CHAPTER 3

RESEARCH

METHODOLOGY
CHAPTER 3
RESEARCH METHODOLOGY

3.1 Introduction:

“According to Wolf & Pant (2005) research activities are designed to discover knowledge aid in answering specific questions or issues.”

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. The use of computers has led to the introduction of CORE banking in India. The use of computers in the banking sector in India has increased many folds after the economic liberalisation of 1991 as the country's banking sector has been exposed to the world's market. The Indian banks were finding it difficult to compete with the international banks in terms of customer services without the use of information technology.

CORE (Centralised Online Real-time Environment) or online banking has brought a 360 degree change in the entire banking industry. In such scenario timing is no longer a constraint and customers can finish their day-to-day tasks easily whenever they have a time. This method has also made shopping and bill payment very easy and convenient. The long queues for these activities have now become history.

The online banking acts as a vehicle that delivers customer’s banking needs to right where they are. This vehicle brings to customer doorstep:

- Information and data related to account and transactions
- Facilities to give instructions, requests, applications to the banks
- Provision to transfer funds as per needs of the account holders

Information systems (IS) security is a critical issue faced by banks worldwide. One of the major concerns with respect to online banking is the safety of customer’s and bank’s data. There are set of regulations laid down by Reserve Bank of India that guide banks on the security aspects of online banking.
The banks are bound to maintain certain security policies related to CORE banking that are approved by the management of the banks. Further there are specifications related to use of updated technology for banking web sites and also the network and database is to be administered and tested on regular intervals by a separate department of the banks.

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 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 confirmed a high number of attacks against banks information resources. The incidents are frequent and costly; management must take security seriously to protect their critical organizational as well as customers information.

The purpose of this study is to explore information security system of urban cooperative banks those have implemented CORE banking solution. The selected methodology in this study was approached by descriptive research. This chapter aims to describe appropriate methodology for achieving of the research objectives. The overall purpose of this research study is 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. The researcher will design information security framework for UCB’s based on the findings, published literature, a conceptual model and hypotheses in relation to the information security of CORE banking. The research methodology has to be robust in order to minimize errors in data collection and analysis. The methodologies namely survey, interviews (telephonic, structured and unstructured) were chosen for data collection. This chapter describes the research purpose, research approach, research strategy, pilot study, and population of the study, instrumentations used for the study, data collection method, and data analysis procedures of the entire study.

3.2 Background of the study:

India is a home to large number of co-operative banks. The cooperatives, as economic enterprises and as self-help organizations, play a meaningful role in uplifting the
socio-economic conditions of their members and their local communities. Over the years, cooperative enterprises have successfully operated locally-owned people-centred businesses.

Many of the cooperative banks and regional rural banks may not have CORE Banking facility at present. With what RBI implies, these banks have to quickly introduce CORE banking. The cooperative banks in India are increasingly going for core banking solutions (CBS) and are introducing various payment channels in order to improve customer’s services. While many UCB’s have already deployed CBS, and some more are in the process of automation, they are often faced with issues of initial capital requirement.

As the technology is getting evolving new challenges faced by the banks are increasing and one of the major challenges is information security. If bank’s customer’s adopts the secure banking services of CORE banking, there are chances of them relying on these services. Following types of risk must be minimised by banks to maintain the confidentiality, integrity and availability of data and information. Hence the cooperative banks role is to implement globally accepted information security standard to minimise the risk.

- **Regulatory risk:** As the Internet allows services to be provided from anywhere in the world, there is a threat that banks will try to avoid regulation and supervision.

- **Legal risk:** Online banking carries considerable legal risks for banks. Banks can potentially expand the geographical scope of their services faster through online banking than through traditional banking. In some cases, however, they might not be fully versed in a jurisdiction's local laws and regulations before they begin to offer services there, either with a license or without a license if one is not required. When a license is not required, a virtual bank—lacking contact with its host country supervisor may find it even more difficult to stay abreast of regulatory changes. As a consequence, virtual banks could unknowingly violate customer protection laws, including data collection and privacy, and regulations on soliciting.

