ABSTRACT OF THESIS
On
“A STUDY OF INFORMATION SECURITY SYSTEMS FOR CORE BANKING IN URBAN CO-OPERATIVE BANKS OF PUNE & MUMBAI”

A Thesis Submitted To
UNIVERSITY OF PUNE

For The Degree Of
(DOCTOR OF PHILOSOPHY)

In The
FACULTY OF COMPUTER MANAGEMENT

Submitted By
RAJESHRREE T. KHENAT

Under The Guidance Of
DR. YASHWANT S. PATIL
Associate Professor and Head, Center for Information Technology,
VAMNICOM

RESEARCH CENTER
Vaikunth Mehta National Institute of Cooperative Management University Road, Ganeshkhind,
Pune-411007

AUGUST 2014
ABSTRACT
ON
“A STUDY OF INFORMATION SECURITY SYSTEMS FOR CORE BANKING IN URBAN CO-OPERATIVE BANKS OF PUNE & MUMBAI”

1. Introduction
The Information Technology revolution has had a great impact on the Indian banking system. It has undergone many a transformation and CORE banking is the latest in the list of such transformations. CORE or online banking has brought a 360 degree change in the entire banking industry. There are many threats that prevent a person from using online banking. The threats are also being faced by banking channels of developed countries. Threats include Phishing, viruses, theft of user identity and password through etc. Bankers are fully dependent upon Information Technology for survival and the need to protect information and mitigate risk is more paramount than ever before. The various national surveys confirm a high number of attacks against organizations information resources. The incidents are frequent and also expensive; management must take security seriously to protect their critical organizational and customer information.

The purpose of this study is to explore and assess information security system of Urban Cooperative Banks that have been implemented CORE banking solution. The overall purpose of this research study was to examine as well as extend the body of knowledge and understanding regarding information security system in UCB’s who have adopted CORE banking solution.

2. Chapter wise Brief Introduction
This study is organized into six chapters.

- **Chapter 1: Urban Cooperative Bank and Information Technology Implementation**, Provides an overview of cooperative banks and role of IT in the development of UCBs.

- **Chapter 2: Review of Literature**, Depicts an overview of existing literature on information security systems and online banking.
- **Chapter 3: Research Methodology**, Illustrates details of research methodology used in performing this research which consist of an overview of the whole research work.
- **Chapter 5: Data Analysis and Interpretation**, present data analysis and interpretation into four parts. It also discusses the pilot study, validity and reliability of the research data.
- **Chapter 6: Findings and Suggestions**, Propose suggestion derived from research data analysis and interpretations as well as conclusions. At the end of the thesis document, a set of references and appendices are included.

### 3. Objectives of the Study

This study aims to achieve the following objectives:

1. To study the present status of overall Information Security Systems of Urban Cooperative Banks (UCBs).
2. To find the gaps in the existing Information Security Systems of UCB’s.
3. To assess the applicability of Security Standard of Information Security System in UCB’s.
4. To study the awareness of Information Security Systems amongst end users of UCB’s.
5. To suggest the effective Information Security System Framework for UCB’s.

### 4. Hypothesis of the Study

Based on the above mentioned objectives following hypothesis is framed

1. The level of Information Security in urban cooperative banks is in infancy stage.

Based on the above main hypothesis following workable information security domain wise sub hypotheses were framed.

1.1 The information security implementation in core banking of UCBs does not comply with information security standards applicable.
1.2 The information security in core banking of UCBs does not comply with the information security policy.

