ISSN No. 0976-5697

Volume 4, No. 8, May-June 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Developing Evaluation Criteria for end Users to Establish the Compliance Fitness of IT Governance in Indian Banking Industry

Anand Mohan Sharma
MBA (IT) Indian Institute of Information Technology
Allahabad India
Imb2011029@iiita.ac.in

Mayank Kushwaha
MBA (IT) Indian Institute of Information Technology
Allahabad India
Imb2011022@iiita.ac.in

Madhvendra Misra
Faculty Member
Indian Institute of Information Technology Allahabad India
madhvendra@iiita.ac.in

Abstract: Banking Sector has made major Investment in its IT Infrastructure to support their banking operations and concerned about the security and privacy of their customer's data. It has seen that banking industry has also high dependencies on third party service providers and vendors for IT support. Banks which are situated in metro cities and Urban region has a structured procedure of IT operations and do regular IT audits, but it has been seen that most of the banks which are far from the city or situated in rural areas does not take it seriously and could not conduct a regular IT audit for their banking processes which may sometimes affect and Question the Banks loyalty on behalf of the security transactions and privacy of a customer data. This paper would derive the factors and criteria on which the banks can evaluate their IT Fitness to ensure the credibility of their Business functions.

Keywords: component; IT governance, IT security, RBI, IDRBT, Cobit, ISO 270001

I. INTRODUCTION

Banking Industry in India is the core business domain which supports other business function within the country. Today every bank is facilitated with IT organization Structure according to its business needs to operate efficiently and effectively. Indian banking Industry governing body "Reserve Bank of India" has done lot of work in term of IT Governance implementation. A guideline Regarding Information technology, Electronic banking, Technology Risk management and cyber fraud was provided to implement in all commercial bank by Reserve bank of India in 2011. Guidelines basically given for Information Technology Governance, Information security, IT Operation, IT services outsourcing, Information security Audit, Cyber Fraud, business continuity Planning, Customer Education, Legal Issue. All this individual unit of IT is critically important for the proper functioning of Banking Industry. For Implementation of these Technical Guidelines Reserve bank of India used best practices. COBIT (Control Objective of Information and Related Technology) and ITIL (Information Technology Infrastructure Library) is proposed for the implementation of IT governance. ISO 27001-2005 is for implement, monitor, maintain and regular improvement of Information Security Management System and ISO 27002-2005 provide the steps which are used for the development of ISMS. In this research paper we are proposing some critical criteria are on the basis of which fitness level of the compliance can measure.

The Information and supporting processes, networks and servers which are used for generating, receiving, storing and retrieving information and the people are important business assets of an organization, especially if we talk about the Indian banking system whose policies and regulations have been defined by the Reserve Bank of India. The Confidentiality, Integrity, Availability and Accessibility are essential for any financial Organization to maintain its competitiveness and effectiveness and also it ensures the credibility of the Governance aligning the business objective of the Banks and the stakeholders.

II. LITERATURE REVIEW

IT governance, ITIL, ISO 27000 family standards are the best practices which are globally accepted and implemented in banking Industry. Global Banking industry in the developed countries have already Implemented the Information system according to the best practices to provide potential edge to the business model of banks. Indian Baking sector is still working on the guidelines provided by Reserve Bank of India regarding Implementation of information system. Re-engineering the whole process and aligning Information technology model with the business model of banking sector to add intelligence factor to banking business process.

Reserve bank of India has a separate research and development wing IDRBT (Institute of Development and Research in Banking Technology). IDRBT has come in existence in 1996 after the recommendation of Reserve bank of India committee in 1994. In 1989 Dr. Rangarajan Committee

recommended the computerization of banking Industry which brought out the need of a national level institute for banking industry. IDRBT prior work are in the field of Networking, security, Soft computing, data Mining and the current research project which are undertaken by IDRBT are financial networks and application, Electronic payments and settlement system, security technology for financial sector, financial information system and business Intelligence.

IDRBT has also worked on IT Governance and Information security governance for the Indian banking Industry. **[5]** In the series of technical draft for IT and Information security governance IDRBT used the internationally accepted best practices COBIT (control objective of Information and related technology) and ISO 27000 family.