- **Operational risk:** The dependence on new technology to provide services makes security and system availability the central operational risk of core banking. The security threats can come from inside or outside of the system, so banking
regulators and supervisors must ensure that banks have appropriate practices in place to guarantee the confidentiality of data, as well as the integrity of the system and the data. The UCB’s security practices should be regularly tested and reviewed by outside experts to analyze network vulnerabilities and recovery preparedness. The management of operational risks should become an integral part of banks. The overall management team and supervisors need to include operational risks in their safety and soundness evaluations.

- **Reputational risk:** The breaches of security and disruptions to the system's availability can damage a bank's reputation. The more banks rely on electronic delivery channels, the greater the potential for reputational risks. The reputational risks also stem from customer misuse of security precautions or ignorance about the need for such precautions. The security risks can be amplified and may result in a loss of confidence in electronic delivery channels. The solution is customer’s education- a process in which regulators and supervisors can assist.

Financial institutions protect their information by instituting a security process that identifies risks, forms a strategy to manage the risks, implements the strategy, tests the implementation, and monitors the environment to control the risks. Information security enables a financial institution to meet its business objectives by implementing business systems with due consideration of information technology (IT). The banks meet this goal by striving to accomplish the following objectives.

- **Availability** - For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning properly. The high availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

- **Integrity of data or systems** - Ensure that information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.

- **Confidentiality** - Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals. For example, a credit card transaction on
the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Confidentiality is necessary (but not sufficient) for maintaining the privacy of the customer whose personal information a system holds.

- **Authenticity** - In computing, e-business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are authentic. It is also important for authenticity to validate that both parties involved are who they claim they are.

- **Non-repudiation** - In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. The electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

- **Accountability** - Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of the records.

- **Assurance** - Assurance addresses the processes, policies, and controls used to develop confidence that technical and operational security measures work as intended.

The six major activities involved in information security are:

1. Policy development.
2. Specification of roles and responsibilities.
3. Designing and developing a security control framework.
4. Implementing a solution.
5. Monitoring and awareness.
6. Training and education.
Any successful organization should have in place various security layers such as physical security, personal security, and operational security, application level security, database level security and network level security etc. to protect its operations.

In order to resolve the issues of information security in online banking the study has been undertaken by the industry and the academia. But, due to the vast nature of these issues in online banking, there is still a need for research and development in these fields. The study of information security systems for core banking in urban cooperative banks is worthwhile so that the quality of information system security in CBS environment of urban cooperative banks can be enhanced in future. The various studies were done on e-banking in developing countries but no study has been undertaken focusing on information security system for CORE banking solution in urban cooperative banks of India.

3.3 Statement of the problem:
Information security may be defined as the prevention of, and recovery from, unauthorized or undesirable destruction, modification, disclosure, or use of information and information resources, whether accidental or intentional. According to Pfleeger (1997), information security is the preservation of the confidentiality, integrity, and availability (CIA) of information and information resources. Information security maintains three basic services:
1. **Confidentiality** of sensitive information, which is concerned with preventing disclosure of information to unauthorized users.
2. **Integrity**, which is concerned with ensuring data, cannot be modified without authorizations.
3. **Availability**, which is concerned with ensuring information, must be available to authorized users whenever needed. (Pfleeger, 1997).

This research study intends to address a research problem i.e. How the Information Security Systems (ISS) protects information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction and data detraction in urban cooperative banks.
This research is concerned with effective information security management in urban cooperative banks of Pune and Mumbai cities who have adopted CORE banking solution. The core research problem that study addresses is:

“What different types of information security measure are to be deployed to be addressed or managed for effective information security system of selected urban cooperative banks of Pune and Mumbai cities context so that the Confidentiality, Integrity and Availability of data are maintained?”

The inspiration of this research is to resolve this problem and thereby provide useful suggestions for bank’s management and implementers of information security programs in CORE banking environment in the Pune and Mumbai cities.

3.4 Significance of the Study:

“Information security, as a recognized business activity, has come a long way in the past decade. The various factors have caused the discipline to mature and it has now attained its "license to operate" within the corporate and public sector environments, becoming one of the core business and organizational enablers.”

