Information Security Risk Assessment for Banking Sector-A Case study of Pakistani Banks

Usman Munir[1], Irfan Manarvi[2]

GJCST Classification
E.5 J.1 H.2.7

***Abstract*- The ever increasing trend of Information Technology (IT) in organizations has given them new horizon in international market. Organizations now totally depend on IT for better and effective communication and daily operational tasks. Advancements in IT have exposed organization to information security threats also. Several methods and standards for assessment of information security in an organization are available today. Problems with these methods and standards are that they neither provide quantitative analysis of information security nor access potential loses information malfunctioning could create. This paper highlight the necessity of information security tool which could provide quantitative risk assessment along with the classification of risk management controls like management, operational and technical controls in an organizations. It is not possible for organizations to establish information security effectively without knowing the loopholes in their controls. Empirical data for this research was collected from the 5 major banks of Pakistan through two different questionnaires. It is observed that mostly banks have implemented the technical and operational control properly, but the real crux, the information security culture in organization is still a missing link in information security management.**

Keywords– Quantitative information security assessment, information security controls, information security, information security management system, risk, risk management.

I. Introduction

Information is considered as an asset like other important business assets and Information Security (IS) is a way of protecting information from a wide range of threats in order to ensure business continuity, minimize risk, and maximize return on investments and business opportunities[1 and 2]. Over the years the usage of Information Technology (IT) has increased massively in organizations and in society and to cater the ever increasing requirement of information flow, information systems has become complex and multifaceted [4]. IT has made electronic communication and internet necessary in all organizations. This necessity has brought efficiency and threats of hacking and intrusion with it [5]. With all these advancements in the field of IT, dependency of organizational business fusnctionality on it has increased the requirement of securing organizational information from threats [3][4][6][8]. Information security is somewhat a hard task to achieve. One of the prime reasons is that not much data related to information security management and threats to organizations‘ information is available due to confidentiality [12]. Second, costs associated to information security restrict organizations from implementing information security management systems in organizations [13]. Third, information security is not just a technical issue, it is more a managerial issue, therefore it is also required to train employees about the information security without which attaining information security is impossible [6]. It is proposed implementing information security management policy in such a way that it calculates the assets values first and then predicts the losses associated to it [10].But so far available quantitative risk assessment methods and tools are either expensive or little information about their usability and performance are available [9]. Although operational risk management techniques are functional in many originations but it is not possible to handle information risks with the perspective of operational risk management. It is therefore advised combining information security management with operational risk management for a better economical solution [7]. More dependency of world on information technology systems and processes made management of information technology risk a practical necessity [14]. Organizations adopt information security product, services, processes and tools which range from complex mathematical algorithms to the expert risk management resources. Organizations are not sure about the optimal security quality and required a cost effective information security methods which can provide them optimal security with minimum cost.Knowledge sharing and collaboration of intra-organizational cross functional teams for risk management is required for proper risk management strategies [15]. Management vision towards information security risk and involving internal stakeholder in this task is the need of the time. A more pragmatic reason is that the development of information security methods within organisations is rather an ad hoc process than a systematic one. This process generates new knowledge about information security risk management by constituting valuable organizational intelligence. Therefore, it is very important to have a systematic process, which ensures that the acquired knowledge will be elicited, shared, and managed appropriately [12].Codification and personalization are two strategies for information security. Codification is the people to document strategy to ensure intranets and databases are loaded with best practices, case studies and guidance for people in their day-to-day work. Personalization is the people-to-people strategy to link people and grow network and information security culture [16]. These two strategies established the reusability of implemented processes in organization and information

About[1]- Department of Engineering Management Department, CASE, Islamabad, Pakistan
About[2]- Department of Mechanical Engineering, HITEC University, Taxila, Pakistan

sharing background in organization. A creditable and effective method for accessing current state of information security in organizations is desirable. Good information about the current system required for good decision. Assessment of current method would help in future improvement in the system traded by its implementation cost [17]. Information security of an enterprise was defined in term of tree structure [18]. Prioritized the structure on enterprise information security basis [19], to clarify the assessment scope and minimize the assessment cost. Finally, the credibility of the assessment results is addressed with a statistical approach combined with ideas from historical research and witness interrogation psychology [20].

II. Information Security Risk Management Tool: COBRA™

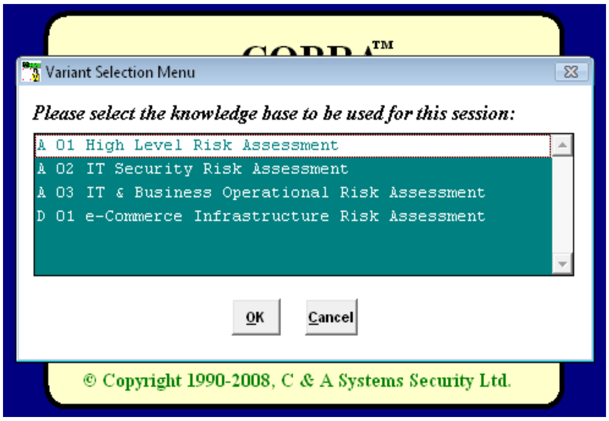
A number of standards are available on information security management system like ISO 17799, ISO 27001, the Control Objectives for Information and related technology (Cobit), and National Institute of Standards and Technology (NIST). These standards describe the requirement of information security in the organizations. But so far experts for information security implementation are requires. Whose services are expensive and rely only on their judgment for information security risk management process. Available tools are also expensive and generic. COBRA™ risk consultant is software which provides the following risk assessment:

- Compliance with the ISO information security standards BS7799 and 17799.
- Support implementing Information Security Management System in organization and also assess risk associated with organization information.
- Quantitative risk assessment of information security threats.
- Supported with a built-in knowledge base which acts as a database for evaluating information security risks.
- Perform risk assessment and also suggest its mitigation approaches.
- Assess Business Continuity Plan of an organization against its profile.
- Provide comprehensive reports about the information security risk.

