ANALYSING INFORMATION SECURITY PRACTICES IN INDIAN BANKS

A SUMMER INTERNSHIP REPORT

Submitted by

HARSHIT GARG

In partial fulfilment for the award of the degree

Of

Master of Business Administration (2013-15)

Department of IME, IIT KANPUR

"Project Trainee"

At

Institute for Development & Research in Banking Technology

Hyderabad - 500057

Institute for Development & Research in Banking Technology

Hyderabad - 500057

CERTIFICATE

This is to certify that this is a bonafide record of the summer internship project work entitled

Analysing Information Security Practices in Indian Banks

Done by

Harshit Garg

of Department of IME, IIT-KANPUR during May-June 2014 in partial fulfilment of the requirements for the award of Degree of Master of Business Administration in Department of IME of IIT – KANPUR.

Dr. G.R. Gangadharan
Project Guide

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to the Institute for Development and Research in Banking Technology (IDRBT) and my guide **Dr. G.R. Gangadharan**, who mentored me throughout the project.

This opportunity of learning all the nuances of Information Security Practices and their implementation in the banking of the country was a boon to me as one rarely gets such exposure.

I would not hesitate to add that this short stint in IDRBT has added a different facet to my life as this is a unique organization being a combination of academics, research, technology, communication services, crucial applications, etc., and at the same time performing roles as an arm of regulation, spread of technology, facilitator for implementing technology in banking and non-banking systems, playing a role of an NGO (without being one) and many more varied activities.

I am extremely grateful to **Dr. G.R. Gangadharan** for his advice, innovative suggestions and supervision. I thank him for giving me the opportunity to approach diverse security practices adopted by different organizations. Also, I express thanks to the various IT officials of the banking firms whose words helped me a lot in carrying out my project work.

I am thankful to the staff at IDRBT for helping me to get familiar with the environment. I am obliged to my department, Department of IME, IIT Kanpur, for giving me this golden opportunity of working at a high-end research institute like IDRBT.

I am thankful to IDRBT for providing such an amazing platform for students to work in real application oriented research. Finally, I thank one and all who made this project successful either directly or indirectly.

Harshit Garg

TABLE OF CONTENTS

Information Security Management System: Information Security Practices in Indian Banks

"There are risks and costs to a program of action, but they are far less than the long range cost of comfortable inaction." — John F. Kennedy

ABSTRACT

Purpose: Many practitioners have designed and proposed various Information Security (IS) standards and practices in order to achieve effective information security management system in small and large organizations. Most of the organizations generally adopt some of these practices according to the need of their operations. The main idea of this study is to observe the various IS practices in effect in two Indian banking firms namely ABC Bank* and PQR Bank*. Also, the purpose of the study is to analyze shift of related control among hierarchical levels in an organization.

Methodology: Initially, the raw data was derived from a semi-structured interview raised to the ABC Bank and PQR Bank officials followed by the preparation of two case studies for both the banks based on the received answers. The officials of ABC Bank were interviewed face to face while answers from PQR Bank personnel's were collected telephonically and via email. Finally, the findings of the research were drawn from these case studies and were compiled in this report.

Value: This paper demonstrates that the information security control shifts with roles and responsibility of the user within an organization. It also fulfils the need in information security for a set of practices and trends in adoption of practices available for both academic usage and practical implementation.

Key Words: Data Security, Risk Management, IS Governance, Security Culture

---

*** Note:** Bank names and official names disguised due to confidentiality and security issues

INTRODUCTION

Now a days, public as well as private sector firms are moving to the online data storage from manual record keeping in form of physical files. This has made the access to the data faster and easier. But, data kept on online servers or activities performed over internet are vulnerable to threats. Such activities often result in unauthorized access to the restricted confidential information. An intruder may modify or steal the data which is termed as information security breach in the organizational terminology. Sometimes, threats may be unintentional or accidental which result due to human negligence, system malfunctioning, natural disasters and human ignorance. An effective Information Security Management System (ISMS) is the critical factor for the success of reliance over the open network systems. In order to achieve an effective ISMS, it is very important for an organization to develop a secure IS culture. Banks and the financial institutions are the example of such firms which solely rely on an effective ISMS. Without secure environment and security policies things can become chaotic in these organisations. Also, frail systems may cause them to lose their business.

Many IS practitioners have given best practices and trends in ISMS which apply globally to most of the industries. But, certain things are dependent on geographical and demographic factors. Also, one requires having an extra caution in case of banking and other financial firms specifically in areas which are still developing technologically. Various studies have shown that the technological as well as non-technological issues are equally responsible for safeguarding the sensitive data or information of an organisation *(Siponen & Oinas-Kukkonen, 2007; Workman, Bommer, & Straub, 2008)*. Thus, it is very important for any organization to keep a balance between technological and non-technological factors to facilitate and implement a sustainable IS practice. Theoretically, things seem to be easy but are quite difficult to exercise practically. An organization need to focus on safeguarding its information assets and imbibing ethically acceptable safe and secure culture within its employees. In order to achieve an effective integrated framework, firstly, all the concerned human, organizational and technological challenges of IT security management *(Rodrigo Werlinger, Kirstie Hawkey and Konstantin Beznosov)* must be determined followed by the implementation of a strategy that can well manage and minimize the effect of these security challenges. Finally, a policy document must be prepared such that it proves its relevancy to the information security objectives of the organisation and is simple to understand by the employees. Also, it must be made sure that the policy is practically implementable and enforceable. One of the most important aspects in this concern is communication of policy. It must be distributed such that it is communicated throughout the organisation to every user handling the information assets.