.................Richard Brown

Information is an asset like other important business assets and is essential to business and consequently needs to be properly protected. This is especially important in the increasingly interconnected business environment, where information is now exposed to growing numbers and wider variety of threats and vulnerabilities. The causes of damage such as malicious code, computer hacking, and denial of service attacks have become more widespread, more determined, and more and more complicated.

The information security is not an 'IT problem', it is a business issue. The compliance with legal and regulatory requirements is important. It provides a very good reason for reviewing information security practices, but it should not in itself be the only or even the main driver. If a business needs to survive then banks must grab the importance of information security and place appropriate information security controls and procedures to monitor those security controls.
The information security is a dynamic process. The attacks against the systems evolve as hackers and fraudsters continuously identify new ways to break through a bank's security shields. Thus, the most important part of an information security program is implementing processes to continuously assess security risks in order to allow banks to respond as quickly as possible with stronger controls.

The security standards and frameworks, such as the International Standard, ISO 27001, are increasingly being adopted by banks, third party service providers and business partners as proof of security credentials. The users are waking up for the security rights and expectations, causing public-facing organizations to tighten privacy policies.

The ISO 27001:2005 states three aspects of information security: organizational, technical and operational. This approach covers not only the IT department but the entire organization. The organizational aspects are security policy, organization of information security, asset management, human resources security, operational procedures and responsibilities, service delivery management, incident management, business continuity management, compliance, whereas technical and operational aspects are physical and environmental security, system planning and acceptance, protection against malicious code, data back-up, network security management, media handling, exchange of information, electronic commerce services, monitoring, access control, information system acquisition, development and maintenance.[1]

3.5 Research Questions:
As the result of preliminary literature review to gain the research objectives, the following research questions were framed:
1. How do urban cooperative banks manage information system security?
2. Which different types of information security domains are implemented in CORE banking environment?

3. How do urban cooperative banks monitor Information system security in CORE banking environment?
4. Does urban cooperative banks have IS policy in place and whether it is well documented?
5. Which of the different Security Measures is included in IS policy?
6. Do urban cooperative banks implement information system security of CORE banking as per information security standard?
7. Do urban cooperative banks conduct information security training and awareness program?

3.6 Objectives of the study:
The main objective of this research is to evaluate information and information processing security system for CBS of urban cooperative banks in Pune and Mumbai cities. This study is carried out to understand present status of overall information security systems of urban cooperative banks (UCBs). The study is also an attempt to evaluate different layer of information security such as Physical Security, Personal Security, Operational Security, and Application level Security, Database level Security and Network Level Security that are implemented and monitored. The results of the present study are expected to contribute literature on CORE banking information systems security. Thus on addressing the above stated research problem, 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.

Furthermore, this research is also expected to suggest effective information security framework and increase awareness of the information security challenges of CORE
banking and serve as a guide for future implementation of such systems with low level of technological infrastructure. This study is more or less a major due diligence exercise for all the UCBs implementing CORE Banking solution.

3.7 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 framed for the study following workable information security domain wise sub hypotheses were framed and the same were tested with collected primary data of 18 urban cooperative banks of Pune and Mumbai cities under the study.

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 information security policy.
1.3 UCB’s does not ensured adequate physical access and environmental security controls in CBS solution environment.
1.4 UCB’s does not ensured 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.

3.8 Scope of the Study:
The present study focuses on information security system in CBS environment of selected urban cooperative banks in Pune and Mumbai cities. The present study is conducted for UCBs who have implemented CORE banking solution.

The boundaries of the present study are described from different angles. First, the area of application under investigation in this study is the information security countermeasures in place in CORE banking of UCB’s. Second the investigation of information security system for CORE banking is limited in urban cooperative banks
of Pune and Mumbai cities. Although, in general sense, the notion of information security system of CORE banking is not restricted to specific banks, however, there is a reservation in terms of the practicality and applicability of technology implementation of information security system models that are established in the UCB’s and other banks of India. Finally, as mentioned earlier data for present study is obtained from a single study that focused on information security system in CORE banking of UCB’s, and from specific user group (i.e. Head of IT Department, Board of Directors/Management Staff and Banks staff/employees operating the CBS).