1.3 UCB’s does not ensure adequate Physical Access and environmental security controls in CBS solution environment.

1.4 UCB’s does not ensure adequate Data security measures in CBS solution environment.

1.5 End users of UCB’s have positive attitude towards training and awareness program conducted by UCBs.

1.6 The password security awareness at all management levels is high in UCBs.

5. Review of Literature

The sphere of the research study is mainly linked with information security in CORE banking, security standards and urban cooperative banks. Therefore the researcher has reviewed the literature focusing on these domains of the study. The literatures available to the researcher on the application of information security in Indian banks are classified according to cooperative banking and Information Technology, Information Technology in banking a global perspective, Online banking security issues: Global Scenario, Information Security, Information Security Standards and Various articles published in newspapers on information security. Researcher conducted an extensive review of the literature to identify the key attributes of information security and related issues and the gaps identified from the literature review are listed below:

<table>
<thead>
<tr>
<th>Risk management in cooperative banks.</th>
<th>Lack of knowledge and skills of the employees</th>
<th>Lack of Prevailing standards and solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of awareness amongst end users about the information security</td>
<td>Information Security Policy and procedure</td>
<td>Training and Education</td>
</tr>
<tr>
<td>Control Access to Information Systems</td>
<td>Physical Security and Environmental security</td>
<td>Information Security Management</td>
</tr>
<tr>
<td>Need Well-established Information Security Management System(ISMS)</td>
<td>Planning, management and monitoring of information security system</td>
<td>Security testing is still in its infancy stage</td>
</tr>
<tr>
<td>Network security is becoming more and more crucial.</td>
<td>Business Continuity Planning and Disaster Recovery Planning</td>
<td>Legal and regulatory framework</td>
</tr>
<tr>
<td>Virus protection software</td>
<td>Data Security</td>
<td>Encryption Techniques</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure communication</td>
</tr>
</tbody>
</table>
The existing research in information security related to online banking implementation showed that there is still lack of studies in the present literature about the information security in CORE banking environment in urban cooperative banks. The researcher also found that there is still an increasing need for comprehensive but specific approaches to information security aspects that would assist management in implementation of effective information security program not only in CORE banking environment of urban cooperative banks but providing the technology based solution including internet banking. It was found from the literature review that there was not a single study carried out on information security system for CBS environment in urban cooperative banks of Pune and Mumbai cities.

6. Research Methodology

The researcher has used survey based research methodology to carry out this research. The present study focuses on information security system in CBS environment of selected UCBs in Pune and Mumbai cities who have implemented CORE banking solution. This research study focuses mainly on assessment of information security system in CBS environment of UCBs. Both primary and secondary are used for this study. Secondary data is obtained through various kinds of documents such as research reports, RBI annual reports, books, articles, research papers from reputed journals and government regulation, and also from website.

- **Selection of Sampling Design:** The simple random sampling has been used for selection of target population i.e. selection of urban cooperative banks. The universe of the study is UCBs and the researcher has selected 18(40%) UCB’s out of 46 urban cooperative banks from Pune and Mumbai cities using simple random sampling method as shown in below table.

<table>
<thead>
<tr>
<th>Selection of Sample</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Population:</strong> Total Number Of UCB in Pune and Mumbai Cities implemented CBS</td>
<td><strong>Sample : Number of selected UCB for the Study (Target Population)</strong></td>
<td><strong>% of Population Sample</strong></td>
<td><strong>Sampling Technique</strong></td>
</tr>
<tr>
<td>46</td>
<td>18</td>
<td>40%</td>
<td>Probability Simple random sampling</td>
</tr>
</tbody>
</table>

Questionnaires were prepared for three different type of respondent (IT heads, the top Level Managements and End Users/Employees) to yield the necessary information.
Target Population and Sample Size: The researcher divided the entire population into three different strata top level management, IT heads and end users (employees of the UCB’s) and selected the final elements with disproportionate and purposive sampling method from the different strata. The researcher first organized the population by urban cooperative banks and then selected appropriate representation of top level management, IT heads and end users. The following table shows the target population and sample size.