The very purpose of this work is to demonstrate what all things actually contribute to the effective IS practices in Indian banks and to exhibit how the security culture within the organisation work in conjunction with the technological measures to achieve highly acceptable

ISMS. This study adopted a case study based approach to display and examine various measures adopted in various banks of India to preserve their information from both internal and external threats to the organization and to take care of the confidentiality, integrity and availability of its critical information. Moreover, it will focus on various facets of these measures such as IS governance, risk management and control, roles and responsibilities associated with different users within an banking organization, regulatory compliance audits and policy awareness programmes and trainings.

INFORMATION SECURITY

Security is the key building block upon which any organization depends; protecting its assets, resources and people. Security is generally related to threats such as accidents, natural disasters, intentional breach etc. Factors affecting security and its standards are categorised into three different segments namely human, organizational and technological *(Beznosov and Beznosova (2007))*. Human factors are those which are related to individuals, their interaction with other human beings and culture. Organizational aspects are related to the organization's structure, its size, industry type and managerial concern towards information security. Technological factors relate to technological solutions such as protocols and applications.

Human Factors

Human factors are one of the significant threats to the information security. The most important being lack of proper communication. An organization requires sustaining an effective communication and understanding of risk and security among different stakeholders. It all depends on individuals how they handle the risks and manage them. Human errors also pose a considerable threat to security. These errors can be accidental as well as intentional and occur mainly due to ignorance, improper communication and diverse thoughts of different individuals.

Organizational Factors

Organization factors generally constitute type of industry, organization size, its structure and top management's support to effectively manage information systems and control risks. Banking and other financial institutions need to invest more in ISMS as transactions are much critical in this industry. Moreover, in large organizations, it often become too complex to manage the information as spherical control is much difficult to implement in such organizations. Without top management support, it is very difficult to enforce security practices and sustain them for a long time. The management is supposed to allocate the required assets and resources for effective functioning of information security. It is essential for the management officials to be aware of risks, their reduction techniques and control measures. Also, they must be capable to handle uncertainties and take strategic decisions in order to control them. Therefore, it can be

stated that this factor is very responsible in deciding the implementation of security controls and practices within an organization to safeguard the information.

Technological Factors

Technological issues present a major challenge in the implementation of security practices. The complexity of technology and costs involved makes it difficult for the strategist to take decisions as comparing them to the risk is quite complicated. Sometimes, complex networks and systems make it difficult for security practitioners to adopt security protocols and applications. Moreover, this complexity is just not a result of innovation in technology but also depends on various other environmental factors such as size of the organization, industry type, open environment, vulnerabilities and IT management distribution. Also, the support from security tools is not sometimes sufficient to meet the security standards and henceforth affect the implementation of security in an organization. Such problems occur as some security tools are so vast and difficult that it becomes unmanageable to handle these tools.

MANAGING INFORMATION SECURITY

Information security is practiced in day to day operations in most of the organizations but managing the risk effectively is something that is termed as "Information Security Best Practice". There are certain processes and activities that define these best practices and support secure environment to perform the operations in an organization. Basically, we define the process model in terms of certain components as follows:

1. **Application Security**— It refers to the use of hardware, software and procedural measures taken throughout the application lifecycle to prevent defects in applications and protecting them from external threats.

2. **Physical Security**— Physical Security describes security measures taken to prevent unauthorized access to the facilities, assets and resources in order to prevent them from unwanted damage or harm. CCTV surveillance, security guards, locks and many other similar security techniques constitute to physical security.

3. **Malware management**— Malwares include some malicious programs that may be in the form of active scripts or codes, other softwares etc. Such objects interrupt system operations, capture sensitive information and sometimes corrupt the important system files. Viruses, worms or trozans contribute to the malicious softwares. To safeguard the system and its information from malware attacks, there are various anti-viruses, anti-malwares and firewalls available in the market.

4. **Data protection and Cryptography**— A large amount of data is present in the open network system. This data may contain some personal or restricted information but is accessible to the public. To prevent this sharing of data, sharing checks and various cryptographic techniques are being used. Cryptography is a phenomenon where the sender encrypts the message before sending and this encrypted message is decrypted at a later stage by the receiver upon receipt of the message. Cryptographic algorithms are based on computational hardness assumptions and are very difficult to break practically.

5. **Asset classification and control**— It refers to the maintenance of appropriate level of protection for different critical assets and resources. Distribution of such assets is done as per the criticality and need of the operation. Also, access to these assets is controlled by multi layered protection protocols and methods e.g. biometric security systems, security passwords, certificates and key pairs.

6. **Communications management**— Proper and secure communication ensures secure use of information and information facilities. It reduces risk of failure and its consequences. Also, effective communication prevents confusions between the two parties and thereby guarantees smooth functioning of operations.

7. **Training and Awareness**— Security standards and practices once finalized, need to be communicated to the concerned users. Communication can be written or oral but the idea is to make the users aware of the security principles. Even the timely updates through awareness briefings, newsletters, circulars and internet posts have to be communicated to the concerned users to ensure flawless functioning. Moreover, trainings are also required sometimes to make people understand the practicalities of certain policies and processes.

8. **Access controls and Responsibility distribution**— User roles determine the access level of a person to use the organizational functional data. Various user roles are assigned to the users according to the nature of their work and accordingly access privileges are provided to these users e.g. an administrator has full power and he can perform any task while a reader just has read access rights to certain data files or systems.

9. **Monitoring and Reviews**— Monitoring and reviewing the information security systems is another significant process. There are various things that can be monitored such as employees and their activities, incident handling reports, system logs, website monitoring records, internal audit reports and so on. In some countries monitoring is possible only if their employees are aware of such activities in place. The only way to handle this is to get employees to sign "*Acceptance Use Policy*". It includes provisions for checking compliance

using different monitoring methods and the consequences if an employee fail to comply with the guidelines.