If we talk about Governance in our Banking system then it is still not as much resilience as it should because of the poor IT infrastructure, legacy policies, less Volatile environment(In terms of Physical risk) and Unstructured Internal Infrastructure. Yet after the strong RBI Regulation and some amendment in SOX Specially in section 404,409,802 which is related to the IS, HIPPA and PCI Compliances have been adopted by the Indian Banking system and these compliance are essential to mitigate the operational risks & Financial risks of these institution and keep the Banks to continue the process without any disruption. Although fulfillment of all the laws and compliances does not ensure the risk free process or 100% resiliency of the system but how much effective of these compliances is? And whether all compliance is essential for every bank? And whether the risk appetite policy of the respected institute is right or it needs some technology up gradation and how we check the fitness of these compliances in the Banks.

According to Gartner's assumption of Strategic Planning (2011), 15% of 2000 Global enterprises, by the end of 2015 will have transformed their Business Continuity Management program into a cross-enterprise business operations strategy and planning function. The Bank's main objective is to securing of financial details of their customers and providing them a secure environment to perform transactions.

So all the Banks & Financial Institution must have to be fulfill all basic Compliances and do Audit of their BCP program. Therefore we try to evaluate the fitness of the existing BCP system with respected to the IT Governance Compliances in our Banks. We only select those critical & important compliances which incorporate with their operational risk and which are integrated with their IT automated system like IT infrastructure, backup alternate server, networks, Information security Risks & compliance and their Contingency policies. For that we take universally accepted Sarbanes-Oxley for IS, ISO 27001 and COBIT frameworks and try to map with the fitness of the organization's objectives and policy.

IT governance is not only important in terms of IT, but it covers wide range of domain in organization like Culture, practices, policies which align with IT management and provide the control objectives in the areas given below.

a. ***IT & Business alignment****:* alignment of bank financial operation with IT, strategic decision in the alignment of IT along with the financial operation and regulation define by regulatory bodies such as Reserve bank Of India, Basel II, Basel III, and Ministry of Finance.
b. ***Value delivery****:* IT Governance provide the confirmation of IT & business organization structure will provide the maximum
c. ***Resource Management****:* Confirm about the adequate IT competent human resource and infrastructure for the current and future plan of the organization. Provide guidelines which bring out the best of IT resource.
d. ***Risk Management****:* Validate that Risk factor are well managed with the process in the plan, it also include IT risk assessment.
e. ***Performance Measurement****:* Compliance can be strategically verified, confirmation about the authentic measurement of the IT contribution.

COBIT is IT governance framework which is globally accepted. COBIT is the product of ISACA and ITGI, Both of this organization has defined COBIT as the benchmark in the field of IT governance which have all the potential recommendation and control framework which organization have to adopt. COBIT 5 is the latest version in the Industry, prior to that COBIT 4.1 was launched. **[4]**COBIT 4.1 principal basically talks about alignment of information technology and the business requirements of an organization, control framework and guidelines delivered in COBIT 4.1 are defined to meet the information requirements of the enterprise which is used to achieve enterprise objectives. When IT governance is considered for implementation in any enterprise, then it is the responsibility of top level management. In COBIT 4.1 a proper framework has been defined about the roles and responsibility of board of directors and management executives.

Business goals drive the need of IT resources which are utilized by IT process and deliver enterprise information which act as business resource. COBIT 4.1 basically have four domains which are plain and organize, acquire and implement, deliver and support, monitor and evaluate, further these domains are subdivided in 34 generic process which are further sub divided in to 300 objective controls which are implemented in the organization according to its industry need.

In this paper we are proposing the critical criteria on which the performance measurement of compliance (IT governance, Information security governance) can be done. In terms of COBIT we have **Information Technology goals and metrics** which define the business requirement from IT and parameters to measure it. Process goals define what IT process will provide to meet the IT objectives and activity goals define the activity within the process to meet the performance required. Metrics help to measure the outcome of both (Process goals and activity goals).

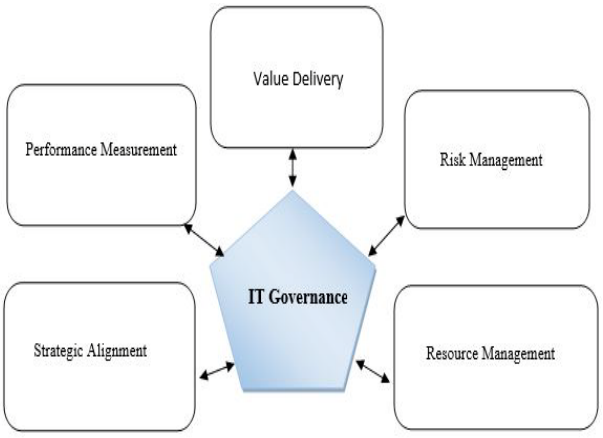

Figure: 1

Plan and organize domain have 10 control objectives which help organization in defining, determining, communicating, managing the higher management strategic objectives

Control objective P01 is signifying IT value management, business IT alignment, assessment of current capability and performance, IT strategic plan, IT tactical Plan, IT portfolio management.