Four knowledge base available to perform risk assessment are as follows and shown in Fig 1:

1. High level Risk Assessment
2. IT Security Risk Assessment
3. IT & Business operational Risk Assessment
4. E-commerce Infrastructure Risk Assessment

Fig 1: COBRA™ front-end



Please select the knowledge base to be used for this session:

```
A 01 High Level Risk Assessment
A 02 IT Security Risk Assessment
A 03 IT & Business Operational Risk Assessment
D 01 e-Commerce Infrastructure Risk Assessment
```

© Copyright 1990-2008, C & A Systems Security Ltd.

For the risk assessment a questionnaire have to be filled by a respondent which then generate a comprehensive report of its organizational risk.

III. Research Methodology

This study was conducted to analyze quantitative risks associated with information of major banks operating in Pakistan and to study security control, which are implemented for protecting their critical information. Two separate questionnaires were designed for the analysis of information security and its controls. First questionnaire was developed by using built-in knowledge base from High Level Risk Assessment section of COBRA™ software. After reviewing the COBRA™ software analysis another questionnaire was designed to evaluate the management control in these banks.High Level Risk Assessment questionnaire was filled by the information security auditors and by higher management of these banks to get the response about their implemented security policies and its impact on their information security management. Second questionnaire was filled by the five persons of various management level of each bank to check the management vision toward the information security and awareness of information security in these banks. To perform information security analysis, threats to information confidentiality, integrity, and availability were checked against the information security controls like management, technical, and operational controls.

IV. Quantitative Analysis of COBRA™ Questionnaire

COBRATM asked questions to evaluate potential threats and security policies in an organization. To determine the high level risk related to the information of the organization, questions were classified into the four categories:

a. Availability
b. Business Impact Analysis
c. Confidentiality
d. Integrity

Few important questions of COBRATM software along with their assigned points are discussed bellow to observe its functionality.

1) *Availability Questionnaire*

In availability section the questions will the highest value are discussed in table 1 below:

Table 1: Availability questionnaire

No	Availability	Answer	Scr
1	Is there a formal and workable Business Redemptions Plan in place?	Yes	0
		No	50
2	How confident are you that the plan is adequate to ensure a controlled recovery and continuance of business within the time frames specified as significant/critical:	100 % Confident	0
		Fairly Confident	0.5
		Comfortable	1
		Concerned	20
		Not Confident	50
3	When the Business Continuity Plan was last tested?	Within the 12 months	0
		1-2 years	0.5
		2-3 years	1
		4-5 years	20
		more than 5 years ago	50
4	Are the contingency arrangements for all key components reasonable and appropriate?	Yes	0
		No	50
5	How confident are you that the contingency arrangements and Business Continuity Plan would enable continuance and eventual recovery from the loss of a key building (due perhaps to serious fire, flooding, explosion, etc) without serious or critical impact on the business?	100 % confident	0
		Fairly Confident	0.5
		Comfortable	1
		Not Really Confident	20
		Concerned	50
6	How confident are you that the contingency arrangements and Business Continuity Plan would enable continuance and eventual recovery from the loss of key personnel (due perhaps to serious accident, industrial action, etc) without serious or critical impact on the business?	100 % confident	0
		Fairly Confident	0.5
		Comfortable	1
		Not Really Confident	20
		Concerned	50
7	Ignoring the recovery element of the Business Continuity Plan, to which of the following (if any), is the exposure level significant?	Fire/Flooding/ Explosion	20
		Hardware/ Equipment Malfunctin	20
		Hardware/ Equipment/ Media/Other	20
		Power Failure	20
		Software Error	20
		Infection By Computer Virus	20
		Intro Of Malicious Coding	20
8	Ignoring the recovery element of the Business Continuity Plan, to which of the following (if any), is the exposure level significant?	Hacking/Electronic Sabotage	20
		Loss Of 3rd Party Service	20
		Loss of Comm/ Network Service	20
		Operator Error /Sabotage	20
		Industrial Action by Key Staff	20
		Other Threat	20
9	Are specific back-up and recovery measures in place to handle both loss of critical data and serious software error in a timely and appropriate fashion?	Yes	0
		No	20
10	Are physical access controls/practices for areas that may hold sensitive/confidential information appropriate?	Certainly Adequate	0
		Generally OK	0.5
		A cause for concern	20
		A major problem	50

The questionnaire pertaining to Availability discussed the business continuity plan, business redemption, and disaster recovery plan. In this section maximum points were given to business continuity plan because it ensures the continuity of critical business functions by providing methods and procedures for dealing with long outages and disasters. It is a broader approach in which continuity of a business during any disaster is ensured until that disaster is either curtailed or business operation returns to its normal circumstances. Physical access controls were also evaluated because appropriate physical controls are necessary to eliminate potential losses and risks associated to information assets, weak physical access controls could not prevent intruder from causing any harm to information processing facility or information assets. Therefore, COBRA^{TM} ask particular questions related to appropriate physical access control not only to evaluate these control for better analysis of security situation but also to create awareness in management for importance of these controls.

2) *Business Impact Questionnaire*

Business Impact considered as a functional analysis in which a team collects data through interviews and documentary resources. Than developing hierarchy of business functions and applies a classification scheme to indicate each individual function critical level. Question from the Business Impact Analysis are shown bellow in table 2.