Geographical territory of the study:
Pune and Mumbai cities are locations of the study. The urban cooperative banks who have adopted CORE banking solutions within Pune and Mumbai cities were studied for the purpose of research. The data has been collected from 18 UCB’s of Pune and Mumbai cities. The map 3.1 depicts the location of study.

Map 3.1: Geographical area of study
3.9 Research Design, Research Approach and Strategy:
The researcher has used descriptive research to describe particular phenomena or relationships within a single group sample. The main goal of this type of research is to describe the data and characteristics of what is being studied. Thus a descriptive study generates a data on who, what, when, where, why and how pertaining to investigation of study. Descriptive designs are typically used as either pilot or preliminary studies and generally have rather basic statistical procedures. They are often more quantitative in nature, requiring questions as a data-collection method. The respondents are selected by means of randomized sampling methods. The Table No. 3.1 shows the research design.

<table>
<thead>
<tr>
<th>Population</th>
<th>All urban cooperative banks implemented CBS Solution (Pune &amp; Mumbai Cities)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling Unit</td>
<td>Every urban cooperative bank that has a core banking facility within the sample.</td>
</tr>
<tr>
<td>Sampling Frame</td>
<td>18 urban cooperative banks implemented CBS Solution (Pune &amp; Mumbai Cities) i.e. 40% of total population</td>
</tr>
<tr>
<td>Sampling design</td>
<td>Probability Random Sampling</td>
</tr>
<tr>
<td>Target population</td>
<td>Bank management members, IT heads, and End users (Employees) from each study unit.</td>
</tr>
</tbody>
</table>

3.10 Data Collection:
The data collection is essential part of research. The nature of data which is collected and used for this research is primary in nature. The relevant and required secondary data has been collected from journals, RBI annual reports, government regulation, magazines, and literature through various search engines.

3.10.1 Primary Data:
The primary data are those which are collected for the first time and which is original in nature. The primary data is a data that is gathered for a specific research in response to a particular problem through interviews, questionnaires or observations.
The primary data is collected from 18 urban cooperative bank’s management members, Information Security Officer (IT heads), and employees by a structured questionnaire. The researcher has also interviewed the Heads of the IT department of the respective urban cooperative banks in Pune and Mumbai cities.

The primary data was collected through three different set of questionnaire. The questionnaire contains the information of the selected urban cooperative banks, with the establishment year, number of branches in Pune and Mumbai, Information security Policy, Measures included for controlling and monitoring information security system such as Information Security Policy and Procedure, Physical Access Control and Environmental Security, Asset Management, Human Resources Security, Logical Access Control System, Network Security, Operating System Access Control, Cryptographic Controls, Training and Awareness Program, Data Backup, Business Continuity Management, ATM Security, Internet Banking security, Information System Security Technologies such as Anti-virus software, Firewall, Vulnerability / Patch Management, Static account logins / passwords, Smart cards and other one-time tokens and Biometrics System etc and the experiences of the UCBs with regard to information security related problems, Training and awareness, roles and responsibility.

3.10.2 Secondary Data:

The secondary data for this study was obtained from published documents and literature relevant to the study. The secondary data is obtained through various kinds of documents such as research reports, RBI annual reports, books and articles, research papers from online journals and Government regulation for core banking and also from web information.

For collecting secondary data the researcher has visited various libraries. A few of these libraries werejaykar Library (Pune University), VAMNICOM, British Library, Sinhgad Institute of Management Library, Sinhgad college of Engineering Library and Pune Zilla Nagari Sahakari Bank’s Association Ltd, Pune.
Also the secondary data regarding number of UCBs, number of employees in UCBs, total number of branches and number of ATMs, deposits and Advances etc. has been collected from reliable sources.