<table>
<thead>
<tr>
<th>Sample Frame</th>
<th>Population</th>
<th>Sample Size</th>
<th>Sampling Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Heads</td>
<td>18</td>
<td>18</td>
<td>Disproportionate Stratified Random Sampling</td>
</tr>
<tr>
<td>Top Management/Board Of directors</td>
<td>240</td>
<td>18</td>
<td>Purposive Sampling</td>
</tr>
<tr>
<td>End Users/Employees</td>
<td>4710</td>
<td>472</td>
<td>Disproportionate Stratified Random Sampling</td>
</tr>
<tr>
<td>Total Sample Size</td>
<td>4948</td>
<td>507</td>
<td></td>
</tr>
</tbody>
</table>

The primary data collected are analyzed with the help of SPSS 16 (Statistical Package for the Social Sciences) and Microsoft Excel – 2007. Cronbach’s Alpha is used to assess the reliability of each of the instruments. The statistical techniques adopted are descriptive statistics such as frequency distribution, means and standard deviation and percentage. To test the hypothesis parametric test such as t-test, z-test was used. A nonparametric chi-square test was also used to test the hypotheses.

7. Analysis of the Data

The main objective of the study is to evaluate the information security controls adopted by UCB’s in CBS solution environment to protect the information and mitigate the risk. The analysis is carried into four parts after doing a pilot survey.

Part I: Data Analysis and Interpretation - Profile of respondents and UCBs

The data analysis and interpretation related to general information of UCBs such as number of branches, number of ATMs, total number of employees etc. and the respondents profile are presented in this section and this information support the first objective of the study.
1. **Demographics profile of UCBs:** The urban cooperative banking sector is characterised by heterogeneity in terms of type, number of branches, and number of employees, profitability and professionalism. It has been observed that Shamrao Vital Cooperative Bank, Mumbai is the oldest bank in selection list having maximum 140 branches in India, 64 branches in Mumbai and 14 branches in Pune with 821 employees. In this profile list Sarvodaya Co-operative Bank Ltd; Mumbai is at the last position because it is with minimum number of branches 4 in India, 4 branches in Mumbai and no branch in Pune with number of employees 70. It is also found that TJSB Sahakari bank, Mumbai has highest profit i.e. 7499 Lacs followed by Gopinath Patil Parsik Sahakari bank, Mumbai(2275 Lacs).

2. **Demographics profile of respondents (IT Heads):** The profile of IT heads are discussed as they are important element of CBS solution environment in implementing and monitoring the security solution. It was found that the highest 23.53% of the respondents are with 1 to 5 years of banking experience, whereas 5.88% respondents are with experience of 11 to 15 years. This indicates that the respondents are experienced in the field of banking business. Majority of the respondents 72.2% have commerce background and 27.8% respondent completed computer post graduation. It is observed that majority of the respondent’s i.e. 52.94% who are leading the IT department do not posses any type of software certification.

- **Part II: Data Analysis and Interpretation - Top level managements**

This section presents the data analysis and interpretation related to the top managements view regarding the CBS such as objectives behind implementation of CBS solution, age of CBS solution, budget provision for IT infrastructure or upgradation, existence of information security policy and conduction of information security audit and this information supports the first and second objectives of the study.

1. **Objectives for implementing CBS solution:** It has been observed that majority of the respondents i.e. 94.4% agreed with that the implementation of CBS solution improve MIS and standardization of process, improve 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.

2. **Age of CBS**: 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.

3. **Budget Provision**: 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.

4. **Information security policy**: 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.

5. **Conduction of IS audit**: It has be found that most of banks i.e. 61.11% do not
conducted IS audit. Only 38.89% banks indicated that the IS audit is conducted to
find out gaps in information security and to ensure integrity of the data.

6. **CBS performance satisfaction level**: When the respondents were requested to
rate their satisfaction level of CBS solution performance, 77.78% of the UCBs
stated that they are highly satisfied.

---

**Part III: Data Analysis and Interpretation - IT Heads**

Head of IT department is responsible for implementation and monitoring of the
security system in CBS solution environment. In this section the background
information of CBS solution and information security domains wise analysis of
data is presented and this information supports the first, second and third
objectives of the study.

