IMPORTANCE OF CYBER SECURITY AUDIT AND ASSESSMENT ON BANK

[1]Vibhisha Ghodasara, [2]Chandresh D Parekh
[1]M.Tech, Raksha Shakti University, Ahmedabad, Gujarat, India
[2]Assistant Professor, Raksha Shakti University, Ahmedabad, Gujarat, India

Abstract: With rising risks of cyber threats, banks face an unprecedented challenge of data breaches and thus reinforce their cyber security positions. The cyber - attack threat is substantial and continually evolving. Cyber - attacks that can result in financial and reputational losses. Many audit committees and boards have set internal audit expectations to understand and evaluate the bank's ability to manage the associated risks. A cyber security audit focuses on cyber security standards, guidelines and procedures and the implementation of such controls. Other operational audits also rely on the cyber security audit. The Paper examines the role and importance that internal audit and internal controls have in bank.

Index Terms **- Internal audit, Framework, Internal Policies and Procedure, standards and Controls, Risk management, Compliance, business objectives**

I. INTRODUCTION

Customer expectations, technological capacity, regulatory requirements, demographics and economics are creating a crucial change together today. This leads to the need for banks to tackle these challenges and take a proactive approach to security. Banks ' use of technology has been gaining momentum ever since. On the other hand, the number, frequency and impact of cyber incidents / attacks has increased many times in the recent past, more so in the case of the financial sector including banks, emphasizing the urgent need to put in place a robust cyber security / resilience framework at banks and to ensure continuous adequate cyber-security preparedness among banks. Given the low entry barriers, evolving nature, growing scale / velocity, motivation and resourcefulness of cyber-threats to the banking system, it is essential to enhance the banking system's resilience by enhancing current defenses in addressing cyber risks. These would include, but not limited to, the establishment of an adaptive Framework for Incident Response, Management and Recovery to address adverse incidents / disruptions when and when they occur.

Here are the reasons why cyber security in banking is important and why it should matter to you–

It seems that everyone is going cashless, using digital money, i.e. Debit and credit card. In this context, ensuring that all cyber security measures are in place, protecting your data and your privacy, becomes very important. Infringements of data can make confidence in financial institutions difficult. This is a serious issue for banks. A weak cyber security system can amount to breaches of data that can easily cause their customer base to take their money elsewhere. When a bank's data is breached, you often tend to lose time and money. It can be time consuming and stressful to recover from the same thing. It would involve cancelling cards, checking statements, and keeping complications in your eyes open.

In the wrong hands, your private data can do a lot of harm. Even if the cards are cancelled and fraud is taken care of immediately, your data is sensitive and can reveal a great deal of information that could be used against you. Banks need more than most firms to be on their guard. This is the cost of keeping valuable personal data that banks do. If not protected from cyber-crime threats, your bank data may be infringed.

II. LITERATURE REVIEW

1. The standard of the International Organization for Standardization 2700X provides guidance on organizational information security standards and information security management practices including the selection, implementation and management of controls, taking into account the organization's information security risk environment. ISO charges the access to this standard.

2. National Institute of Standards and Technology (NIST) Special Publication 800-53 provides controls on federal information systems, but it may be used by commercial entities. NIST provides the 800 Cyber Security Framework (CSF) and the Federal Information Processing Standard. There is no charge for access to the standard.

3. Initially developed by SANS, the Internet Security Center maintains a standard of 20 controls. There is free access to this standard.

4. The Information Systems Audit and Control Association provide COBIT with the information security framework. Aligned with ISO 27000 series, Information Security Forum standard, and BMIS. A charge is applicable for access to the standard.

5. The Data Security Standard of the Payment Card Industry Security Council, a joint venture between major credit card companies, is a set of policies and procedures aimed at enhancing card transaction security. Compliance is mandated by the credit card companies. In addition, some state laws either refer to it or mirror some of the standard's aspects.

6. The Cloud Security Alliance provides the Critical Focus Security Guidance for the adoption of cloud computing technology in cloud computing v4.0 to enhance security and mitigate risk.

7. According to Cai Chun (1997), the internal audit function is a vital and controversial issue in the theory and practice of global auditing. There was a widespread view in the Western auditing circles that internal audit is an independent evaluation function.

8. In June 1999, the Institute of Internal Auditors (IIA) officially adopted a new definition of internal auditing function. The Guidance Task Force has developed the new definition and defines the function of internal audit as:' an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization achieve its objectives by providing a systematic, disciplined approach to assessing and enhancing the effectiveness of risk management, control and governance processes (IIA, 2001)

9. According to Symantec, today's organizations need to address four major IT risks: safety risks, availability risks, performance risks, and compliance risks. Security risks are unauthorized information access: data leakage, privacy, fraud, and endpoint security. The security risks also include wide-ranging external threats such as viruses and more targeted attacks on specific applications, specific users and information.

