A Study of Information System training controls in Urban cooperative banks in Pune

By

Dr Manik Kadam
PhD GuideAIMS,Pune-01 R
MSc,MBA,MPhil,PhD

Sadique Sache
esearch Scholar,AIMS,Pune-01
BE,MBA,MPhil,CISA

ABSTRACT:-
In the last few years the changes in the banking domain and related technology have been tremendous. To maintain their competitive advantage and legal requirements, banks have implemented various IT solutions. Most of the banks now have their entire data computerized. This computerization has given rise to new risk and issues and Information system security is now a major concern for all the banks. Organization need proper software training so that their employees can be highly proficient and successful utilizing new technology. It is recognized that the human connection is the weakest connection in the information security chain. Subsequently, there is an indispensable requirement for an underlying and continuous information security related training. The research paper is an attempt by the researcher to understand the status of existing information system security and application training status in Urban cooperative banks in Pune city

1.1 Introduction

Banks world over are increasingly being computerized and this trend is likely to continue for the years to come. Use of Information Technology has become crucial for the success and survival of Financial Institutions.

The pivotal role of Information Technology has increased the need for security and control of Information System.

It is recognized that the human connection is the weakest connection in the information security chain. Subsequently, there is an indispensable requirement for an underlying and continuous information security mindfulness program. The program might be occasionally refreshed keeping in view the changes in information security, dangers/vulnerabilities as well as the bank's information security system. There should be an instrument to track the viability of preparing programs through an evaluation/testing process composed on testing the comprehension of the important information security strategies, at first as well as on an occasional premise. Anytime of time, a bank needs to keep up a refreshed status on client preparing and mindfulness identifying with information security and the issue should be a vital motivation thing amid Information Security Committee gatherings.

Businesses develop various software to make the work easier, but little do they realize the problems encountered by the software users, because of the lack of sufficient knowledge in knowing the software. This ignorance of software usage is catering to various emotions like computer rage and resentment. Training the software users essentially involves utilizing built-in functionality, to personalize layouts and menus, to the employee’s roles and responsibilities in an organization. Employees belonging to different departments utilize software functionality in different ways to accomplish their tasks. Software training makes repetitive tasks quick and easy. It also organizes information in an orderly manner, for easy access. Many studies have been done that have analyzed the obstacles and challenges in implementing new software. One would think the biggest issue would be related to technology, product shortcomings, infrastructure, costs and internal politics. However, most have concluded that the number one obstacle is inadequate training.

Organization need proper software training so that their employees can be highly proficient and successful utilizing new technology

Right application software training provides the following advantage to the organization.

- Increased job satisfaction and morale among employees
- Increased employee motivation
- Increased efficiencies in processes, resulting in financial gain
- Increased capacity to adopt new technologies and methods
- Increased innovation in strategies and products
- Reduced employee turnover

The following points are covered as part of Application Software Training Control

- Different types of training
- Management of the training
- Instructor for the training
- Adequacy of the training for troubleshooting
- Awareness of steps to be carried in case of contingency

The Indian Banking System broadly made up of the commercial banking and the Co-operative banking. The State Bank of India and its subsidiaries, public sector banks, regional rural banks and private sector banks represent the commercial banking system. The State Co-operative bank at the apex level, District Co-operative Bank at the district level and primary agricultural credit societies at the grass root level represents the Co-operative banking.

With the winds of changes blowing, the Indian Banking system is also not untouched. Most of the banks, whether commercial or Co-operative, have tried to adjust to these changes in information and technology. Most of the Banks have computerized their operations with the advancement in technology. The concepts of e-banking, tele-banking, ATM's and online banking are now synonymous with most of the Indian Banks.

Since Urban Cooperative Banks are closer to the general public and because of the place specific and people specific nature, the researcher felt the need to understand the Information System security controls in the Urban Cooperative Banks.

1.2 Objectives of the Study

1. To understand the adequacy of the application software training provided to employees of Urban Cooperative Banks in Pune
2. To understand the training needs of the employees of Urban Cooperative Banks with regards to Information System security controls

1.3 Hypotheses

The Hypotheses for the research study are as follows: -

1. The employees of the Urban Cooperative Banks are provided adequate training on the application software
2. The employees of the Urban Cooperative Banks are not aware of the concept of security controls and need training

1.4 Research Methodology

The research is divided into two parts

a. Primary Research
b. Secondary Research

The following methodology will be used for undertaking Primary Research

1. **Questionnaire: -** A questionnaire under different headings was prepared to gather the primary information regarding the various training controls in the Urban Cooperative Banks.
2. **Personal interview and Discussion: -** Interviews and discussions were held with the various staff of the Urban Cooperative Banks to gather information to various question and queries in the questionnaire.
3. **Observation:**- It will be one of the most important methodology followed for gathering the information regarding the actual situation of the controls in the various Urban Cooperative Banks.