Control Objectives P02 define the Information Architecture which provide the detail description of enterprise information architecture model, enterprise data dictionary and data syntax rules, data classification scheme and integrating management.

Control Objective P03 determine technological direction which provide the detail description of technological direction planning, technology infrastructure plan, monitor future trends and regulation, technology standards, IT architecture board.

Top level management role and responsibilities are defined on the basis of RACI (Responsibility, accountability, Consulted, Informed) Chart. RACI chart is the most important tool of COBIT which provide the brief understanding that who will be responsible for what, so stockholder, board of management, managers should have the proper understanding of RACI chart.

Domains **acquire and implement, deliver and support, monitor and evaluate** also have the control objectives which define the different function and objectives which are to be compliance by the organization**.[6]**

III. METHODOLOGY TO EVALUATE THE CRITERIA FOR END USER TO ESTABLISH THE FITNESS OF COMPLIANCE

a. Respond to Business requirement in alignment with the business strategy.
b. Respond to governance requirement in the line with board direction.
c. Ensure satisfaction of End user with services offering and services levels.
d. Optimize use of Information.
e. Create IT agility
f. Define how business functional and control requirement are translated in effective and efficient automated solution.
g. Acquire and maintain integrated and standardized IT Infrastructure.
h. Acquire and maintain IT skill that responded to the IT strategy.
i. Ensure mutual satisfaction of third party relationship.
j. Ensure seamless integration of application into business process.
k. Ensure transparency and understanding of IT cost, Benefits, strategy, policies and services Levels.
l. Ensure proper use and performance of the applications and Technology.
m. Account for and protect all IT assets.
n. Optimize the infrastructure, resource and capabilities.
o. Reduce Solution and services delivery defects and rework.
p. Protect the achievement of IT objectives
q. Establish clarity on the business impact of risks to IT objective and resources.
r. Ensure that critical and confidential information withheld from those who should not have access to it.
s. Ensure that IT services and infrastructure can properly resist and recover from failure due to error, deliberate attack and disaster.
t. Minimum business impact in the event of IT disruption or changes.
u. Make sure IT services are available as required.
v. Improve its cost-efficiency and its contribution to business profitability.
w. Deliver project on time and on Budget, meeting quality standard.
x. Maintain the integrity of Information and processing infrastructure.
y. Ensure IT compliance with laws, Regulation and contracts.
z. Ensure IT demonstrates cost efficient services quality and continuous Improvement and readiness for future change.

IV. INFORMATION SECURITY

In section 409 of SOX which specifically related to the deadline of recovery time i.e. the data must be retrieved and recovered with an appropriate speed and within a scheduled time because It has seen that in March 2004 Bank of America had to pay $10 million as it could not respond to an information disclosure request in a reasonable amount of time then SEC fined. So in order to implement and convergence with the best fit of their Contingency plan the process timing of a particular process must be taken care in all the BCP compliance. SOX (section 404) not only talks about the audit compliance for financial record but also email, voice mail and video records and it also touch some parts of IT process which entails security administration, data centre management & disaster recovery, application change control and asset management. The five test quality of a data must meet with respect to compliance and for trustworthiness. [**1]**Integrity, Accuracy, Accessibility, Authenticity and Confidentiality. Under any circumstances all these five qualities must fulfil to ensure the success of their Business continuity resiliency. This new regulatory constraint shows that IS departments will have to ensure the integrity of

the entire information system and provide the data necessary for the development of numerous conformity reports.

If we talk about IT influence in the Banking Sector then Most of the Banks have been rolled out with highly sophisticated complex IT system and are functioning on Core Banking Solution or Centralized Banking System (CBS). It's an integrated software system that facilitates integrated & on time processing of data i.e. Under which the information relating to the customer's account (i.e. financial transactions, profession, income, Personal details etc.) is stored in the Central Server of the bank (i.e. available to all the networked branches) instead of the branch server only. Depending upon the size and requirements of a bank, it could be accessible for all the operations or for limited operations.