10. ASQ (American Quality Society) describes internal audit as a first-party audit. ASQ (American Quality Society) is performed within an organization to measure its strengths and weaknesses against its own procedures or methods and/or external standards adopted by (voluntary) or imposed on (obligatory) the organization.

III. CHALLENGES

(1) Strict compliance regulations: it has become extremely challenging for banks to manage regulatory compliance. The volume of regulations has increased dramatically over the past couple of years. Smaller banks are also required to fulfill the regulatory obligations along with the larger banks. (2) The struggle to secure customer data: there are a number of ways in which infringements of privacy can occur in the banking sector, such as stolen or loss card data, unauthorized data sharing with third parties and the loss of personal data of the customer due to improper security measures. (3) Risk of third parties: banks must exercise due diligence on third parties with whom they are associated. As per the data security standard of the payment card industry, any critical issues related to the card data environment must be reported to the bank by third parties. (4) Evolving cyber threat landscape: technology development leads to the latest cyber threats, such as ransom wares of the next generation, web attacks, etc. The exponential growth of India's digital payment platform and the push toward a cashless economy has re-focused on the need to reinforce cyber security posture.

Few of the major challenges faced by banks include: transaction fraud: technology for fraud detection should be in place with due consideration of risk based on business factors. Secure SDLC: Banks need SDLC security to incorporate banking products and applications.

IV. FRAMEWORK

The current digital society has high expectations of flawless customer experience, on-going availability and effective data protection. For all public and private organizations, as well as for wider society, information assets and online services are now strategically important. These services are vital for a vibrant digital economy to be created. They also become systemically important for the economy as well as for wider national security. All of which highlights the need to protect sensitive data and transactions, thereby ensuring confidence in the financial sector as a whole.

The stakes are high with respect to the confidentiality, integrity and availability of information assets, and the application of new online services and new developments (e.g. mobile app, web app); while improving resilience to cyber threats. The dependence on these services is not only increasing, but the threat landscape is changing rapidly. The financial sector recognizes the rate of evolution of cyber threats and risks, as well as the changing technology and business landscape.

The objectives of general security include the following:

Confidentiality –Information assets are only accessible to those authorized to access them (i.e., protected against unauthorized disclosure or (un)intended leakage of sensitive information).

Integrity –Information assets are accurate, complete, and correctly processed (i.e., protected from unauthorized modification, including authenticity and non-repudiation).

Availability –If required, information assets are resilient and accessible (i.e., protected from unauthorized disruption).

What is the Cyber security Framework?

The Framework provides organizations with a compilation of guidelines based on risk that can help them identify, implement and enhance cyber security practices. Instead of introducing new standards or concepts, the Framework leverages and integrates cyber security practices developed by organizations such as NIST and the International Organization for Standardization (ISO). The Framework will be used to evaluate the maturity level periodically and evaluate the effectiveness of the banks ' cyber security controls and to compare them with other banks. The framework is based on RBI's banking requirements and industry cyber security standards.

The Framework refers to this compilation of practices as "the core." This core consists of five concurrent and on-going functions— identifying, protecting, detecting, responding, and recovering — that provide a strategic view of the lifecycle of cyber security risk management by an organization. Furthermore, each function is divided into categories linked to programmatic needs and specific activities. Furthermore, each category is divided into subcategories pointing to informative references. These references refer to specific sections of standards, guidelines and practices which illustrate a method for achieving the results associated with each subcategory.

The five functions represent the key elements of effective cyber security. Identify helps organizations gain an understanding of how systems, assets, data, and capabilities can manage cyber security risks. Protect helps organizations develop the necessary controls and safeguards to protect against or deter threats to cyber security. Detecting are the steps organizations should consider taking to provide proactive and real-time alerts of events related to cyber security. Responding helps organizations develop effective responses to incidents. And Recover is the development of continuity plans so that after a breach, organizations can maintain resilience — and return to business.

FUNCTION	CATEGORY
IDENTIFY	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
PROTECT	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
DETECT	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
RESPOND	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
RECOVER	Recovery Planning
	Improvements
	Communications

V. REGULATORY PERSPECTIVE

To ensure security in banking industries, the Reserve Bank of India removed a Circular, where all banking institutions have to comply for. Some of the key features of the regulations are: (1) Cyber Security Policy to be distinct from the broader IT policy / IS Security Policy of a bank. (2) Arrangement for continuous surveillance. (3) Comprehensive network and database security. (4) Protection of customer information. (5) Cyber security preparedness indicators. (6) Cyber Crisis Management Plan (7) IT architecture should be conducive to security. (8) An immediate assessment of gaps in preparedness to be reported to RBI. (9) Cyber security awareness among stakeholders/ Top Management/ Board.