1. **CBS solution environment background information**:  
   - It has been found that, 12 UCB’s are using fully developed and customized CBS
     solution which comes to 66.67 percent of total sample.
- It is observed that, 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
- It has been observed, 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.
- It was found that, 83.33 percent stated that they do not have escrow agreement in place for access to source code of CBS solution software.

2. **Physical and environmental security**
- 55.56 percent urban cooperative banks have deployed electronic access controls (access cards/Swipe-card) to restrict access to sensitive area.
- 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.
- 50 percent urban cooperative banks have not ensured such CCTV monitoring system.
- IDSs or IPSs (Intrusion Detection System/Intrusion Prevention System) are the solutions that include these requirements. 55.56 percent urban cooperative banks have not ensured the installation of Intruder Detection System to detect the network attacks.
- It was observed, 61.11 percent urban cooperative banks installed security locks to restrict access to the sensitive area like server rooms.
- 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.
- 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.
- 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 feed power supply, UPS, generator backup are in place.
3. Assets Management

- 88.89% UCBs have restricted access to sensitive area such as server room, data center; UPS room, backup server room etc.

- Majority of urban cooperative banks i.e. 89.79 percent have established registration process for new application system, hardware etc.

- 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.

- 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.

- 61.1 percent urban cooperative banks have maintained detailed inventory of information assets as per ISO standards.

4. Human Resources Security

- 77.80 percent urban cooperative banks have defined roles and responsibilities of personnel.

- 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.

- 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.

- 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.

- 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.

5. Access control
   - 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.
   - Majority i.e. 94.40 percent urban cooperative banks followed the segregation of duties to avoid the conflict and minimize the fraud.
   - 83.3 percent urban cooperative banks have defined business requirements for logical access control security.
   - 83.30 percent urban cooperative banks stated that they creates user ID created based on roles and responsibilities.
   - All the urban cooperative banks i.e. 100 percent provide individual password for accountability and password is changed on regular basis to avoid unauthorized access to information system. Similar percentage is supported for the passwords stored in encrypted form and password is not displayed on screen.
   - Majority of the UCBs i.e. 94.50 percent have controlled access to operating by secure log-on procedure.
   - It was observed from the statistical analysis that all the 18 urban cooperative banks i.e. 100 percent stated that system logout and screen logout facility is activated.
   - 88.90 percent urban cooperative banks indicated that inactive terminals are shut down/log off automatically after a defined period of inactivity.
   - Majority of the UCBs i.e 94.50 percent urban cooperative banks have carried out review of monitoring activity on regular basis.

6. Network security
   - The statistical findings revealed that 77.80 percent urban cooperative banks stated that they have implemented users logging from remote locations are identifiable by terminal IDs / IP addresses.
   - 66.70 percent urban cooperative banks stated that firewall is in use as per ISO standard.
- 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.
- 50 percent urban cooperative banks stated that they network prevent entry or exit through any network port that is not required by banks.
- 61.10 percent urban cooperative banks stated that filtering process is in place for email attachment to reduce the risk of systems.
- Remote login is enabled to access the system revealed by 72.2 percent urban cooperative banks.
- It has been found from the statistical data that 55.6 percent urban cooperative banks stated that they have automated vulnerability scanning tools for all systems on network.

7. **Cryptographic Controls**
   - 72.2 percent urban cooperative banks stated that cryptography key management is not in place to support the use of cryptographic techniques.

8. **Data Security**
   - 61.10 percent urban cooperative banks stated that they have their own data centre.
   - It was also found that, 94.40 percent urban cooperative banks have documented and tested data backup strategies and procedures.
   - It has been observed that 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.
   - 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.
   - 72.30 percent urban cooperative banks stated that data backup is scheduled automatically.
   - It has been also observed that 88.90 percent UCBs 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.
44.50 percent urban cooperative banks depend on disaster site for back up data, while over 55.50 percent urban cooperative banks does not have disaster site for data backup.

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.