3.10.3 Tools of Data Collection:
The data collection is an important aspect of any type of research study. The inaccurate data collection can impact the results of a study and ultimately lead to invalid results. Research data are categorised as primary and secondary data. The primary data collected by the researcher using data collection techniques such as survey, interviews and observations. In order to efficiently use the survey method a questionnaire were developed.

a. Survey/Structure Questionnaire: The questionnaire is concise, pre-planned set of questions, designed to yield specific information to meet a particular need of research information about a related topic. This method of data collection is used because expense and time involved in interview are reduced by using questionnaires. Each respondent receives the same set of questions phrased in exactly the same way. The questionnaires therefore, yield data more comparable than information obtained through an interview. Two types of questionnaire open-ended and closed-ended were designed for the collection of primary data. Three different types of questionnaires set were prepared for three different types of respondents (IT heads, the top level managements and end users/employees) to yield the necessary information. All the questions are of objective type and of type dichotomous questions (yes/no type), rating scale questions, five point likert questions and also three point likert questions. The questionnaires were filled from respondents of urban cooperative bank those have implemented core banking solution from Pune and Mumbai cities by visiting head office and branches of the banks. During the visit some of the respondents were unable to fill the questionnaire because of their busy schedule so the questionnaires were also forwarded through e-mail.

1. Top Level Managements: This set of questionnaire was adopted by the researcher to help to answer the question related to information security policy documentation and training and awareness of staffs/employees, budget provision, general background information of UCBs, objectives behind
implementation of core banking solution, and overall information security level in CORE banking environment.

2. IT heads of UCBs: This set of questionnaire is designed to assess the security controls are in place in CBS environment. The researcher organized a questionnaire based on different 16 domains of information security. This questionnaire includes general information of Core Banking Solution (CBS), Modules of Core Banking Solution (CBS), Information security policy and procedure, Physical Access Control and Environmental Security, Asset Management, Human Resources Security, Logical Access Control System, Network Security, Operating System Access Control, Cryptographic Controls, Training and Awareness Program, Data Backup, Information System Security Technology, Business Continuity Management, ATM Security and Internet banking Security. Each security domain represents a subset of entire questionnaire.

3. End users (employees) assessment: The third set of questionnaire was developed to assess the information security awareness and training imparted by the top management of the banks regarding information security in CORE banking environment.

b. Interviews: In order to gather in-depth information about perceptions, insights, attitudes, experiences which could not be effectively covered through questionnaire an interview technique was used. This method was also adopted by the researcher to clarify ambiguities and incomplete answers follow up.

c. Observations: The observation method was adopted by the researcher to observe the infrastructure facility, physical access control system, information security technologies, data center security measures in place in CORE banking environment. This facilitated the researcher a better understanding of what is happening in the background. It helped the researcher to understand how things are organized and prioritized, how roles and responsibility of people are defined, and what the intellectual parameters of information security system are?
3.10.4 Sampling Design and Sample Size:

The research objective is translated into research questions that enable the researcher to identify the information needed. There are two types of sample design.

1. Probability sampling design
2. Non-Probability sampling design

It was impossible to study an entire population due to time constraint. The researcher therefore relied on sampling to acquire a section of the population to carry out the research study. It is important that the group selected be representative of the population, and not biased in a systematic manner. For this reason, randomization is employed to achieve an unbiased sample. The sampling design used for the study is probability sampling because element in the population have a known chance of being as subject in the sample. The probability sampling designs such as simple random, disproportionate stratified random sampling are used in this study.

a. Simple Random Sampling: The simple random sampling is the basic sampling technique where researcher selects a sample for study from a larger group (a population). Each individual is chosen entirely by chance and each member of the population has an equal chance of being included in the sample. Every possible sample of a given size has the same chance of selection.

The researcher has used random sampling method for selection of sample i.e. target population. The researcher has attempted almost 40% of the sample out of total population. The sample is urban cooperative banks (UCBs) who have implemented CORE banking solution from Pune and Mumbai cities. On carrying out field study the researcher found that there are total 46 urban cooperative banks in Pune and Mumbai who have implemented CORE banking solution. The researcher has selected 18 urban cooperative banks whose head offices are in Pune and Mumbai cities. This research is mainly based on primary data. The researcher gathered the information from Pune urban bank association and Reserve Bank of India website.

The simple random sampling has been used for selection of target population. There are total 46 urban cooperative banks in Pune and Mumbai cities who have implemented CORE banking solution. The probability sampling method is used
for the selection of individuals from the population so that they are representative of the population. The universe of the study is urban cooperative banks 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 Table No. 3.1. The random sampling is a scientific and most important method among all types of sampling methods. It is simplest possible sampling method and it is most appropriate when the population is more or less homogeneous with respect to the characteristics under study.