Table 2: Business Impact questionnaire

No	Business Impact	Answer	Scr
11	What was the total revenue for this business function/service during the last financial year?	Less Than 10,000,000	0
		10,000,000 to 100,000,000	1
		100,000,000 to 500,000,000	5
		More than 500,000,000	20
12	What is the highest likely financial value throughout per day :	Less than 500,000	0
		500,000 to 5,000,000	1
		5,000,000 to 50,000,000	5
		More than 50,000,000	20
13	Which of the following types of function are directly performed :	Financial Accounting	5
		Trading/ Dealing	5
		Payroll	5
		Management info/ Support	6
		Research	5
		Manufacturing	5
		Infra-structure Support	5
		Retail	5
		Other	5
14	How many other systems or business units internal to this enterprise have a dependency upon this one?	Minor Dependency	1
		Significant Dependency	2
		Total Dependency	3
15	In the worst case scenario means no backup, how quickly could unavailability result in SIGNIFICANT impact in terms of current/future revenues and other direct financial losses?	2 hours	200
		24 hours	20
		7days	2
		1 month	1
		Never	0
16	In the worst case scenario, how quickly could unavailability have a SIGNIFICANT impact in terms of customer, shareholder, public or departmental confidence?	2 hours	999
		24 hours	200
		7days	20
		1 month	1
		Never	0
17	How quickly could unavailability have a SIGNIFICANT impact in terms of contractual, regulatory, or legal obligations?	2 hours	200
		24 hours	20
		7days	2
		1 month	1
		Never	0
18	If confidential/key information was disclosed to one or more competitors, what is the worst impact that could result:	None	999
		Moderate	200
		Significant	20
		Substantial	1
		Critical	0
19	If confidential/key information was disclosed, what could be the worst impact in terms of current/future revenues and other direct financial losses?	None	200
		Moderate	20
		Significant	2
		Substantial	1
		Critical	0
20	If confidential/key information was disclosed, what could the worst impact be in terms of customer, shareholder, public or departmental confidence?	None	999
		Moderate	200
		Significant	20
		Substantial	1
		Critical	0
21	If confidential/key information was disclosed, would there be any implications in terms of contractual, regulatory, or legal obligations?	None	0
		Moderate	1
		Significant	5
		Substantial	25
		Critical	150
22	If the data/information lost its integrity (through error, deliberate unauthorized alteration, fraud, etc), what could be the worst impact in terms of direct financial loss?	None	0
		Moderate	1
		Significant	5
		Substantial	25
		Critical	150
23	If the data/information lost its integrity, what could the worst impact be in terms of customer, shareholder, public or departmental confidence?	None	0
		Moderate	1
		Significant	5
		Substantial	25
		Critical	150

24	If the data/information lost its integrity, would there be any implications in terms of contractual, regulatory, or legal obligations?	None	0
		Moderate	1
		Significant	5
		Substantial	25
		Critical	150

In business impact analysis section the COBRA™ gave maximum points to questions which have direct and indirect impact on the stakeholders and customers. The confidence of customer and internal and external stakeholders on business products and business management process is essential for the success. All these questions are concerned on unavailability of critical information to business in term of customers and stakeholders confidence on the organization. COBRA™ also bifurcate impact of losing critical information with respect to time to establish minimum time when the organization would have maximum disadvantage of losing that information. The confidence of organization or management on its internal and external employees and stakeholders is considered as a key to establish proper information security checks.

3) *Confidentiality Questionnaire*

This section of software is about establishing confidentiality of information. Assurance that the information is not disclosed to any unauthorized individual, programs or processes. Organizations implement information confidentiality separately for business viability. Questions and points assigned by COBRA™ are discussed in table 3:

Table 3: Confidentiality questionnaire

No	Confidentiality	Answer	Scr
25	How confident are you that there is no serious threat of a third party having unauthorized sight of sensitive hardcopy output?	100 % confident	0
		Fairly Confident	0.5
		Comfortable	1
		Not Really Confident	20
		Concerned	50
26	Are physical access controls/practices for the building appropriate?	Certainly	0
		Okay	0.5
		Cause of Concern	20
		Major Problem	50
27	Are physical access controls/practices for areas that may hold sensitive/confidential information appropriate?	Certainly	0
		Okay	0.5
		Cause of Concern	20
		Major Problem	50
28	Are logical access controls sufficient to protect sensitive data/information from unauthorized EXTERNAL scrutiny?	No weakness	0
		Minor Weakness	0.5
		Not Sure	1
		Some Concerns	20
		Major Weakness	50
29	Are logical access controls appropriate and sufficient to protect sensitive data/information from unauthorized INTERNAL scrutiny?	No weakness	0
		Minor Weakness	0.5
		Not Sure	1
		Some Concerns	20
		Major Weakness	50
30	Are practices with respect to hardware, equipment and media adequate and appropriate?	Yes	0
		No	50
31	Is the security infra-structure and culture of the enterprise:	Good	0.5
		Reasonable	1
		Poor	50
32	Are there any other exposures evident?	No Major Exposure	0
		Some concerns	20
		Significant Exposure	20
33	Are there measures/plans in place to mitigate or manage any breach of confidentiality?	Yes	0
		Outlines only	0.5
		Ideas Only	2
		Nothing	50

COBRA^{TM} gives emphasis on questions related to the physical and logical access controls because in the current scenarios when companies have threat over internet about the security breach and intrusion, lapses on these parts can harm the organization in term of market repute and profitability. Besides these other important questions are related to security structure and culture of an enterprise. Information security is based mostly on culture of an organization. If in an organizations every employee is aware about the information security requirement, policies, and have good understanding of their responsibilities towards information security, organization will have less threats of losing information than.