9. **Business Continuity Management**

- 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.
- 50 percent urban cooperative banks review policies, procedures, standards and guidelines regularly for business community.
- 61.10 percent urban cooperative employed high availability designs for IT systems, networks etc. to support critical business processes.
- 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.
- It was observed that 55.60 percent urban cooperative banks have no single rational framework for business continuity planning in their urban cooperative banks.
- It has been found from the statistical data 61.10 percent urban cooperative banks follow adequate business continuity plans and the planning process to satisfy the identified information security requirements.
- 61.10 percent urban cooperative bank’s business continuity plans are regularly exercised or tested to ensure that they are remaining up to date and effective.

10. **Information security policy domains**

- 44.4 percent urban cooperative banks implemented patch management.
- It has been found 55.60 percent urban cooperative banks follow the best practice for configuration management.
- 38.9 percent urban cooperative banks have implemented the best practices for change control management.
- Only 22.2 percent urban cooperative banks have adopted computer forensics techniques to capture and maintain forensic evidence.
11. Periodic Penetration Testing
- It has been found that 55.6 percent UCBs do not conduct penetration testing on regular basis to indentify the gap in information security architecture

12. Viruses protection
- Majority of UCBs i.e. 94.4 percent have policy procedure is in place for virus protection.
- It has been also observed that all the urban cooperative banks under the study update antivirus software regularly.
- 94.4 percent urban cooperative bank’s computers external device is checked for viruses, worms and malwares.
- It has been found that 83.3 percent urban cooperative banks have ensured end user computer’s USB ports are locked.

13. ATM Security
- It has been found that 66.7 percent urban cooperative banks stated that to operate ATM, dual control is set up and similar number of urban cooperative bank’s ATM cash dispenser and depository shaft designed to prevent “fishing” and “trapping.
- 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.
- In addition, 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.
- 50 percent urban cooperative bank’s ATM provides customers with adequate privacy to prevent bystanders from observing details of their transactions.
- 72.20 percent urban cooperative banks revealed that security guard is appointed at the ATM centre.

14. Internet Banking Security
- 50 percent urban cooperative banks provided internet banking facility to their customer
It has been also observed 33.33 percent urban cooperative banks indicated that a security policy for internet banking was duly approved by the board of directors and was supported for two-factor authentication for fund transfers through internet banking.

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.

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.

88.89 percent urban cooperative bank’s CBS system application software maintains password length minimum 6 or 8 characters or with combinations of alpha, numeric and special characters.

15. Types of cyber attacks experienced by UCB’s

- It has been found that 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.

- 16.70 percent urban cooperative bank’s computer systems were experienced password sniffing and financial fraud.

- 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 UCBs.

- 5.6 percent urban cooperative banks agreed upon insider abuse of internet access or e-mail, Exploit of DNS server and instant messaging abuse.

- It is also observed that 16.70 percent urban cooperative banks stated that unauthorized access to the system by insider was taken place.

16. Regulatory Compliance

- It has been found that 72.2 percent urban cooperative banks have carried out implementation audit for CBS solution.

- 66.7 percent urban cooperative banks have carried out compliance audit for implementation audit.
17. Monitoring features of CBS solution

- It is found that 61.1 percent urban cooperative bank’s CBS is featured with comprehensive application logs with options for information, warning and critical message and alerts.
- 77.8 percent urban cooperative bank’s CBS solution is featured with monitoring of full usage statistics.

18. Applicability of information security standards

- 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.
- 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.
- It is also found that COBIT (IT Governance) standard is followed by 11.1 percent urban cooperative banks.
- 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.

Part IV Data Analysis and Interpretation- End Users (Employees)

The data regarding the employee’s perception about training and awareness program, information security awareness level are presented and analysed in this section. This information supports the fourth objective of the study.

1. Assessment of the training and awareness program on information security amongst the end users (Employees)

- It was observed that 72.5 percent respondents have positive approach towards management of UCBs conduct training and awareness program on information security. 55.1 percent respondents stated that the training program duration is one to seven days.
- Majority of the respondents’ i.e. 99.12 percent stated that the training program gives the better idea of information security.
- 45.91 percent of the respondents were highly satisfied, whereas 22.80 percent of
the respondents were highly dissatisfied with training and awareness program, 19 percent of the respondents were somewhat satisfied and 12.28 percent respondent were not answered.