A. Information Security Governance:

The Information security governance considering the managing, developing the organizational structures and Processes that protect information and mitigation of increasing information security threats like those detailed above.Following broad activities have been carried out as part of ISO 27001compliance at the Data Centre and IT Operations in Banks :

a. Risk Assessment & Risk treatment of banking process and associated assets
b. Rectifying of risk by risk analysis
c. Awareness of end users about information security risks
d. Physical security review
e. ISO 27001 controls using technology
f. Identifying Information security policies.
g. Management awareness on periodic basis
h. Incident reporting & management
i. Change control management
j. Compliance audits

So, meeting the necessity of the business and benefits of Information security governance would help in reducing the uncertainty in the Business operations. It gives an assurance that critical decisions are not based on faulty information & observations which will help the organization in process improvement.

B. Information Security Management:

From above discussion it is clear that the security of information with its integrity and confidentiality is necessary in a financial institution. It is said that information should not only be secure, it should appear to be secure i.e. demonstration of information security is required to convince the customer, government and business partner. So in this paper we are going to propose the evaluation criteria of the fitness of Information security w.r.t. audit compliance in the Bank.

An organization can achieve recognition for its Information security by getting BS 7799 certificates also known as ISO 27000 series.BS 17799 can be divided into two parts BS 17799-1(ISO 27002) which talks about the "code of practices for Information security management" and BS 17799-2(ISO 27001) provides specification, requirements and guidance for use. In Banks generally IS audit follows a three phase route, first is a **planning phase** in which various applicable rules, policies, regulations and laws have to be studied and appropriate tests and checks that would be used in order to check the security measures noted. Second is a **test or Control** phase in which all the tests as planned in the first phase would be carried out sequentially and all the Variations and observations would be noted down. Last phase **tested** a sample of Bank's Transaction in detail.

Let us talk about the Compliance regulations by taking an example of an electronic fund transfer from account of a customer of the host country to the account of a customer of the other bank in other country. Now the regulatory guidelines, foreign exchange management laws, taxation policies of the two countries would be require to be examined. Instead of this what type of procedures to be followed to debit or credit the customer account require to be examined and money laundering or any other financial irregularity need to be examined. All these complex issues need to be examined during intra exchange transactions. So we can take fulfillment of **regulatory laws and policy** as the key points in Information security.

Similarly we can have internal operations issues like employee's authentication security, Network Server security & incident handling ability plus roles and responsibility (RACI Chart) under different circumstances. So for that we'll take **Access Control** & **Incident management** measures and what are the **Governance risks & control (GRC)** practices used in the banks. For GRC evaluation we introduce a Requirement solicitation Questions (RSQ)

Table: 1

S.No.	Figure (RSQ)
1.	What is your biggest GRC area of concern
2.	How do you rate the effectiveness of your security controls?
3.	What compliance and regulations are applicable to your area?
4.	In the past audits have you failed any area of compliance? If so, what were the findings?
5.	To prioritize the security budget what improvements would you like to see in your current mechanisms?
6.	What are the critical threats in a Banking process?
7.	How many times have you experienced these threats during last one year?
8.	What would you like to see in the reports indicating the current status of compliance?
9.	What area are you more concerned about whether inside threats or external threats? Please provide specific.
10.	Do you have a good data classification mechanism?
11.	How do you evaluate risks currently? What are the possible areas of improvements?
12.	Have any of your end user expressed dissatisfaction with the extra step and authentication check they have to pass because of the security controls?

C. :Banking Structure Roles & Responsibilities:

Banks have a separate Department or Functions exclusively to focus on the Information security management. The duties have been segregated in different groups for managing Information system security and Technology division. It is reported that the Information security Governance related structure or Information security group should not be fully outsourced yet specific operational function can be outsourced but its control should always be rests within the bank. The top management people of the banks plays a major role in

establishing necessary organizational processes for information security and the Senior manager should establish the expectation for cyber security and should convey it to their employees down the line. So the effectiveness of information security governance is much more dependent on the dedication of Board or senior management in appropriate monitoring of the Information security function. The Information security committee also consists of CIO, CFO and CEO's of the organization.