10. **Incident management**— Incident management is a process or a set of processes which ensures that normal operations are restored as quickly as possible which a minimal impact on operations as well as the user. Incident management has three basic components: identify, analyze and correct the hazards to prevent future recurrence of incidents.

11. **Policy management**— IS Policies are the set of guidelines and procedures that are critical for information security management or IT related risks. It consists of a number of principles that each employee needs to follow in order to preserve the confidentiality, integrity and availability of significant information and data. The IS policies are mainly concerned with the following regulations:
    a. Controlling access to the assets and IT resources
    b. Application control over the network
    c. Antivirus installation and update policy
    d. Remote access policy
    e. Network and IT facilities usage policy
    f. User account policy
    g. Emailing and data classification
    h. Logging and monitoring policy
    i. Encryption guidelines
    j. External storage device usage policy

    In an organization, failure to have an effective IS policy management system may lead to a lot of operational and functional risks.

12. **Network security**— Various outsider attacks such as viruses, trojans, worms, hacker attacks, thefts, spywares and denial of service attacks pose the network security threat to an organization's network and data. Generally, these attacks can be prevented through accomplishment of hardware or software security. There are various components of network security such as firewalls, anti-malwares, anti-viruses, virtual private networks (VPNs), and anti-spywares. Network security ensures undisruptive operation flow and helps an organization to meet certain compliance standards. It also prevents consumers' data from thefts and hence preserves the reputation of the business which is the most significant asset of any organization.

13. **Vendor management**— It ensures that the third party service providers adhere to the same information security guidelines which the organization practices because addition of an external entity to the organization's operations makes the system less secure and more prone

to the risk. This can be ensured by monitoring the vendor operations and their daily activities. External certifications such as ISO 270001 also endorse the vendor's operations complying with the security protocols.

14. **Compliance and Audits**— Compliance is set of instructions that ensure that all the rules and regulations laid by the highly accepted prevalent security policies are complied by an organization and its people so that the security goals set by the practitioners are met. Security audits are the official inspections conducted by the experts make sure that all the employees maintain order and compliance. These audits may be internal as well as external conducted by a third party depending on the situations.
15. **IS Governance**— It is the functional and hierarchical distribution of responsibilities to a set of people who are accountable to preserve information security within an organization. The governance structure is so developed that it can support business operations without any disruptions due to security issues. IS governance mainly consists of board of directors and higher IT officials or managers who manage and control the ISMS in an organization. **Fig.1** gives an example of an IS governance structure for Indian banking sector as discussed by IDRBT:

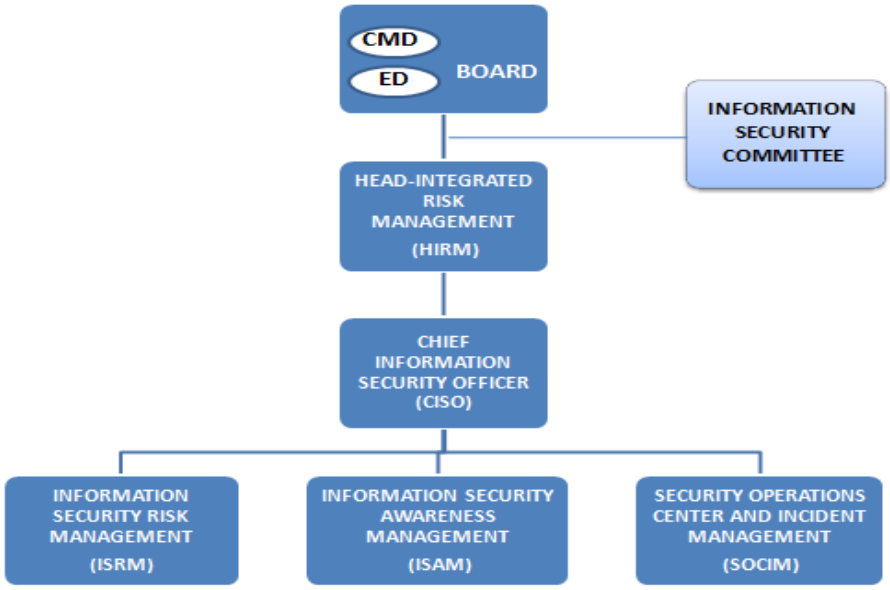

Fig.1 Organizational Chart for IS Governance

16. **Risk management**— Risk management is a process of identifying security threats and vulnerabilities, deciding the counter measures to treat the risk involved and implementing the controls to prevent the operations from being affected. Basically, there are four

components that constitute the risk management: Plan→Do→Check→Act (PDCA model) i.e.

a. Accessing the risk and various security policies and standards
b. Treating the risk using qualitative and quantitative measures
c. Selecting and implementing the controls to mitigate the risk
d. Monitoring the control measures for their effectiveness and repeating the process for another control measure if required

17. **Business continuity assurance**— Business continuity is a mechanism that enables an organizations capability to operate its critical operational units during planned as well as unplanned disruptions such as failures, incidents, natural disasters or catastrophe. The planning is required to be prepared of such situations so that regular and critical operations are not affected. It moreover reduces recovery costs and efforts along with some operational overheads. ISO 22301 defines business continuity as follows:

- Identify and manage current and future threats to the business
- Take a proactive approach to minimizing the impact of incidents
- Keep critical functions up and running during times of crises
- Minimize downtime during incidents and improve recovery time
- Demonstrate resilience to customers, suppliers and for tender requests

18. **Secure system development and maintenance**— It ensures any loss or misuse of information due to operating system and applications is prevented during the SDLC of organization specific software or applications. The process also involves development, testing and production under separate environments to prevent any information loses during any phase. Chief information security officer (CISO) is responsible for coordinating the development, review and approval of system security plans and their execution. Also, Information system security administrator (ISSA) coordinates with the CISO and plays an active role in developing and updating the system security strategies.