VI. POLICES

Cyber Security Policy provides an integrated set of protection measures to be applied consistently across banks to ensure a secure operating environment for their business operations and provide the IT Assets with the necessary security controls. Customer information, bank information, IT systems support, processes, and people that generate, store, and retrieve information are important bank assets. Information availability, integrity, and confidentiality are critical to building and maintaining our competitive edge, cash flow, profitability, legal compliance, and corporate image.

Cyber security policies have been framed at Bank, taking into account the security requirements, based on a series of security principles. All policies on cyber security and their need were addressed below:

- Asset Management Policy
- Risk Management Policy
- Data Classification Policy
- Incident Management Policy
- Control of Software Installations
- Physical & Environmental Security
- Network Security Policy
- Secure Configuration Policy
- Anti-virus and Patch Management Policy
- Access policy
- Audit logging and Monitoring Policy
- Security Monitoring Policy
- Remote Access Policy
- E-mail Security Policy
- Removable Media Policy
- Policy on Secured Discard of IT Assets
- User/Employee/Management/Customer Awareness Policy
- Backup and restoration policy
- Contract and Vendor Management
- New Technology Adoption Policy

VII. COMPLIANCE WITH CYBER SECURITY POLICY AND PROCEDURE

All facilities for the processing of assets and data shall be used in accordance with cyber security policy and acceptable policy of use. While bank respects its employees ' privacy, it reserves the right to audit and/or monitor its employees ' activities and information stored, processed, transmitted or handled on any assets / devices / services employees use. The exception to the security policy and procedure is approved through the process of exception management. Policy exceptions shall be reviewed at least annually on the basis of anticipated safety risks, emerging threats, etc. as deemed necessary. Violations or attempted breaches of security policies and procedures will result in disciplinary action.

VIII. AUDIT PLAN

The main objectives of a security audit are: to check the existence of security framework, policies, standards, guidelines and procedures; to identify deficiencies and to examine the effectiveness of existing policies, standards, guidelines and procedures; to identify and understand existing vulnerabilities and risks;

Security audits should be conducted periodically (vulnerabilities and threats change with time and environment) to ensure compliance with security policy and to determine the minimum set of controls required to reduce risks to an acceptable level. The audits may include new installation / improvement audits, regular audits, random audits or non-office hour audits. The techniques used in the audit process may include automated auditing

tools (ready-made security audit systems and/or tools developed by the own security auditors) or manual auditing techniques (e.g. social engineering attacks and audit checklists) may exist.

There may be several steps in an audit process. Networks proposed an audit process in seven steps (1) vulnerability scanning— infrastructure scanning, (2) auditing reports such as logs, reports on intrusion detection systems, etc., (3) security architecture auditing— auditing the existing security architecture, (4) baseline auditing — auditing the security setup to verify that it conforms to the organization's security baseline, (5) auditing the security setup.

During and at the end of the audit process, a series of reports can be drawn up: a report with the vulnerabilities identified in the information system of the organization, a report with the threats and risks that the organization faces as a result of the existing vulnerabilities, including faulty policy, architecture, etc., and an audit report that provides a security overview and the results of the audit process.

IX. CONCLUSION

Audits shall be conducted to ensure compliance with policies, procedures and guidelines on cyber security. To prevent possible misuse of tools, the use of information systems audit tools shall be controlled and authorized. With the increasing complexity of information systems, the security audit process is becoming more difficult to undertake. Internal or external, a safety audit is one of the best ways to determine the effectiveness of security.

REFERENCES

1. ISO, The ISO 27000 Directory, 2009, Retrieved 2010, from http://www.27000.org/
2. Calder, Information Security Based on ISO 27001/ISO 27002 - A Management Guide (2nd ed.), Zaltbommel: Van Haren Publishing, 2009.
3. The Payment Card Industry security council's Data Security Standard.
4. Networks, 3., Security Audit. Retrieved 2010 February, from Scribed, http://www.scribd.com/doc/12734608/ Security- Network-Audit Steps.
5. The National Institute of Standards and Technology's (NIST) Special Publication 800-53 provides controls for federal information standard. https://nvd.nist.gov/800-53
6. The Information Systems Audit and Control Association offer the COBIT framework for information security. http://www.isaca.org/COBIT/pages/default.aspx.
7. NSAA and GAO. (2001, December). Management Planning Guide for Information Systems Security Auditing. Retrieved January 2010, from U. S. Government Accountability Office, http://www.gao.gov/special.pubs/mgmtpln.pdf