Sampling:- As per the annual report of 2015-16 of the Pune District Urban cooperative Banks Association Ltd. there are 32 Urban cooperative banks in Pune city. A stratified random sampling of 19 Urban Cooperative Banks has been taken for the research

The following methodology is used for undertaking Secondary Research

4. **Library: -** Initially referring books, reports and journals from libraries of University of Pune, AIMS, NIBM, VAICOM, Pune District Urban cooperative Banks Association Ltd etc. will be done to gather secondary information about the topic and to get an understanding of the various aspects of the subjects.
5. **Internet: -** The Internet will be surfed and the related sites on Information System security control like isaca.org, itgi.org, sans.org, www.rbi.org.in etc.

1.5 Hypothesis Testing

1.5.1 Hypothesis 1 :- The employees of the Urban Cooperative Banks are provided adequate training on the application software

1.5.1.1 Statistical test :- sign binomial test

1.5.1.2 Variables and measurement:- The bank system administrators were asked to provide information on the following areas related to the above hypothesis. The responses were later converted into 2-point scale (1= "Acceptable" and 2= "Not acceptable") using "The recode into different variable" command of IBM SPSS 21.

Level of significance $\alpha = 0.05$

Table 1-1 Hypothesis 1 statistical analysis

		Category	**N**	**Observed Prop.**	**Test Prop.**	**Exact Sig. (2-tailed)**
Are the users provided training on application system functioning	Group 1	Acceptable	19	1	0.50	p=0.000
	Group 2	Not Acceptable	0	0		
	Total		19	1.00		
Who provides the training	Group 1	Acceptable	16	0.84	0.50	p=0.04
	Group 2	Not Acceptable	3	0.16		
	Total		19	1.00		

Is adequate training in the technical details of the application system provided for necessary trouble shooting / help to users	Group 1	Not Acceptable	17	0.89	0.50	p=0.01
	Group 2	Acceptable	2	0.11		
	Total		19	1.00		

Finally, from the above table it can been seen in all the 3 control parameters, observed proportion is more than 0.5 and the p value is less than 0.05 and hence the null hypothesis is rejected and hypothesis *"*The employees of the Urban Cooperative Banks are not aware of the concept of security control and need training*"* is proved

1.5.2 Hypothesis 2:- *"*The employees of the Urban Cooperative Banks are not aware of the concept of security controls and need training"

1.5.2.1 Statistical test :- sign binomial test

1.5.2.2 Variables and measurement:- The bank system administrators were asked to provide information on the following areas related to the above hypothesis. The responses were later converted into 2-point scale (1= "Acceptable" and 2= "Not acceptable") using "The recode into different variable" command of IBM SPSS 21.

Level of significance $\alpha = 0.05$

Table 1-2 Hypothesis 1 statistical analysis

		Category	**N**	**Observed Prop.**	**Test Prop.**	**Exact Sig. (2-tailed)**
Have you gone through a Information system security training	Group 1	Not Acceptable	13	0.68	0.50	p=0.008
	Group 2	Acceptable	6	0.32		
	Total		19	1.00		
How do you remember your password	Group 1	Not Acceptable	14	0.74	0.50	p=0.000
	Group 2	Acceptable	5	0.26		
	Total		19	1.00		

Do you know Why do you need a more than 8 digit password with Alphanumeric character	Group 1	Not Acceptable	17	0.89	0.50	p=0.000
	Group 2	Acceptable	2	0.11		
	Total		19	1.00		
Have you read the security policy	Group 1	Not Acceptable	17	0.89	0.50	p=0.000
	Group 2	Acceptable	2	0.11		
	Total		19	1.00		
Are you aware of the steps to be carried in case of contingency due to non-availability of systems.	Group 1	Not Acceptable	14	0.74	0.50	p=0.000
	Group 2	Acceptable	5	0.26		
	Total		19	1.00		
Does the Employee wear identification badge	Group 1	Not Acceptable	16	0.84	0.50	p=0.000
	Group 2	Acceptable	3	0.16		
	Total		19	1.00		

Finally, from the above table it can been seen in all 6 control parameters, observed proportion is more than 0.5 and the p value is less than 0.05 and hence the null hypothesis is rejected and hypothesis *"*The employees of the Urban Cooperative Banks are not aware of the concept of security control and need training*"* is proved

1.6 Findings

1. In all the 19 banks under study in 100% banks users were provided training on application system functioning. Hence in all banks the users were provided training on application system functioning and the control was properly implemented and in tune with the best practices