METHODOLOGY

The research is based on studies made over IS standard operating procedures of two nationalized Indian banks; ABC Bank and PQR Bank. The work involves development of two case studies, one for each of the two banks. In multiple-case study, evaluation of different IS practices was done on the basis of semi-structured questionnaire. The answers to the questionnaire were taken both as face-to-face interviews as well as in form of written communication. The data collection almost took a month time preceded by the designing of questionnaire and classification of the same according to the different subjects of IS e.g. governance, senior management role, management policy, risk management, compliance and audits, HR roles etc. Thereafter, data

filtration was being performed according to the validity and relatedness of the collected data to the research objective. These case-studies carefully examine the different settings of IS policies and practices in diverse setups. The analysis supported by the studies explains how IS control is distributed among various organizational levels and how it gets shifted from one level to the another depending on the roles and responsibilities of the user.

CASE STUDY: ABC BANK

ABC bank having its most of the operations online now is using the internet for more than a decade and security is the key building block upon which the bank depends. Information security is valued at high level creating operational, financial backing and making it a significant asset to the organization.

Mr. RST, Manager- IT explains, "Financial business can't sustain without security checks. 24x7 monitoring is needed to safeguard the information. If we fail to comply with the security guidelines we can face heavy fines and severe damage to our reputation". According to him, the business integrity, confidentiality and availability of information need to be preserved for giving reliable banking services to its customers. For this, he and his colleague Mr. XYZ, Senior Manager, IT mainly insisted on risk analysis, regular updating the applications and processes, access checks and business continuity. Above all, they also added that ABC Bank is in the final process of achieving ISO/IEC 27001 information security certification that offers a comprehensive approach to the information security. Mr. RST continues, "This certification will assure the customers of our quality of service in security."

Focus at Department of IT, ABC Bank

ABC bank according to its officials represents safety and security. The bank has got a dedicated IS governance that controls the whole idea of information security within the organization. IS governance mainly consists of Board members, Head-Integrated risk management and chief information security officer (CISO). The top management supports resolution of IS issues and is responsible for aligning information security mechanisms with the bank's operational objectives and goals. These officials are also responsible for assessing and implementing new technologies and other measures to preserve the information.

Apart from that, IS issues are discussed and new strategies are devised in the quarterly board meetings. The status of new initiatives taken in the past, security incidents, audit reports and logging reports are being reviewed and analysed in these meetings. Moreover, the top management is also accountable for approval of new projects based on the cost benefit analysis document produces by the cost benefit analysis (CBA) team and risk analysts. CISO directly heads the Information Security team, Risk Management team and Network team.

Information Security team is responsible for continuous monitoring the logs of the tasks performed at different machines and assigning access rights to the employees. Log monitoring is documented monthly or sometimes quarterly in the form of reports and is submitted to the CISO for further review. Moreover, IS team manages login credentials of the employees and other users. They assign a new domain login identity for each employee which is different for each employee. An employee's work is identified by the logs associated with his/her domain login. Also, IS team ensures that all the USB ports of the employees' systems are disabled and they are not able to install any software not even from the internet. Such restrictions are lifted and administrative rights are provided to the employees but for a certain period of time and upon approval from Deputy General Manager. IS team also arranges different training programmes for the employees. Mostly, the trainings are given by the third party trainers and its staff colleges located in different part of the country. Any policy updates, notices or circulars are distributed among the employees via group emails and updating the bank's portal. If some updating requires personal communication or trainings, then these trainings are mainly provided to the "*Zonal Officers*" which communicate the same to the respective employees of their branches. Generally, policy is updated annually by the experts in month of April, at the start of the every financial year.

On the other hand, *Risk Management (RM)* team performs risk analysis against the cost involved for the newly proposed projects. Also, if some security incident is reported, RM team analyses the criticality of the incident and performs root cause analysis (RCA) of the incident. If it is found that the incident is highly critical or something erroneous has been done intentionally by some employee, strict actions (sometimes termination from services) are taken against the offender. Whenever an employee is terminated or leaves the organization, it is immediately intimated to the IS team so that his/her login credentials can be deleted instantly.

Network team plays a crucial role in preserving IS over the internet and business continuity through disaster recovery and high availability multiprocessors. This team monitors business support network fluctuations and provide the maintenance as per the needs. In case of emergencies such as floods, famines or any other hazards that affect server availability, the network load is shifted to Disaster Recovery (DR) server set up at a different location in India itself. DR servers are the clones of primary servers. If any update is made on primary server it is available to the secondary (DR) server within few minutes. Moreover, the team ensures that antivirus and system updates are installed periodically throughout the organization systems. Network team also maintains multilayered hardware and software firewalls which prevent unauthorized accesses, misuse, modification and implements denial to the irrelevant or malicious webpages.

Other Implementations

Besides the roles and responsibilities of different security teams discussed above, there are various IS practices which have been adopted by the ABC Bank. These practices are –

1. **Security at Data Centres—** Data centres are much more secure than any other area. Access to these areas is provided to just a few members and that too under high security protocols. A person must possess access cards as well as biometric access to enter these areas. Data centres are under 24x7 video surveillances by the highly specialized teams. Also, the CCTV videos are reviewed every three days by the security administrator to avoid any pilferage.

2. **Maker-Checker for Financial transactions—** This concept ensures that a transaction made by any employee using his domain credentials is complete only if any other official approves the same by logging in with his/her credentials. Dual member transaction processing prevents chances of frauds and insider's threat until a person possesses the credentials of both the parties. In this way, implementation of Maker-Checker model has made the system more secure and effective.