4) *Integrity Questionnaire*

Integrity of information means protecting data and information resource from being altered in an unauthorized fashion. The questions in the integrity section are assigned the following scores as in table 4:

Table 4: Integrity questionnaire

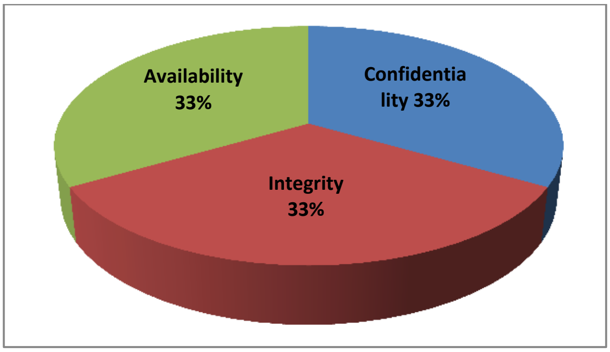
No	Integrity	Answer	Scr
34	How confident are you that there is no significant risk of serious ERROR being introduced during the input of important data/information?	100 % confident	0
		Fairly Confident	0.5
		Comfortable	1
		Not Really Confident	20
		Concerned	50
35	Consider the situation with respect to INTENTIONAL unauthorized manipulation of input data/information, by both internal and external parties. How confident are you that there is no significant risk of serious breach during the input of important data/information?	100 % confident	0
		Fairly Confident	0.5
		Comfortable	1
		Not Really Confident	20
		Concerned	50
36	How confident are you that there is no significant risk of serious error being introduced via program error or malfunction?	100 % confident	0
		Fairly Confident	0.5
		Comfortable	1
		Not Really Confident	20
		Concerned	50
37	Are the controls in place to prevent the unauthorized modification of program source code appropriate?	Certainly	0
		Okay	0.5
		Cause of Concern	20
		Major Problem	50
38	Are logical access controls sufficient to protect sensitive data/information from unauthorized EXTERNAL access?	No weakness	0
		Minor Weakness	0.5
		Not Sure	1
		Some Concerns	20
		Major Weakness	50
39	Are logical access controls appropriate and sufficient to protect sensitive data/information from unauthorized INTERNAL access?	No weakness	0
		Minor Weakness	0.5
		Not Sure	1
		Some Concerns	20
		Major Weakness	50
40	Are the controls over computer operations adequate and appropriate?	Certainly	0
		Okay	0.5
		Cause of Concern	20
		Major Problem	50
41	Is the security infra-structure and culture of the enterprise:	Excellent	0
		Good	0.5
		Reasonable	1
		Poor	50
42	Are there any other exposures evident?	No Major Exposure	0
		Some concerns	20
		Significant Exposure	50

In this section the COBRA^{TM} asks management about their confidence on internal and external security checks which are implemented to save data from any unofficial changes. Organizations mostly have external and internal threats to their information. The internal threat can lead to more catastrophic impact than the external one. Therefore it is important for the organization to have a full confidence on the internal security controls and procedures on retrieving and adding data. If internal procedure and process of input and output of information has some loopholes then it is important to adjust and redefine these procedure and make it as firm as required for the integrity of information. As a result organizations assign different privileges to users so that only designated officials can alter or process information. These controls help organization in maintaining the security checks and also give sense of responsibility to the personals authorized for any changes.

5) *Bifurcation of Information Threats in COBRA^{TM}*

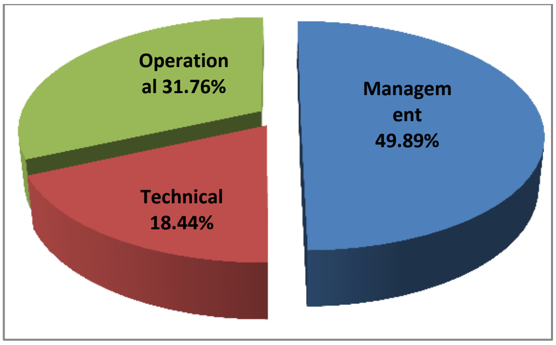
Besides the importance of some particular questions on others COBRA^{TM} has given equal score to availability, integrity and confidentiality of information as shown in Fig 2 that all parts have given equal percentage of 33%.

Fig 2: Bifurcation of C.I.A in COBRA^{TM}



To evaluate organization information security controls, COBRA^{TM} questions were plotted against three information security controls. By this, it has observed that COBRA^{TM} constructed questions in such a format that the major distribution of these questions were related to management control with a percentage of 49.89% following the operational control with 31.76% and finally technical control with 18.44% as shown in Fig 3.

Fig 3: Bifurcation of security controls in COBRA^{TM}

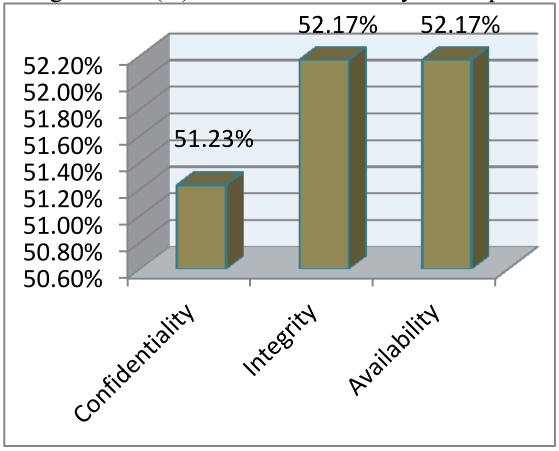


V. COBRA^{TM} APPLICATION IN BANKING SECTOR

1) *High Level Risk Assessment of Bank (A)*

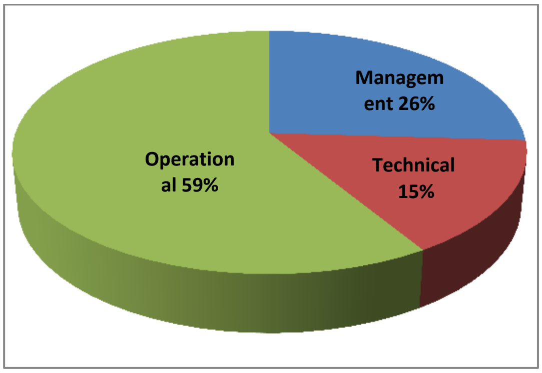
Bank (A) is one of the largest banks of Pakistan with presence in Hong Kong, UK, Nepal, Nigeria, Kenya and Kyrgyzstan and rep offices in Iran and China. Key areas of operations encompass product offerings and services in retail and consumer banking.The analysis done by the COBRA^{TM} on threats to information availability, integrity and confidentiality is shown in Fig 4. According to it, threat to information confidentiality is 51.23% showed that the information could be intruded. Whereas threat to integrity of information is 52.37% means information could be altered or in some cases a completeness of information was questionable for organization. Threat to availability of information in this bank was at 52.17% too. This software suggested implementing security checks on data warehouses and physical data places.

