A Study of Information System logical access controls for system administrator in urban cooperative banks in Pune

Sadique Sache
BE,MBA,MPhil,CISA
Research Scholar, AIMS,Pune.

Dr Manik Kadam
MSc,MBA,MPhil,PhD
Professor,MBA,AIMS,Pune.

1.1 :-ABSTRACT:-

Information technology has revolutionized the entire banking scenario in the word. Banks cannot afford to stay aloof from the winds of changes in the information technology. In the last few years the changes in the banking domain and related technology have been tremendous. Banks to maintain their competitive advantage and legal requirements, 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. The role of a system administrator has come to the forefront in this scenario. The system administrator is responsible for ensuring the CAI (Confidentially, Availability and Integrity of the data. The objective of this paper is to understand the various logical access controls for system administrator in urban cooperative banks in Pune

1.2:-**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. Information technology has broken the barriers of time, distance and speed and has dramatically changed the way transaction is done.

Computer based information system differ from manual record system, in the way of concentration of information. In a manual system, the information is scattered across different locations in various files and folders. However, in a computer system all the necessary records are maintained at a single site or computer. So, for someone to gain access to all the information of the bank, he needs to just get access to one machine. This concentration of information system assets and records also increases the losses that can arise from computer system disaster or

abuse. It is very well understood that the three pillars of information security are Confidentiality, Integrity and Availability (CIA) and it is the key role of the system administrator to ensure these 3 pillars remain intact for the smooth working of the bank.

Confidentiality :- refers to prevention of unauthorized disclosure of information whether intentional or unintentional. Protecting confidentiality hinges upon defining and enforcing appropriate access levels for information. Doing so often involves separating information into discrete collections organized by who should have access to it and how sensitive it is.

Integrity:- Integrity refers to the unauthorized modification of the data. An integral system ensures that changes to the data are made only by the authorized personnel. It also ensures that when authorized people make changes that shouldn't have been made the damage can be undone. The data is consistent across the system and there is no variation in it.

Availability :- This concept of Information security ensures that the information is available to authorized users as and when required. 'Availability' ensures the system is working properly and is up and running whenever the required information is sought.

The Indian Banking System broadly comprises 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.

As per the circular UBD. BPD.Cir.No. 71/12.09.000/2013-14, The Reserve Bank of India has advised Cooperative banks across India to introduce EDP Audit to mitigate the risks and issues arising from the adoption of computer technology. As per the circular, UCBs may adopt an IS audit policy, if not already done, appropriate to its level of operations, complexity of business and level of computerization and review the same at regular intervals in tune with guidelines issued by RBI from time to time. One of the key aspect of the EDP Audit is the validation of Information System Security Control.

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 logical access controls for system administrator in the Urban Cooperative Banks.

1.2 :-Objectives of the Study

1. To identify the various logical access controls for system administrator in Urban cooperative banks in Pune

1.3:- Hypothesis :- "The implementation of logical access controls for system administrator in Urban Cooperative Banks are satisfactory"

1.4.:-Research Methodology

The research is divided into two parts

a. Primary Research
b. Secondary Research

The following methodology is used for undertaking Primary Research

1. ***Questionnaire:*** **-** An exhaustive questionnaire was prepared to gather the primary information regarding the Information System logical access security 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 is one of the most important methodology followed for gathering the information regarding the actual situation of Information System logical access security controls in the various Urban Cooperative Banks.

The following methodology is used for undertaking Secondary Research

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

1.5:- Sampling:- As per the annual report of 2014-2015 of the Pune District Urban cooperative Banks Association Ltd. there around 36 cooperative banks in Pune. A random sampling of 19 Urban Cooperative Banks was taken for the research paper

1.6:- Hypothesis Testing

Hypothesis:- "The implementation of logical access controls for system administrator in Urban Cooperative Banks are satisfactory"

Purpose :- The purpose of the hypothesis is to understand the implementation of logical access control for system administrator

Statistical test: - sign binomial test

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.

Sr. No	Variable
1	Dedicated system administrator
2	Backup system administrator
3	Period for password change
4	Maximum length of the password acceptable
5	Minimum length of the password acceptable
6	Acceptance of alphanumeric characters
7	Acceptance of previous password as change password
8	Automatic disconnection of login session
9	Deactivation of logon ids not used for a number of days
10	Time for deactivation
11	Permanent deactivation of login ids with multiple attempts of incorrect password
12	Track of unsuccessful trails
13	Change of password on the first access to the system
14	Password of an employee who has been transferred
15	User groups creation
16	Restricted menu display for each user profile

Test proportion: - Test proportion was taken as 0.5. Since more than 50% of favorable responses to a category suggest greater approval for this category.

Hence P=0.5

H0 :- P<= 0.5 (Proportion of response indicating “The implementation of logical access controls for system administrator in Urban Cooperative Banks are satisfactory ” is less than or equal to 50%)

H1 :- P>0.5 (Proportion of response indicating “The implementation of logical access controls for system administrator in Urban Cooperative Banks are satisfactory ” is more than 50%)

Level of significance $\alpha = 0.05$

		Category	**N**	**Observed Prop.**	**Test Prop.**	**Exact Sig. (2-tailed)**
Who is the system administrator	Group 1	Not acceptable	3	0.16	0.5	p=0.04
	Group 2	Acceptable	16	0.84		
	Total		19	1		
Are there more than one system administrators	Group 1	Not acceptable	6	0.32	0.5	p=0.167
	Group 2	Acceptable	13	0.68		
	Total		19	1		
How often is the password for the system administrators changed	Group 1	Acceptable	16	0.84	0.5	p=0.004
	Group 2	Not acceptable	3	0.16		
	Total		19	1		
What is the maximum length of the password acceptable	Group 1	Acceptable	19	1	0.5	p=0.000
	Total		19	1		
What is the minimum length of the password acceptable	Group 1	Not acceptable	1	0.05	0.5	p=0.000
	Group 2	Acceptable	18	0.95		
	Total		19	1		