3. **Job segregation—** Theory of job segregation avoids task dependency. Also, whenever an employee is on leave, he may handover the task to the other employee so that operational continuity is not affected. Moreover, job segregation accounts to distribution of accountability. If a user is using other person's credentials and perform some misconduct, the person whose credentials were used will be accountable for the delinquency. So, sharing of passwords and systems has been reduced owing to this concept and this has resulted in the lowering of risk and reduction in number of security incidents.

4. **Compliance Policy—** Every new employee is provided with the IS policy document and has to sign "Acceptance Use Policy" which refers to the statement that "I shall abide to all rules and regulations mentioned in the above policy document. In case, I fail to comply by the foresaid guidelines, I am liable to be lawfully trialled" i.e. organization is free to take legal actions in case an employee is found indulged in any wrongdoing. Also, it includes the provision for check compliance through use of monitoring methods.

5. **Security Auditing—** ABC Bank takes the help of third party auditors such as Deloitte and KPMG to execute security audits within the organization. Third party auditing ensures that any cognitive biasing can be prevented during the time of inspection. This makes the process more efficient and effective.

6. **ISO/IEC 27001—** ABC Bank has lately applied for ISO/IEC 27001 security certification that covers improved security for the bank as well its clients. It also gives assurance of best

practices to the bank's stakeholders and enhanced security awareness among the staff members. Firms like Deloitte Consulting India Private Limited performed the GAP analysis for the same and has helped the bank to potentially improve its security processes. As a part of the progression, the operations, processes and different standards of the organization have been documented in the recent past. ABC Bank has finally reached the concluding stage of this accreditation and will soon be known for its quality of security.

7. **HR Processes—** Human Resource team has also played a significant role in maintaining the IS standards in ABC Bank. While recruiting a new staff, including contractors, temporary staff and cleaning staff, the HR team is responsible for arranging police verification of these people against any criminal act. Also, when an employee resigns from the bank, he is closely monitored for a notice period of 3-months as he may not be involved in some misconduct while leaving the bank. HR officials also ensure that all the credentials are deleted and all the assets including the access rights assigned to the employee are taken back on last day his/her service.

The bank has since planned and prepared for the IS implementation, it has achieved its goals of having an effective Information Security Management System and reached a level of being certified to ISO/IEC 27001. As for the future, further focus of ABC Bank is to update its processes periodically and manage the insider's threat which is still a major issue for the whole banking industry as observation and control of human mind is much more complicated. Another concern of the ABC Bank security team is to control and manage the tailgating issue. It is sometimes authorized and sometimes unauthorized depending on the circumstances but it is a serious subject as managing access for visitors is a complex task. The bank has a proper control mechanism for controlling such problems for the employees and the 3rd party staff but visitors are often accompanied by some of the staff member possessing the access cards to the working space. It is officially a legal tailgating case but may be a potential threat to the organization's security. The bank is looking forward to overcome this problem and come up with a resolution in the near future enhancing the security control mechanism.

CASE STUDY: PQR BANK

PQR Bank is a premier bank owned by government of India. As the bank insists on Tech-Friendly banking, it needs strong information security network to safeguard critical data and information. Being a baking institution, PQR processes large amount of sensitive data which makes it to regulate at highly regulated environment than other sectors.

BALANCING OF RISK & CONTROL

Basically, a large amount of sensitive information is present in an organization. This may be in the form of personally identified information, banking details such as balances or history, confidential corporate information, etc. But, how is this information secure in PQR Bank? Mr. LMN, a bank official explains "The biggest threat to the information is unauthorized disclosure and access. But, the bank has a separate Information Security policy to safeguard its critical data and these policies are reviewed periodically." Mr. LMN identified some measures to ensure the availability and security of information that the bank needs to carry out the business operations effectively. The main focus areas were physical access security mechanisms, control mechanisms for IT system and services, management support to implement IS and inclusion of a clause related to compliance with bank's security policy in contract for 3rd party partners. He was determined that these measures are business oriented, risk based and cost effective. With this in mind, PQR Bank is also in the process of getting certified for ISO 27001 which is an international standard that covers planning, implementation, monitoring and improvement of an Information Security Management System (ISMS) (Zames Zhou, 2011). PQR Bank is technology oriented and thus focussed on creating a security environment within the organization. Mr. LMN continues, "Bank regularly provides education and updates on information security to its employees. In addition, the information security implementation team carries out the awareness programs for the employees. Besides, Acceptable Use Policy (AUP) is also provided to the employees at the time of joining and updated periodically and compliance is received." AUP includes set of rules and regulations applied by the bank and the provision for check compliance through use of monitoring methods. It is often asked by the new members of the bank to sign an AUP before they are given any access to the bank's information systems.

Although, PQR Bank has a secure environment but incidents of non compliance can occur any time accidentally or intentionally. This may result in severe penalties to the bank in the form of financial, reputational and customer loss. Regarding this, Mr. LMN added, "Bank conducts regular audits annually and remedial measures (if required) are completed periodically. To prevent Cyber-attacks and Malware, Firewall and Intrusion Detection System (IDS) have been implemented in the network. Anti-virus software is also deployed in all PCs and Servers in the bank." Bank also has an incident reporting tool to register and manage the incidents. He added "The incidents are logged into the system, assigned to line managers and escalated as per the predefined procedure and the criticality of the incident."

He continues, "Business continuity is the important asset of a banking institution. Business Continuity Plan and Disaster Recovery Plan (BCP DRP) are available and tested periodically by conducting drills." This plan testifies how the business will continue its operations after the disaster. According to him, the bank's governance structure and role distribution plays a significant role in effective implementation of ISMS. Management is also very supportive and

regularly takes updates on implemented processes and procedures. He says, "Bank has a Chief Information Security Officer (CISO) under whom the security implementation and monitoring and audit teams are working. At operational expenditure (opex) level the audit committee of the board reviews the IS Security governance."