Fig 4: Bank(A) information security risk report



The figure 5 shows the percentage of security controls in bank (A). It may be seen that the management control is lower being 26% against suggested 49.89%. The operational control is being at 59% where the suggested percentage at 31.76%. Technical control being lower than the suggested 18.44% was at 15%. This showed that the bank overall operational threats were catered properly whereas the implementation of information security policy was uncertain and lack of information security awareness in the management functions.

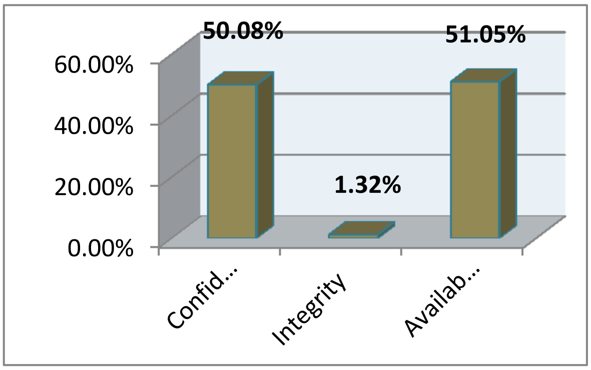
Fig 5: Bank(A) information security controls report



2) *High Level Risk Assessment of Bank (B)*

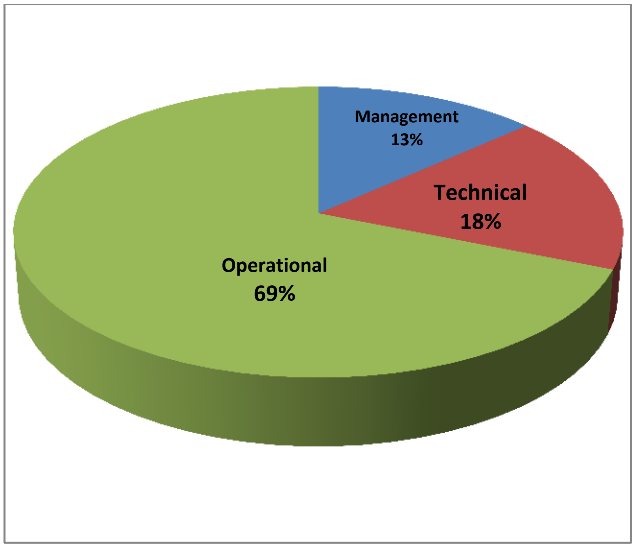
It is the fourth largest bank of Pakistan has a customer base of approximately 4 million, 1,026 branches, and over 300 ATMs. The bank (B) risk assessment through COBRA^{TM} shown in Fig 6. The threats to confidentiality of information were at 50.08% showed an unauthorized access of data. The threats to integrity is maintained well which were at 1.32% only. Threats to availability of information were reported 51.05 % showed concern to information record keeping. Precise review of report showed that information integrity related to the information accuracy was well maintained in the bank. But other information security threats like confidentiality and availability were quite high. These high levels of threats showed that the availability of critical information to unauthorized and unwanted individuals or to the third-part. This can harm the reputation of the bank and ultimately can affect its business.

Fig 6: Bank(B) information security risk report



The Fig 7 showed the percentage of security controls in bank (B). It may be seen that the management control was lower being 13% showed a high threats related to it. The technical control and operational controls were optimal being at 18% and at 69%. This showed an improper management control in this bank. It led to a risk of improper information security policy and its implementation, information leakage by employees, unsecure risk culture in organization, and unawareness of information security.

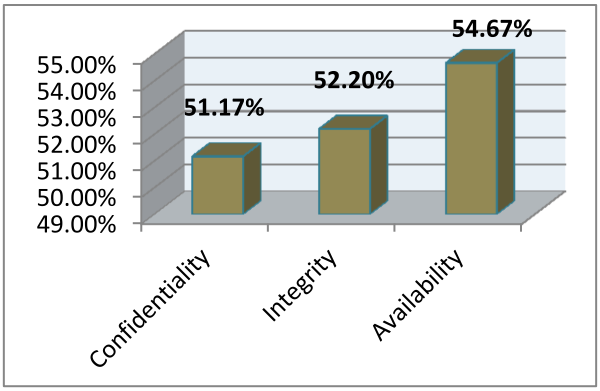
Fig 7: Bank(B) information security controls report



3) *High Level Risk Assessment of Bank (C)*

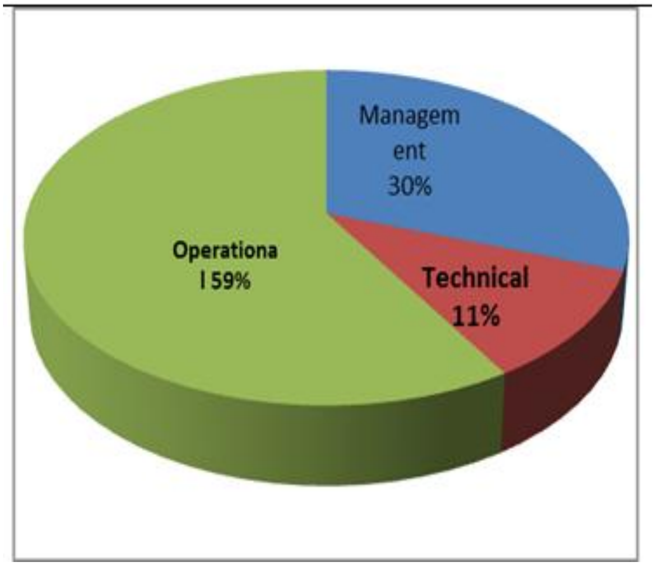
Bank (C) is the seventh largest bank of Pakistan with over 240 branches. The risk assessment done by COBRA^{TM} is shown in Fig 8. The threats to availability of information were highest at 54.67% followed by integrity at 52.20% and confidentiality at 51.17%. These high threats showed that availability of critical information were to unauthorized and unwanted individuals or to the third-part. This could harm bank reputation and ultimately to its business. These high threats also showed vulnerability to correctness, completeness, and protection of information from intrusion.