2. **Perception of employees (end users) regarding awareness about information security**

- Majority of the respondents i.e. 93.3 percent has positive approach towards password protects system, service or programs.
- 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.
- It has been also observed that 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.
- 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.
- 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.
- 43 percent respondents stated that it is difficult to remember the password if changed regularly.
- It has been revealed that 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.
- It was observed that 37.1 percent respondents stated that they do have access to transfer the data to external storage device.
8. Testing of Hypothesis
Hypotheses were tested through mathematical and statistical tools.

- **Testing of hypothesis 1.1** “The information security implementation in core banking of UCBs does not comply with information security standards applicable.”

**Ho Null Hypothesis**: The information security implementations in core banking of UCBs comply with information security standards applicable.

**H1 Alternate Hypothesis**: The information security implementation in core banking of UCBs does not comply with information security standards applicable

**Test statistics**: One sample t-test at 5% level of significance

This hypothesis has been tested by using the information security standard applicable to CBS environment by means of percentage. The applicability of information security standard are tested using seven parameter such as ISO/IEC 27002:2005 (Code of Practice for Information Security Management), ISO/IEC 15408 (Evaluation Criteria for IT Security), ISO/IEC 13335 (IT Security Management), COBIT (Payment Card Industry Data Security Standard), ISO/IEC 20000 SERIES (Information Technology Infrastructure Library (ITIL)), ISACA Standards (IT Governance) and ISO 17799 (writing and implementing security policies). It has been observed from statistical analysis that out of total banks under the study 16.7% of the banks comply with information security standard such as ISO/IEC 27002:2005 (Code of Practice for Information Security Management).

The statistics for the t-test is shown in the above table. The one sample average t-test statistic is 8.594 and which is greater than 1.740 (table t –statistic) and the average p-value from this statistic is 0.000 which is less than 0.05 (the level of significance). Such a p-value indicates that reject H0 (Null hypothesis). Hence alternative hypothesis of the study “The information security implementation in core banking of UCBs does not comply with information security standards applicable” is accepted. **Hence the hypothesis of the study is accepted.**
Testing of Hypothesis 1.2 “The information security in core banking of UCBs does not comply with the information security policy”.

**Ho Null Hypothesis:** The information security in core banking of UCBs complies with the information security policy.

**H1 Alternate Hypothesis:** The information security in core banking of UCBs does not comply with the information security policy.

**Test statistics:** One sample t-test at 5% level of significance

This hypothesis has been tested by using the information security policy, procedure implemented by UCBs in CBS environment by using one sample t-test. It has been observed from the statistical analysis that most of banks i.e. 66.67% do not have IS policy in place for securing the CBS solution environment. Only 33.33% banks indicated that the information security policy is in place. The one sample t-test statistic is 5.831 and the p value remains 0.000 and this is less than 0.05 (the level of significance usually used for the test). Such a p-value indicates that reject H0 (Null hypothesis). Hence alternative hypothesis of the study “The information security in core banking of UCBs does not comply with the information security policy” is accepted. **Hence the hypothesis of the study is accepted.**

Testing Of Hypothesis 1.3 “UCB’s physical and environmental security controls in CBS solution environment are inadequate.”

**H0 Null Hypothesis:** UCB’s ensure adequate physical and environmental security controls in CBS solution environment.

**H1 Alternate Hypothesis:** UCB’s physical and environmental security controls in CBS solution environment are inadequate.