COGNITIVE INTERVENTION

The bank has worked to optimize its security protocols and procedures in the recent past and looking forward to continue the same in the coming times. There are however still many challenges involved in the people and processes. In developing countries like India, new processes can evolve and succeed if there are some human elements involved that can motivate participants to adopt such practices. It is an appropriate metrics that can frame a secure effective system and can result in a significant good customer experience. Culture, ethics and behaviour of individuals and bank frame the base of success in the organization structure.

OBSERVATIONS AND FINDINGS

Based on the above studies, several inferences and IS improvement mechanisms have been analysed in this section. The research learning has been classified under three-major categories as follows:

- Need for elaborative ISMS implementation model
- Understanding IS control flow within the organization
- Overcoming tailgating or piggybacking issues for visitors

Extensive ISMS PDCA Model

Currently, the organizations generally adopt the well known PDCA process approach practiced by ISO/IEC 27001 ISMS standard. PDCA model basically emphasises on-

- PLAN-designing and establishing the ISMS,
- DO- Implementing and deploying the ISMS,
- CHECK- Monitoring and reviewing the ISMS and
- ACT- improving and updating the ISMS

It is not always easy for an organization to understand the model as the above model doesn't really describes the processes and activities involved at each phase of the cycle. Such problem often results in adopting an ISMS implementation plan that may be unrelated to the business objectives. Unclear vision tends to ineffective and inefficient ISMS which imbalances the involved costs and benefits of the project. As a matter of fact, the whole purpose of implementing an ISMS is diluted in such circumstances. Therefore, based on our research and

findings, we have come up with an elaborated enhanced PDCA cycle (**Fig.2**) that is based on standard PDCA implementation approach but provides a clear picture of procedures at each stage of the cycle.

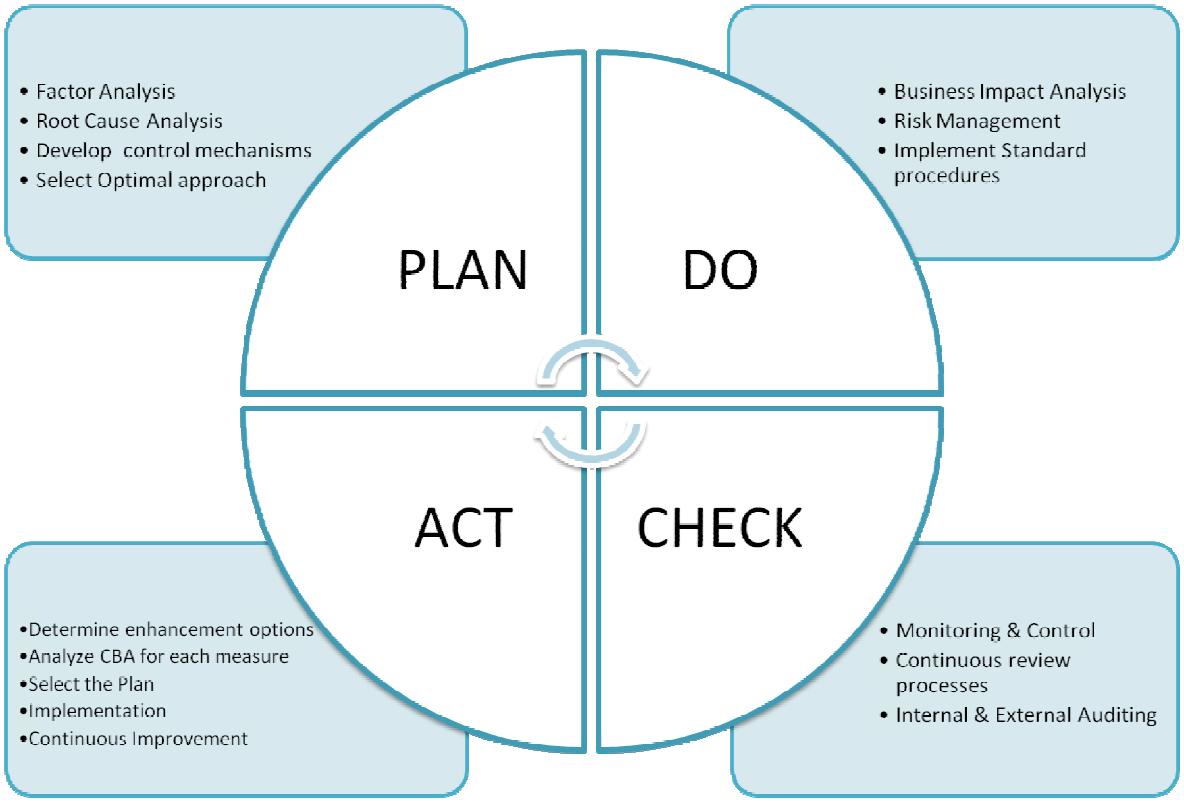

Fig.2 Extensive ISMS PDCA Model

Here, each stage is divided into control areas which provide a comprehensive coverage of organizational requirements for managing the Information Security. The model also aligns the business objectives and processes with the risk management across the business involving people, information, processes, services and organization assets. Unlike basic model, it also involves continuous improvement since implemented processes and systems are regularly monitored for they are functioning efficiently and if they are not, then improvement controls are executed.

Understanding IS control flow within the organization

An organizational system enforces a control to authorize any access to the space or information in interconnected systems. Any object is allowed to move within the information system when it is recognized by the regulating authority. The purpose of IS control is to overcome the IT security issues due to environmental changes, organizational complexity, costs and human resources.