Fig 8: Bank(C) information security risk report



The security controls bifurcation in bank (C) is shown in Fig 9. It may be seen that technical and management controls were lower being at 11% and 30%. Operational control maintained properly as its being at 59%. Risks associated to management controls like policy establishment and information security culture could be higher in this bank.

Fig 9: Bank(C) information security controls report

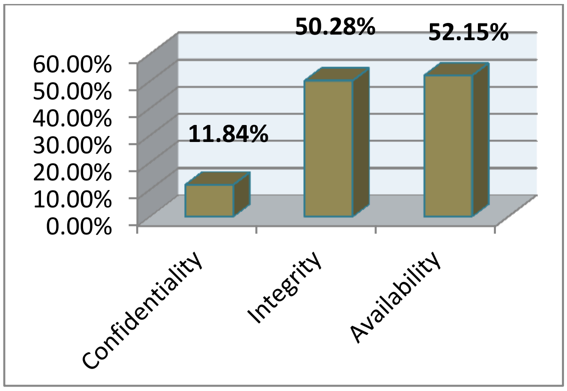


4) *High Level Risk Assessment of Bank (D)*

Bank (D) has the network of over 700 online branches in Pakistan.

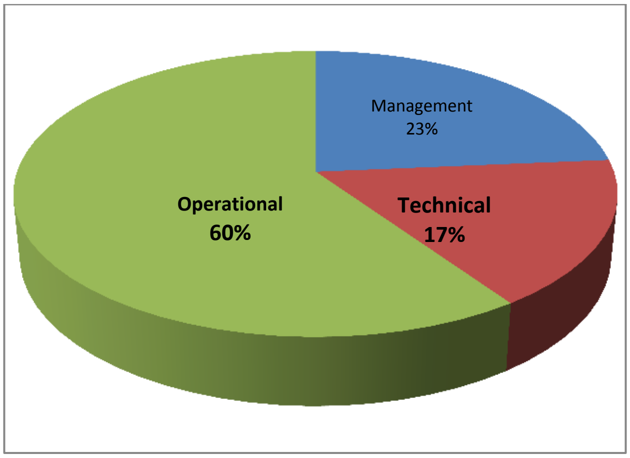
The risk assessment done by COBRA^{TM} is shown in Fig 10. The threats to availability of information were highest at 52.15% followed by integrity at 50.28%. Threats to confidentiality of information were reported at 11.48%. The high threats of availability and integrity showed that critical information were accessible for unauthorized changes. On other hand information were not available at required time or were not managed properly.

Fig 10: Bank(D) information security risk report



The Fig 11 showed security controls percentage in bank (D). It may be seen that technical control is being at 17% than suggested 18%. Management control being at 23% is lower than suggested one. The operational control was being managed properly as it was at 69% against the suggested 31.76% by the software. The management control at 23% showed that a risk on policy establishment, weak information security culture, and poor management vision towards information security.

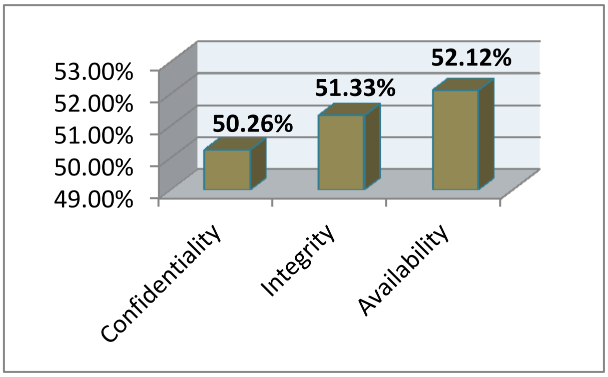
Fig 11: Bank(D) information security controls report



5) *High Level Risk Assessment of Bank (E)*

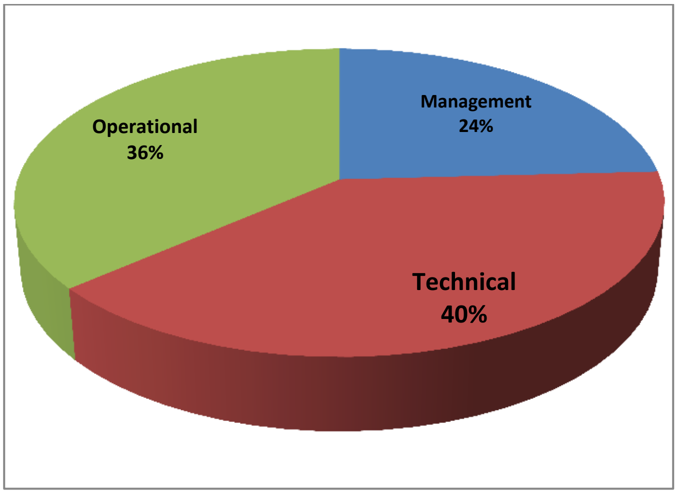
The Bank (E) provides microfinance services and act as a catalyst in stabilizing the country's newly formed microfinance sector. The risk assessment done by COBRA^{TM} is shown in Fig 12. The threats to availability of information were highest at 52.12% followed by integrity at 51.33% and confidentiality at 50.26%. The high threats showed that critical information were accessible for unauthorized change. Availability of information was at required time or was not managed properly. Threat of unauthorized changes and completeness of information were also present.