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

The researcher has administrated the questionnaires to these 22 urban cooperative banks that have been adopted CBS solution. Out of the 22 UCB’s selected for the study except 4 UCB’s reported to the complete satisfaction of the researcher and therefore sample of the study is 18 UCB’s. The profile of these selected UCB’s is shown in the Table No. 3.3.
b. Stratified random sampling: A stratified sampling is a sampling technique in which the researcher divided the entire target population into different subgroups, or strata, and selects randomly the final subjects proportionally or disproportionally from the different strata. This type of sampling is used when the researcher aim to attempt to highlight specific subgroups within the population. The researcher used a disproportionate stratification that considers the variance of the mutually exclusive strata to determine the sample size for each stratum and with the disproportionate stratification for those strata with \( n_h < N_h \) where \( N_h \) is the population size of stratum \( h \), researcher select a random sample of \( n_h \) out of \( N_h \) elements.

The researcher divided the entire population into three different strata i.e. representatives, top level management, IT heads and end users (empioeys 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. This technique helped the researcher to ensure that the adequate representation of elements from each stratum in the final sample. The table No. 3.4 depicts the target population and sample size.

**Table No. 3.4: Target Population & 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><strong>Total Sample Size</strong></td>
<td><strong>4948</strong></td>
<td><strong>507</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Sample Size Calculation:**

**Sample size =507 at 98% confidence level**

According to research division of the National Education Association has published a formula for determining sample size. (ROBERT V. KREJCIE (University of Minnesota, Duluth), DARYLE W. MORGAN (Texas A. & M. University)
Sample Size = 
\[ s = \frac{\chi^2 NP (1 - P)}{d^2 (N - 1)} + \chi^2 P (1 - P) \]

Where:

- \( s \): Required sample size
- \( \chi^2 \): The table value of chi-square for 1 degree of freedom at the 98% confidence level = 5.024
- \( N \): The population size = 4948
- \( P \): The population proportion (assumed to be .50 since this would provide the maximum sample size) = 0.50
- \( d \): The degree of accuracy expressed as a proportion (0.05)

It should be noted that as the population increases the sample size increases at a diminishing rate and remains relatively constant.

3.11 Limitations of the study:

- The study was limited to urban cooperative banks (Management members, Head of IT department and employees of urban cooperatives banks) in Pune and Mumbai cities (Maharashtra, India) who have implemented CORE banking solution.
- The study was focused on how information security systems and the information security standards are implemented and monitored in CORE banking environment.
- The study was limited Pune and Mumbai cities due to time constraint. However, the results said to be representative, a more accurate results may be possible if more areas are included in the study.
- The findings and conclusions of study are totally based on the primary data collected from UCBs.
- The present study has relied largely on quantitative methodology of data collection (though qualitative methodology was used to some extent) and is therefore restrictive. Therefore, more of qualitative methodology of data collection may be used to provide a more thorough understanding of the information security systems and standards in CORE banking environment.
collection may be undertaken in future for conquer of wider perspective to the present study.

- The customer’s are also playing an important role in securing their own financial information. The customer awareness and perception about the information security in CORE banking environment is equally important but it was beyond the scope of the study.

3.12 Reference period of the study:
The duration of study considered by the researcher is from 2010-2014.

3.13 Chapter Scheme:
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 UCB.

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, the background of the study, significance of the study, statement of the problem, objectives of the study, hypothesis of the study, scope of the study, data collection method, and how the study is organized.

Chapter 4: Conceptual Framework of Information Security & Core Banking, Present conceptual framework of information security, Information security standards & CORE banking.

Chapter 5: Data Analysis and Interpretation, present data analysis and interpretation and research findings obtained through this methodology. It also discusses the validity and reliability of the research results and hypothesis testing.
Chapter 6: Findings and Suggestions. Propose suggestions derived from research findings and analysis as well as conclusions of research work. At the end of the thesis document, a set of references and appendices are included.