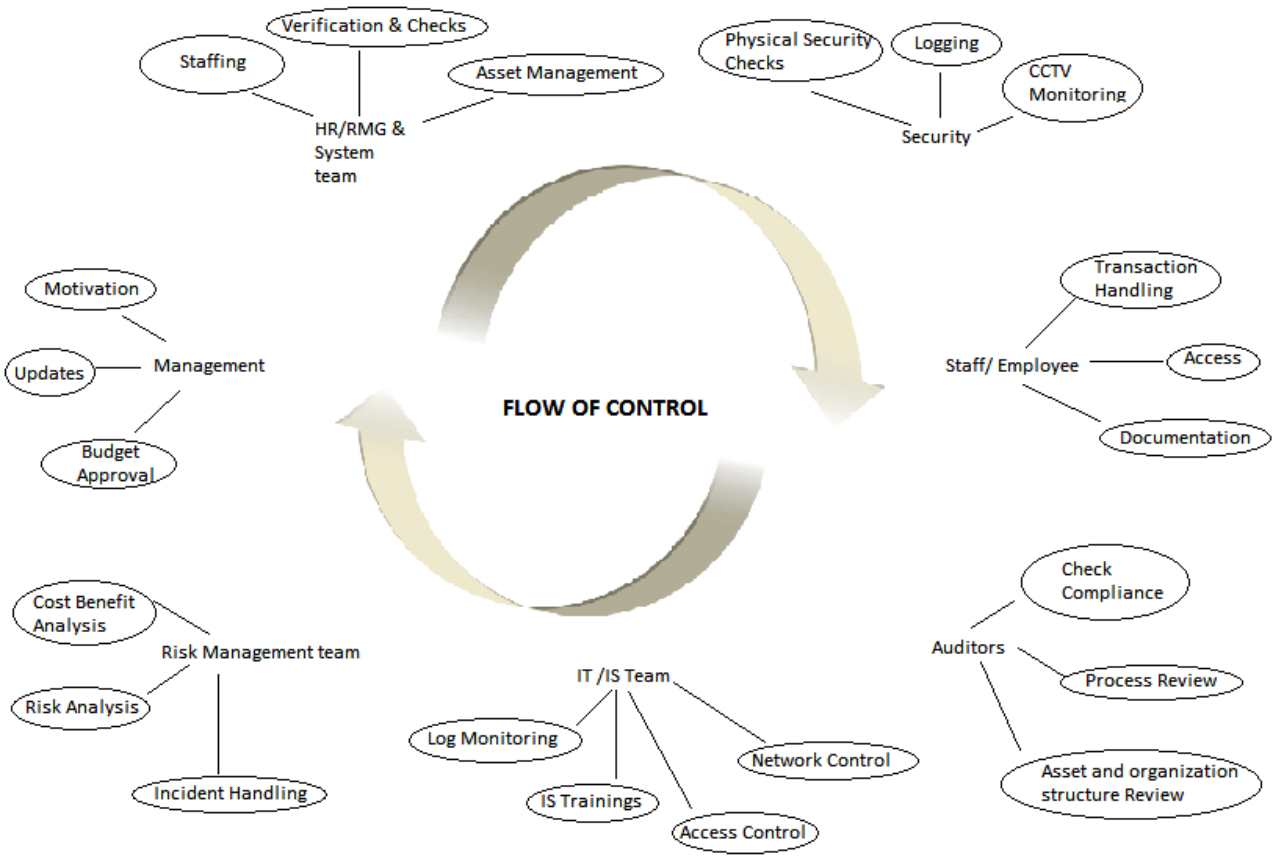

Fig.3 Adaptive IS Control Model

The diversity in security attributes on information is unmanageable in a central system. It's the distributive nature of a IS control that binds the multiple systems and its resources together. The process of this control shift is named as "*Adaptive IS control model*" that describes that control in a system adapts itself according to the IS domain e.g. Risk management team has the control of the system while performing cost benefit analysis or risk analysis or incident handling. Similarly, control shifts to an auditor while he is reviewing the organizational processes and structure or checking the compliance. The detailed flow of IS control has been described in the **Fig.3**. Here, the model describes how different security handling domains perform their work which is distributed according to the functionality.

At each level, IS control evolves with the roles, responsibilities and accountability of the participant of the system. It is the distributed IS control in interconnected systems that makes an effective and efficient ISMS and helps in preserving the confidentiality, availability and integrity of critical information of an organization. Adaptive IS Control can also be used for rewarding the employees when the actions comply with the standards. It acts as the facilitator and can add further as a motivation factor in implementing an ISMS. Although, there are always the reasons

for resistance to the control but encouraging employee participation and developing the verification procedures since initial stage are to best way to overcome such problems.

Overcoming tailgating or piggybacking issues for visitors

Tailgating is the most common security breach that starts out innocently with an employee opening the door with his access and some others follow him entering a working area. The problem becomes unnoticeable when a visitor without access badges or cards are accompanied with an employee having the access. His entry and exit to the doors is unnoticeable even when his data is recorded at the doors. Inaccuracies in record keeping are least avoided when security incidents are involved. Such things open the building and information to sabotaging, theft and vulnerabilities. Not all the visitors are threat though but overcoming uncertainties is desirable for any firm and that too, when uncertainties are related to security. There are many measures that have been taken to prevent such issues e.g. long range readers, camera analytics, air locks, etc. But, In India, most of the firms are untouched with the multilevel security. Relying on the above measures to prevent security and allowing piggybacking of visitors make the environment and data unsecure. There must be a smart card access that should be allotted to the visitors. These smart cards can bear multiple credentials on one card. Also, the access of the visitors can also be restricted by manipulating the access areas from the security desk. The detailed flow of the method can be well seen in **Fig. 4.** The system can be made more secure by assigning a unique area code for each door and mapping the visitor details to these required access area codes. All these mappings can be stored in these smart cards and these cards should be assigned to the visitors for authorized and identified access. Although anti-tailgating systems are not required at every door and for such areas standard control is not required as system should prevail just to address a problem and not creating any new problems.