**Test statistics:** One sample t-test at 5% level of significance

This hypothesis has been tested by assessing the physical and environmental security controls implemented by UCB’s in CBS solution environment by using percentage. For testing this hypothesis, physical access and environmental security controls that are considered in the study are Electronic access control (access cards/swipe-card), biometric system, security guards, perimeter walls, CCTV/Web Camera, security locks, intruder detection system, information
security controls for natural disasters (like fire, earthquake, flood etc) risk, information controls for manmade disasters (like theft of information) risk, The power and telecommunications cabling, facilities like feed power supply, UPS, generator backups, network diagram and restricted access to sensitive area

The average t-statistics is 3.92 and p value is 0.003 which is less than 0.05. Such a p-value indicates that reject H0 (Null hypothesis). Hence alternative hypothesis of the study “UCB’s does not ensure adequate physical access and environmental security controls in CBS solution environment” is accepted. **Hence the hypothesis of the study is accepted.**

- **Testing Of Hypothesis 1.4 “UCB’s data security control measures in CBS solution environment are inadequate.”**

  **H0 Null Hypothesis:** UCB’s ensure adequate data security measures in CBS solution environment.

  **H1 Alternate Hypothesis:** UCB’s data security controls measures in CBS solution environment are inadequate.

  **Test statistics:** One sample t-test at 5% level of significance

This hypothesis has been tested by assessing the data security controls implemented by UCB’s in CBS solution environment by using percentage. The variable that are considered are backup strategies and procedures, strategies cover data, programs, system files, parameter files etc, backup media protected against loss, theft and damage, disaster site for back up data, data backup is scheduled automatically, physical and environmental security at data centre and disaster site, duplicate onsite backup of data and accountability of data backup.

The average p value is 0.001 and which is less than 0.05 for data backup strategies and procedure. Such p value indicates that reject H0 (Null hypothesis). Hence alternative hypothesis of the study “UCB’s data security control measures in CBS solution environment are inadequate.” is accepted. **Hence the hypothesis of the study is accepted.**
Testing Of Hypothesis 1.5 “End users of UCB’s have positive attitude towards training and awareness program conducted by UCBs.”

H0 Null Hypothesis: 73% or more employees (End Users) have positive attitude towards training and awareness program conducted by UCBs. (H0: p=0.73)

H1 Alternate Hypothesis: < 73% employees (End Users) do not have positive attitude towards training and awareness program conducted by UCBs. (H1 <0.73)

Test statistics: Z-test is used at 5% level of significance.

This hypothesis has been tested by using the training and awareness program conducted by UCB’s on information security for employee using percentage. It has been observed from the statistical analysis that the majority of the respondents i.e. 72.5 percent are positive attitude towards training and awareness program conducted by UCBs.

Table value of Z for one tail test at 5% level of significance is 1.64. Calculated value of Z(0.24) is less than the table value of z-statistics i.e. $Z_{cal} (0.24) < Z_{table}(1.64)$, hence accept H0 which means more than 73 percent respondents have a positive attitude towards management of UCBs conduct training and awareness program on information security. Hence hypothesis of the study is accepted.

Testing of Hypothesis 1.6 “The password security awareness at all level of management is high in UCBs.”

H0 Null Hypothesis: The password security awareness at all level of management is low in UCB.

H1 Alternate Hypothesis: The password security awareness at all level of management is high in UCBs.

Test statistics: chi-square Goodness of fit (One Sample Test)

This hypothesis has been tested by using Chi-square for password security awareness at all management level. Password security awareness is tested by checking the knowledge of end user regarding the password security standards, practices and guidelines. At the 5% level of significance calculated value of $\chi^2$ (214.851) is greater than table value of Chi-square (12.592) i.e. $\chi^2_{cal} (214.851) < \chi^2_{table} (12.592)$, hence null hypothesis is rejected and alternate hypothesis is
accepted. This means that the password security awareness at all level of management is high in UCBs. **Hence hypothesis of the study is accepted.**

- **Testing of main Hypothesis** "The level of information security urban cooperative banks is in infancy stage."