Does the password allows alphanumeric characters	Group 1	Acceptable	19	1	0.5	p=0.000
	Total		19	1		
Does the system allows a previous password as change password	Group 1	Acceptable	19	1	0.5	p=0.000
	Total		19	1		
Does the system automatically disconnects a login session if no activity has occurred for a period of time	Group 1	Acceptable	19	1	0.5	p=0.000
	Total		19	1		
Are logon ids not used for a number of days deactivated	Group 1	Acceptable	18	0.95	0.5	p=0.000
	Group 2	3	1	0.05		
	Total		19	1		
What is the time period	Group 1	Acceptable	17	0.89	0.5	p=0.001
	Group 2	Not acceptable	2	0.11		
	Total		19	1		
If a wrong password is entered for a predefined number of time is it permanently deactivated	Group 1	Not acceptable	3	0.16	0.5	p=0.004
	Group 2	Acceptable	16	0.84		
	Total		19	1		
Does the system	Group 1	Not acceptable	7	0.37	0.5	p=0.359

keeps track of unsuccessful trails	Group 2	Acceptable	12	0.63		
	Total		19	1		
Is a client forced to change his password on his first access to the system	Group 1	Acceptable	19	1	0.5	p=0.000
	Total		19	1		
What is done to the password of an employee who has been transferred	Group 1	Acceptable	15	0.79	05	p=0.019
	Group 2	Not acceptable	4	0.21		
	Total		19	1		
Are the user groups created	Group 1	Acceptable	19	1	0.5	p=0.000
	Total		19	1		
Is there a restricted menu display for each user profile	Group 1	Acceptable	19	1	0.5	p=0.000
	Total		19	1		

1.7:- Interpretation

1. Dedicated system administrator

Observed proportion: 0.84, Test proportion: 0.5 , $p<0.05$

Hence more than 50% of the banks have either a dedicated system administrator or the manager playing the role of system administrator which is an acceptable practice.

2. Backup system administrator

Observed proportion: 0.68, Test proportion: 0.5, $p>0.05$

Hence more than 50% of the banks have a backup system administrator which is an acceptable practice.

3. Period for password change

Observed proportion: 0.84, Test proportion: 0.5, $p<0.05$

Hence in more than 50% of the banks the password for system administrator is changed every month which is an acceptable practice.

4. Maximum length of the password acceptable

Observed proportion: 1, Test proportion: 0.5, $p<0.05$

Hence in more than 50% of the banks the maximum length of the password for system administrator is more than 8 digit which is an acceptable practice.

5. Minimum length of the password acceptable

Observed proportion: 0.95, Test proportion: 0.5, $p<0.05$

Hence in more than 50% of the banks the minimum length of the password for system administrator is more than 8 digit which is an acceptable practice.

6. Acceptance of alphanumeric characters

Observed proportion: 1.0, Test proportion: 0.5, $p<0.05$

Hence more than 50% of the banks mandate alpha-numeric password for system administrator which is an acceptable practice.

7. Acceptance of previous password as change password

Observed proportion: 1.0, Test proportion: 0.5, $p<0.05$

Hence more than 50% of the banks do not allow previous password as changed password for system administrator which is an acceptable practice.

8. Automatic disconnection of login session

Observed proportion: 1.0, Test proportion: 0.5, $p<0.05$

Hence in more than 50% of the banks the session automatically disconnects a logon session if no activity has occurred for a period of time which is an acceptable practice.

9. Deactivation of logon ids not used for a number of days,

Observed proportion: 0.95, Test proportion: 0.5, $p<0.05$

Hence in more than 50% of the banks logon ids not used for a number of days are deactivated either automatically or manually which is an acceptable practice.

10. Time for deactivation

Observed proportion: 0.84, Test proportion: 0.5, $p<0.05$

Hence in more than 50% of the banks logon ids not used for a number of days are deactivated either automatically or manually within an weeks' time which is an acceptable practice.

11. Permanent deactivation of login ids with multiple attempts of incorrect password

Observed proportion: 0.89, Test proportion: 0.5, $p<0.05$

Hence more than 50% of the permanently deactivate login ids or ensure user has to start logon again in cases of multiple attempts of incorrect password which is an acceptable practice.

12. Track of unsuccessful trails

Observed proportion: 0.63, Test proportion: 0.5, $p>0.05$

Hence more than 50% of the banks track unsuccessful trails which is an acceptable practice.

13. Change of password on the first access to the system, $p<0.05$

Observed proportion: 1.0, Test proportion: 0.5, $p<0.05$

Hence more than 50% of the banks ensure the system administrator change the password on the first access to the system which is an acceptable practice.

14. Logon id of an employee who has been transferred

Observed proportion: 0.79, Test proportion: 0.5, $p<0.05$

Hence more than 50% of the banks deactivate login id of employee who has been transferred which is an acceptable practice.

15. User groups creation

Observed proportion: 1.0, Test proportion: 0.5, $p<0.05$

Hence more than 50% of the banks have created user groups which is an acceptable practice.

16. Restricted menu display for each user

Observed proportion: 1.0, Test proportion: 0.5, $p<0.05$

Hence more than 50% of the banks have restricted menu displayed for each user which is an acceptable practice.

1.8Conclusion:- From the above discussion, it can been seen that for all the 16 control parameters the observed proportion is more than 0.5 and the p value in 14 controls is less than 0.05 and hence the null hypothesis is rejected and the hypothesis "The implementation of logical access controls for system administrator in Urban Cooperative Banks are satisfactory" is proved

1.9:-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.