible for:

1. Alignment of information security program with business objectives
2. Information security risk assessment
3. Defining control procedure for regulatory compliance
4. Synchronize the development and maintenance and review of information security policy, procedure and standards
5. Document critical assets and the controls that are implemented for each of them.
6. Identify the roles and responsibilities for information security
7. Conduct the training and awareness program on information security
8. Define the procedure for business continuity management and incidents management
9. Control procedure for information security audit planning and conduction
10. Monitor and review information security program regularly
11. Information security policy reinforcements

Layer 2: Operational Layer
Operational layer includes appropriate security controls and operational best practices for the physical security, network, information systems, applications, and information throughout the UCBs CBS solution environment. These controls may be defined, implemented, maintained to ensure the confidentiality, integrity and availability of information and include the following:

a. Monitoring controls that define the event information that will be recorded and monitored, and alert system that is used to trigger for incident response. These controls may be defined, implemented, maintained, and includes the following:
   - A Logging process for application, system, and network activity
   - A monitoring capability for critical systems
   - An intrusion detection system

b. Physical controls that define the process and system for protecting the physical facilities such as data center, physical assets, equipments, network and critical information systems. These controls may be defined, implemented, maintained, and include physical protection and access processes for buildings that house critical information, technology and systems.

c. Asset identification controls defines the planning and operational procedures related to asset inventory, accountability, responsibility, and information classification. These controls may be defined, implemented, and maintained to identify, inventory, assign ownership, and classify information and information systems.

d. Network Security controls defines the security controls for protecting the network. It may include the appropriate security controls and operational best practices for
the UCBs CBS networks security. These controls may be defined, implemented, maintained by UCBs and may include the following:

- Access control system
- A malicious code and unauthorized software countermeasure process
- Firewall and internet control process
- Configuration management process
- Security testing procedure
- Defining controls procedure based on roles and responsibility

**Layer 3: Technical Layer**

The technical layer defines the technical security controls and access controls to restrict access to CBS information in accordance with the information security and privacy policies and standards. The technical security controls are defined for authentication, authorization, accounting and auditing. Identification and Authentication are critical building blocks of information security since they are the basis types of access control and for ascertaining user accountability. Identification and Authentication are technical measures that prevent unauthorized people (or unauthorized processes) from entering an automated information system. Access control usually requires that the system be able to identify and differentiate among users. Access control is based on least privilege, which refers to the granting access to users for only those are required to perform their duties. User accountability requires the linking of activities on a system to specific individuals and therefore, requires the system to identify users. These controls may be defined, implemented, maintained by UCBs and may include the following:

- An access authorization process for all users and information systems
- An authentication mechanism for all authorized users and information systems
- Network, system, and application level access controls protection measures.
- Access controls for system development and maintenance
- Access controls for secure communication and operations management

A detailed suggested methodology for the implementation of information security protection framework was suggested based on above mentioned countermeasures, which helps the UCBs to implement information security program from the points of technology, management, and operation.
6.6 Scope for further Research:

Based on knowledge gained during the study by the researcher for information security and scope covered for the study, the researcher has identified certain important areas related to information security for UCBs and broad areas identified are as given below.

1. IT Security Risk assessment & Risk Management for UCBs
2. Technology intervention and role of stakeholders in optimizing technology usage for UCBs.
3. Virtualization, digitization and paperless banking through technology for UCBs
4. IT Governance preparedness with Business Intelligence & challenges in technology driven banking environment for UCBs
5. Integration of technology based non-banking modules in banking application