Fig 12: Bank(E) information security risk report



The Fig 13 showed security controls percentage in bank (E). It may be seen that technical control was at 40% followed by operation control at 36% and management control at 24%. It is being observed from the Fig that management main focus is on technical control. Operational control is also maintained at 36% comparing with suggested 31.76% by software. The management control at 24% showed a risk on policy establishment, information security culture, and poor management vision towards information security

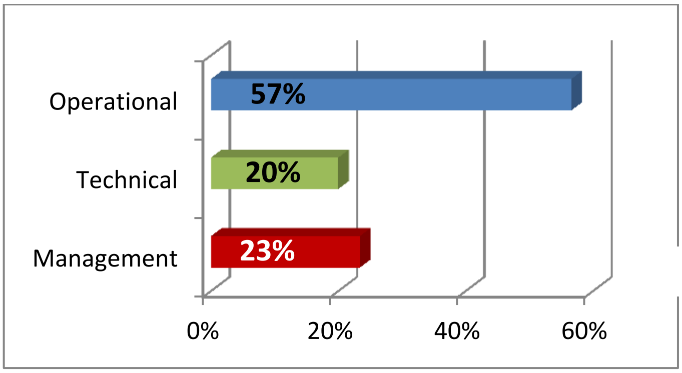
Fig 13: Bank(E) information security controls report



6) *Consolidated High Level Risk Assessment*

The security controls implemented in all banks is being evaluated in Fig 14. It is being seen that operational control in all banks was at 57% followed by management control at 23% and technical control at 20%.

Fig 14: Information security control in all banks



The COBRA^{TM} suggested a percentage of 49.89% to management control, 31.76% to operational control, and 18.44% technical control for optimal information security. The comparative analysis of proposed and actual percentage of control showed that operational control in all banks was well maintained. The technical control was also maintained properly. The management control in all banks individually and in this consolidated report was at lowest percentage being at 23% shown that its not up-to the COBRA^{TM} recommended mark that is almost 50%. Therefore the risk associated to management control must have to be high in all banks according to COBRA^{TM} reports. Risk associated with the management control.

- ➢ Ineffective decision making
- ➢ Poor establishment of information security risk management policies/ procedures
- ➢ Unawareness of Information Security related risks
- ➢ Information secure culture
- ➢ Information Security not a part of overall business process.
- ➢ Fraudulent system usage
- ➢ Reputational damage
- ➢ Lack of business continuity planning
- ➢ Information security not a part of strategic planning

Consolidated Analysis of Management Contols

The second phase of survery is accomplished by developing sepecific questionnaire to evaluate the COBRA^{TM} results. The questionnaire was divided into two sections. First section was about the management vision towards information security. Second section was about the information security awareness and information security culture in banks. A specific value was assigned to all the questions to have a quantitave analysis of banks management control.

To check the matuarity level of management control in these banks, overall score of the questinnaire was lied between -20 to 20. The maturity of management control was further classified into four levels shown in Fig 15.

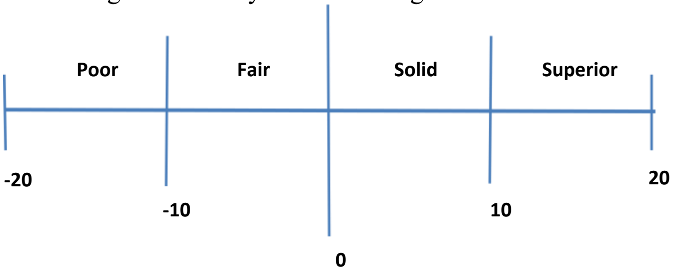
a. -20 to -10 = Poor

b. -10 to 0 = Fair

c. 0 to 10 = Solid

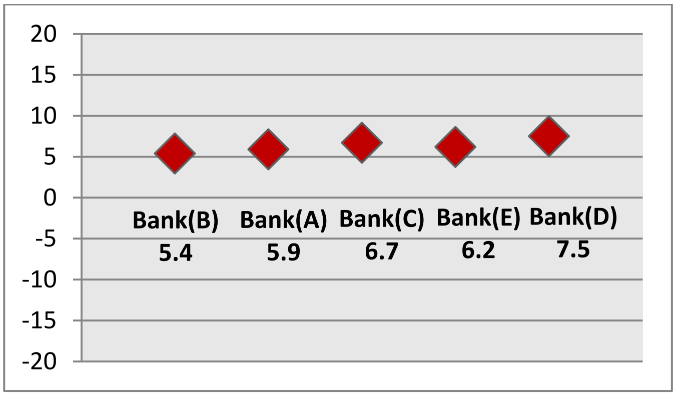
d. 10 to 20 = Superior

Fig 15: Maturity line for management control



Information security is more a management issue than a technical one. Effective management control is essential to establish information security culture. Establing secure information is a continus journey which can be achieved though action, policies, values, and positive management style. The questinnaires were filled by five personal of different management level of each bank. The result of all banks management control is shown in the Fig 16.