  The main hypothesis consists of six related sub hypothesis considering the major domains were tested with appropriate statistical tools and tests. The researcher on analysis observed that all the related sub hypothesis framed comply with the main hypothesis. From the testing of hypothesis it was observed that out of total six information security domains which are considered for testing the main hypothesis, four information security domains are inadequate to protect the information and information system. It was revealed from the hypothesis testing that:

  1. The CBS environment of UCB does not comply with information security standard applicable.
  2. The CBS environment of UCB does not comply with the information security policy, procedure and guidelines.
  3. UCB’s physical and environmental security controls in CBS solution environment are inadequate.
  4. UCB’s data security control measures in CBS solution environment are inadequate.
  5. End users of UCB’s have positive attitude towards training and awareness program conducted by UCBs.
  6. The password security awareness at all level of management is high in UCBs.

Therefore the main hypothesis of the study “The level of information security urban cooperative banks is in infancy stage” is accepted.

9. **Findings and Conclusions of the study**

- **Domain wise information security percentile of UCBs in CBS solution**
  - 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.
- 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.
- 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.
- 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.

Domain wise overall information security level of UCBs

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
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 solutions, 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.

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 solutions. These controls provide a high level of security and therefore minimize the risk of information security breaches in CBS solution environments.

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 solutions in CBS solutions. 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 domain 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.

- 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 following table 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 above it has been observed that out of total urban cooperative banks under the study only 2 UCBs i.e. 11% are implemented high level 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, cryptograghic 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 observations 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:

<table>
<thead>
<tr>
<th>View security as of little importance</th>
<th>Lack of Information Security Standard</th>
<th>Budget constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non existence of escrow agreement</td>
<td>Lack of information security policies and procedures in place</td>
<td>Inadequate physical and environmental security controls</td>
</tr>
<tr>
<td>Inadequate access control procedure</td>
<td>Weakness in Network Security</td>
<td>Absence of adequate cryptography controls</td>
</tr>
<tr>
<td>Data security controls with non compliance to recommended standards</td>
<td>Poor implementation of security policies</td>
<td>Poor implementation of information Security controls</td>
</tr>
</tbody>
</table>

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.

10. Suggestions
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). With reference to explanation at findings and conclusions 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. Based on the findings and conclusion of the study the following suggestions are offered by the researcher:

- **Management of UCBs would provide support for design, develop and implementation of information security program:** 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. The management of UCBs have to define the business objectives. Based on the business goals, risk assessments have to be carried out.

- **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.

- **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.

- **Budget provision for up-gradation of IT infrastructure:** The urban cooperative banks, both large and small, include the information security budget in the overall budget.
IT budget. 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.

- **Escrow agreement for outsourced software:** 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.

- **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.

- **Adequate physical and environmental security:** 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 as mentioned below:
  - 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 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.

**Procedure for maintaining inventory of information assets:** The urban cooperative banks may ensure the detailed procedure for maintaining inventory of information assets and classification of assets as shown below:

- 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 and 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.

**Control systems to protect the computer network from intrusion:** 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. Also 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 and 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.

Data center for high availability and integrity of data: One of the main concerned of UCBs are 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. A data center is the one of the most reliable, effective and efficient method 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.
- 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 and 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.

**Appropriate procedure and practices for business continuity management:**
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.
- 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.
- 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.
- 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.
Cryptographic controls for high level of security in business process:
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. 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.

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.

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. Also 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.

- **Best practices for information security management:** To fulfil 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.

### 11. 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. The 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. 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.

#### 11.1 “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 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.

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. An information security framework is designed based on 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. This layered framework suggests is - Plan, Do, Check, Act cycle (PDCA cycle) (ISO, 2005) cycle within the UCB’s.
The below figure shows the comprehensive layered information security framework for CBS solution environment of UCBs.

Comprehensive layered information security framework for CBS solution environment of UCBs
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. This proposed framework is divided into three different layers for effective management of information security to ensure Confidentiality, Integrity and Availability.

1. **Management 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.

2. **Operation 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.

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.
12. 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 stake holders 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

Ms. Rajeshree Khenat       Dr. Yashwant S. Patil
Research Student           Research Guide