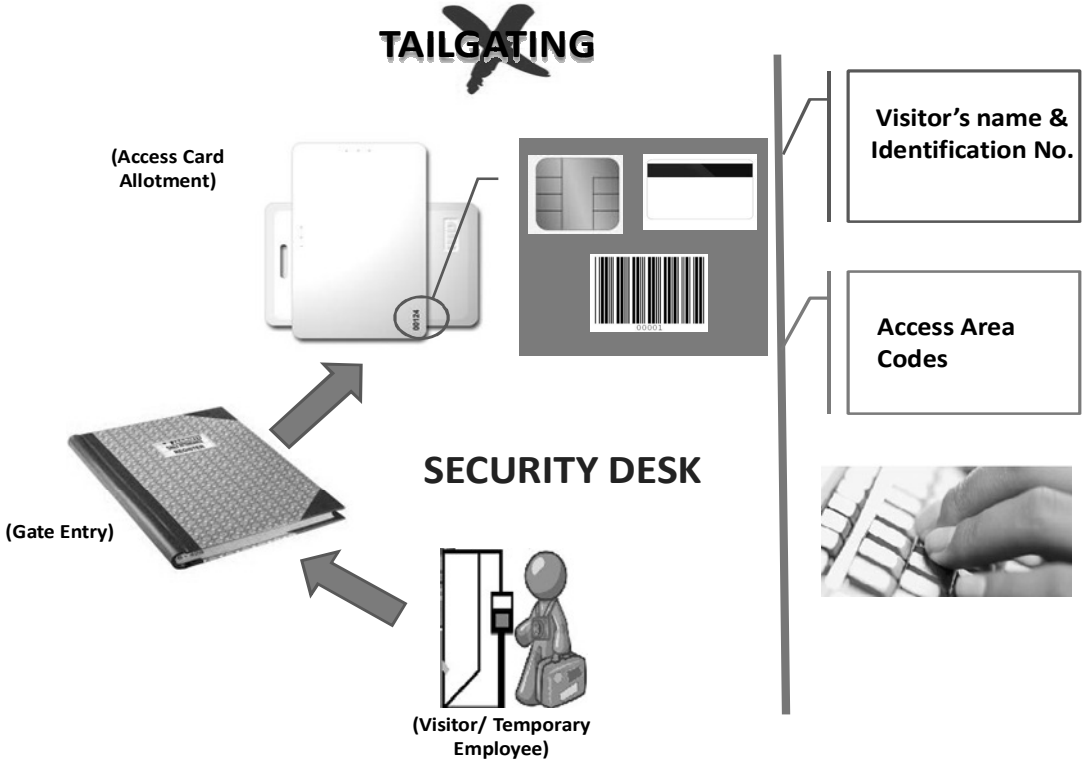

Fig.4 Preventing tailgating of visitors in an organization

CONCLUSION

There have been various contemporary technical controls to secure the information and many control measures are still to implement but there was and will always be a need for secure environment and culture to practice these controls effectively. A secure system requires a sense of understanding and awareness among the people. Information Security is implemented as a control but it should more be a responsibility. Technology keeps on evolving with time but the people and the environment are long lasting. There is a need to adopt a sustainable security culture in Indian banking and other financial institutions so that fear of IS risk and investments on the same can be controlled for a better and secure future customers and their trust.

REFERENCES

1. Nosworthy, J. D. (2000). Implementing information security in the 21st century - do you have the balancing factors. Computers & Security, 19 (4), 337-347.
2. Ward, P., & Smith, C. L. (2002). The development of access control policies for information technology systems. Computers & Security, 21 (4), 356-371.
3. Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. Information Management & Computer Security, 17 (1), 4-19.
4. Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2010). Factors influencing information security management in small-and medium-sized enterprises: a case study from Turkey. International Journal of Information Management, 31 (4), 360-365.
5. A conceptual framework for information security management by Thomas Finne.
6. Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behavior through dialogue, participation and collective reflection: an intervention study. Computers & Security, 29 (8), 432-845.
7. Chang, E. C., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106 (3), 345-361.
8. Germain, R. S. (2005). Information security management best practice based on ISO/IEC 17799. The Information Management Journal, 2005 (July/August), 60-66.
9. Höne, K., & Eloff, J. H. P. (2002). Information security policy: what do international information security standards say? Computers & Security, 21 (5), 402-409.
10. Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: the critical role of top management and organizational culture. Decision Sciences, 43 (4), 615-659.
11. Humphreys, E. (2008). Information security management standards: compliance, governance and risk management. Information Security Technical Report, 13 (4), 247-255.
12. Kankanhalli, A., Teo, H. K., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23 (2), 139-154.
13. Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: an organizational-level process model. Computers & Security, 28 (7), 493-508.
14. Ma, Q., Johnston, A. C., & Pearson. J. M. (2008). Information security management objectives and practices: a parsimonious framework. Information Management & Computer Security, 16 (3), 251-270.

15. Stan Stahl, Kimberly A. Pease (January, 2007). Effectively Managing Information Security Risk: A guide for executives- Citadel Information Group, Inc
16. Karin Hone, J.H.P. Eloff. Information Security Policy. What do International Information Security Standards Say?
17. An Overview Of Information Security Standards, February 2008, The Government of the Hong Kong Special Administrative Region
18. Teresa Susana Mendes Pereira, Henrique Santos (2010). A Security Framework for Audit and Manage Information System Security
19. James Zhou (2011). ISO 27001 Information Security Management
20. IDRBT, IT Governance series Journal. Information Security Governance for the Indian Banking Sector
21. ISO/IEC 27035:2011 Information technology-Security techniques-Information Security Incident Management
22. K.K. Mookhey, Gopalakrishna Committee 2011. RBI Guidelines : Report of the Working Group on Electronic Banking