2. Out of the 19 respondents, in 84 % banks the training was provided by the vendor and 16% cases the training wad provided by experienced employees. Hence in majority of the banks the training was provided by the vendor and the control was properly implemented and in tune with the best practices
3. Out of the 19 respondents, in 89 % banks employees said that adequate training was provided and 11% said they were not provided adequate training. Hence in majority of the banks adequate training in the technical details of the application system was provided for necessary trouble shooting / help to users and the control was properly implemented and in tune with the best practices
4. Out of the 19 respondents 31.6% banks employees said that they have undergone information system security related training and 68.4% said No. Hence majority of the banks did not provide training on Information System security to its employees and the control was not properly implemented
5. Out of the 19 respondents 26.3% banks employees memorize their password, 26.3% write it down in a secure place and 47.4% write it down close to the office table. Hence majority of the banks did not memorize their password and the control was not properly implemented
6. Out of the 57 respondents 26.5% bank employees responded that they are aware of the steps to be carried in case of contingency due to non-availability of systems and 73.5% said they were somewhat aware of the steps. Hence majority of the employee not fully aware of the steps to be carried out in case of contingency due to non-availability of systems and the control is not properly implemented

Recommendations and Suggestions

1. Identification badges establishes the identity of an employee of the organization. It also helps customers to identify the right person to reach out for their need. Hence it is very important to have identification badges. It is therefore strongly suggested that in cases where the employees are not provided the identification badges, the banks should provide the same at the earliest and ensure the employees wear them during office hours

Fig. 6-2 Notification for employees to wear ID Cards

2. If your personnel do not know or understand how to maintain confidentiality of information, or how to secure it appropriately, you not only risk having one of your most valuable business assets (information) mishandled, inappropriately used, or obtained by unauthorized persons, but also risk being in noncompliance of a growing number of laws and regulations that require certain types of information security and privacy awareness and training activities. You also risk damaging another valuable asset, your bank's reputation. In view of the same it is important the employees of the bank are provided proper training on information system security. It is seen from the study that most of the banks have neglected this area. It is therefore strongly suggested that employees be provided training in information system security on a periodic basic so as to emphasize on the importance of it.
3. It was observed that maximum employees were not aware of the steps to be carried in case of contingency due to non-availability of systems. Since availability of the information is utmost important in a banking scenario, the employees should be provided proper training on the steps they need to carry out in case of contingency due to non-availability of the system.

References

1.http://web.archive.org/web/20070903115947/http://www.sei.cmu.edu/publications/documents/03.reports/03tr002/03tr002glossary.html
2. Kroenke, D M. (2008). Experiencing MIS. Prentice-Hall, Upper Saddle River, NJ
3. O'Brien, J A. (2003). Introduction to information systems: essentials for the e-business enterprise. McGraw- Hill, Boston, MA
4. Alter, S. The Work System Method: Connecting People, Processes, and IT for Business Results. Works System Press, CA
5. Gordon B Davis, Olson Margrethe (2007) Management Information System, Tata Mcgraw-Hill, India
6. Kenneth C. Laudon and Jane P. Laudon (1998) Management Information Systems Organization and Technlogy, Printice-Hall,India
7. http://www.britannica.com/EBchecked/topic/287895/information-system
8. COBIT® 5 for Information Security ISBN 978-1-60420-255-7 Printed in the United States of America
9. http://en.wikipedia.org/wiki/Information_security
10. Nina Godbole (2009). Information systems security, Wiley India Pvt ltd, India
11. Ron Weber (2003) Information Systems Control and Audit, Pearson Education, India
12. T.N. Haliya (1998) Principle Problem and Practice of Cooperative Banks
13. Report on Trend and Progress of Banking in India 2011-12- Reserve Bank of India
14. Nov 17,2003 :- Overivew Reserve Bank of India
15. Annual report of Pune District Urban Co-Operative Banks Association Ltd. Year 1999-2000
16. http://www.dnb.co.in/bfsisectorinindia/BankC6.asp
17. Kakoli Saha (July-September 1986) Computerization in Banks: Implications for Organizational Development- Vikalpa Journal Vol 11
18. http://www.banknetindia.com/banking/bsoftware.htm
19. Keynote address Dr. Rakesh Mohan, the then Deputy Governor, RBI at the Conference on e-Security organised jointly by IBA and MAIT on July 30, 2004 at Mumbai.
20. Apr 30, 2004 : Information System Audit - A review of Policies and Practices, Reserve Bank of India. 21. Website www.isaca.org
22. Webste www.rbi.org.in
23. Annual reports of the banks under study.