Fig 16: Maturity standing of all banks



The management controls in all banks is being at the solid level with a range from 5.4 to 7.5. The maximum management control is being in bank (D) at 7.5 and lowest in bank (B) at 5.4. The bank (A) is being at 5.9 followed by bank(C) and bank (E) at 6.7 and 6.2. Management control of all banks lied at the solid level. It was not in superior level in any of the banks.At solid level organization achieved the following management control:

- Information security policy is being rolled out
- Supporting standards and procedures are being developed
- Employee awareness has begun
- Confidentiality, Integrity, and availability of information is being considered
- Initial employee awareness process has begun
- Access to sensitive areas is generally restricted
- Employees are aware of fire safety procedures
- Contingency plans have been developed

- Management supports for information security has begun

VI. FINDINGS

COBRA$^{\text{TM}}$ gave a comprehensive information security risk analysis report but few short coming of this tool are:

- Risk raiting is not established properly in the COBRA$^{\text{TM}}$ e.g Fire cause more demage to information/ infrastructre etc than malfunctioning of any hardware. COBRA$^{\text{TM}}$ has given the same score to such cases.

- For risk assessment it is recommended to do the asset evalution of all the tangible and intangible assets of the organization. COBRA$^{\text{TM}}$ doest not evaluate individual asset value of organization in high level risk assessment. Due to this in case of any loss the accurate financial loss can not be predicted through this software.

- In risk assessment process, the range of accepted risks in COBRA$^{\text{TM}}$ is very low, from 0-19 score. any score above than 19 will be treated as a high expectancy of threat to organization. One drawback of this hard coded low risk acceptancy is that the risk level of all organization mostly falls in between 50% and above which in real scenario is exceptionally high risk for any organization. Secondly, perdiction for which organization like to use quantitaive tools than qualitative assessment tool is not obtainable.

- COBRA$^{\text{TM}}$ risk assessment reports coveres lot of information security risk area and also inform the requirement of security improvement at the exact areas, but do not inform the exact measures to mitigate them.

- Awareness of information security requirement to all employees of organization is essence of information security management system. Since as per NIST [9], employees are the biggest threat to organization information than any other attack. COBRA$^{\text{TM}}$ ignores that High Level Risk Assessment domain.

- Re-assessment of COBRA$^{\text{TM}}$ results by conducting second survey showed substantial differences, for instance, in COBRA$^{\text{TM}}$ reports the level of the management control implementation in all banks was between 13% to 30% whereas in re-assessment survey this range was between 50% to 75%.

- Besides all these drawbacks COBRA$^{\text{TM}}$ still facilitate the management in identification of information security risks.

VII. FUTURE WORK

Information security risk management framework which would cover the information security governance and show the results related to the information security controls so that organizations can focus and improve the deficient area regarding information security management.

VIII. REFERENCES

1) ISO/ IEC FDIS 17799 ―Information Technology- security techniques- Code of practice for information security management" 2005.
2) ISO/ IEC FDIS 27001:2005(E) ―Information Technology- Security techniques- Information Security Management Systems- Requirements", pp 1 – 9
3) Thomas Nowey and Hannes Federath ―Collection of Quantitative Data on Security Incidents" 0-7695-2775-2/ 2007 IEEE.
4) Daniel Port, Rick Kazman, Ann Takenaka, Department of Information Technology Management, University of Hawaii ―Strategic Planning for Information Security and Assurance" 978-0-7695-3126-7/ 2008 IEEE.
5) Fong-Hao Liu ―Constructing Enterprise Information Network Security Risk Management Mechanism By Using Ontology" 0-7695-2847-3/ 2007 IEEE.
6) Ching- Jiang Chen and Ming-Hwa Li ―SecConfig: A Pre-Active Information Security Protection Technique" 978-0-7695-3322-3/ 2008 IEEE
7) Heinz Lothar Grob, Gereon Strauch and Christian Buddendick" Applications for IT-Risk Management –Requirements and Practical Evaluation" DOI 0-7695-3102-4/ 2008 IEEE.
8) Wade H. Baker and Linda Wallace ―Is Information Security Under Control? Investigating Quality in Information Security Management" 1540- 7993/ 2007 IEEE.
9) ENISA (European Network and Information Security Agency), ―Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment method and tools", Available online: http://www.enisa.europa.eu, 2006 pp 39 - 51.
10) Julie J.C.H Ryan and Danel J. Ryan ―Performance Metrics for Information Security Risk Management" 1540-7993/ 2008 IEEE.
11) Xiao Long, Qi Yong and Li Qianmu ―Information Security Risk Assessment Based On Analytic Hierarchy Process and Fuzzy Comprehensive" 978-0-7695-3402-2/ 2008 IEEE.
12) Papadaki, K., Polemi, D., ―Towards a systematic approach for improving information security risk management methods", in Proc. 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communication (PIMRC), 2007.

13) Thomas Finne, Abo Akademi University, Institute for Advance Management System Research(IAMSR) —A DSS for Information Security Analysis: Computer Support in a Company‘s Risk Management"0-7803-3280-6/ 1996 IEEE.
14) Symantec, —IT Risk Management Report 2: Myths and Realities", Available online at http://eval.symantec.com, 2008.
15) Brown, J S & Duguid, P, —Knowledge and organization: A social-practice perspective", Organization Science, 12, 2: 198-213, 2001.
16) Desouza, K.C.,Awazu, Y., Baloh, P. —Managing Knowledge in Global Software Development Efforts:
Issues and Practices", IEEE Software 23(5), 30–37, 2006.
17) Ekstedt M., et al., —Consistent Enterprise Software System Architecture for the CIO – A utility-Cost Approach", Proceedings of the 37th annual Hawaii International Conference on System Sciences (HICSS), 2004.
18) Johansson E., et al., —Assessment of EIS - An ATD Definition", in the Proceedings of the 3rd Annual Conference on Systems Engineering Research (CSER), March 23-25, 2005.
19) Johansson E., et al., —Assessment of Enterprise Information Security – The Importance of Prioritization", In the Proceedings of the 9th IEEE International Annual Enterprise Distributed Object Computing Conference (EDOC), Enschede, The Netherlands, September 19-23, 2005.
20) Edvardsson B., —The Need for Critical Thinking in Evaluation of Information", Proceedings of the 18th International Conference on Critical Thinking, Rohnert Park, USA, 1998.