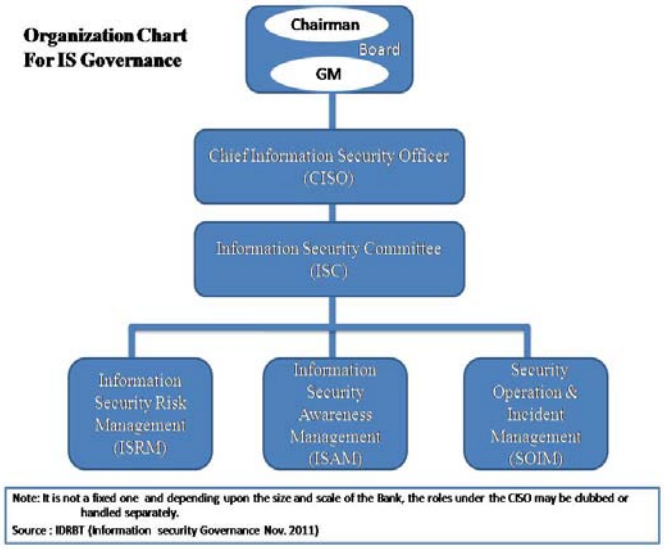

Figure: 2

D. Critical Component of IS:

Keeping in view their business needs Banks frame IS policy and these policies need to be supported with their relevant standard, Guidelines and procedures. The Framework comprises of some Key components like:

a. Scope, Objectives, ownership & end user should be explicitly defined.
b. Responsibilities of Information security related specific roles like IT security manager, administrators, security specialist and Information asset specific roles like custodian end users etc.
c. The CISO must explain the exception policy for handling the non-compliance instances with proper justification of the genuine need for exception plus management of the exception log/register and expiry & granting authority of exception.
d. Management of Firewalls, Antivirus-Malware software, Intrusion Detection & prevention system, Cryptographic method and monitoring analysis tools or techniques.
e. An Event or Incident management team should be as much competent enough to monitor the identification and classification of any phishing, hacking and Malpractices in the bank's Transaction.
f. It is important to communicate the Job responsibility, specific security roles and its accountability to every employee. Every employee, officers must be obliged to comply with security and protect the Information assets.

E. Risk Assessment:

Now if we talk about the Risk Assessment Policy and procedures in banks then most of the banks quantify their operational risks on the basis of Likelihood and its impact on the Organizational Business in terms of loss of asset, financial loss and the Confidentiality breach which matters a lot for a Financial Institutions. Controls in existing application should not dilute, while migrating data to the new application. The Risk assessment process consists of Identification of Assets and their values, threat assessment corresponds to the process of identifying and detecting the malicious activities inside or outside the organization in a process. It should not restricted with the above one but should also consider some other threats like dust, electromagnetic radiation, electrical supply interference, explosives, fires, floods, theft, terrorist activities etc. The Security threats can also be assess as Quantitative and Qualitative threats. Quantitative generally uses the numerical measurement of total risks and residual risks, these measures may include cost of safeguard, number of people involved, probability and the effectiveness of controls. Qualitative analysis is a scenario based risks assessment techniques which works on probability of occurrence of the expected scenarios, its sensitivity and designing of the control steps to prevent that problem.

F. Remote Security:

Nowadays use of E-banking and Mobile banking systems is very common so it should be tested such that segregation of duties cannot be bypassed to each other. Given the increasing reliance of customers on electronic delivery channels, any security related issues may have the potential to bleach public confidence in the use of e-banking and may lead to reputation risks. [3]

Mutual Authentication i.e. a two-way authentication process may be used for E-banking security access system in which a client first has to prove his identity to a server, and then server has to prove its identity to client, prior any application traffic is sent over the client-to-server connection so in this way it can prevent the duplication & fake website related issues [3]. Identity can be proved through a trusted third party and use of shared secrets or through cryptographic means as with a public & Private Key infrastructure. For e.g., the mutual authentication connection can occur only when the client trusts the server's digital certificate and the server trusts the client's certificate. The certificates exchange will happen through special protocols like the Transport Layer Security protocol (TLSP).Therefore this process reduces the risk that an unsuspecting network user will inadvertently reveal security information to a malicious or insecure web site.

G. Incident Management:

It maintains the capability to manage the incident within a bank and achieved recovery of any Information assets within a specified time. Some main points which need to be keep in mind while framing an incident management framework for Banks are:

a. Developing the processes for preventing, detecting and responding any Information security incident.

b. There must be some Data Recovery Back up plans i.e. Cold Site or Hot site system can be considered in this activity.
c. Maintain the Communication with internal and external parties.
d. Developing the Communication process with lines of Authorities.
e. Provide Training to Bank's employees to responds for any unfavored incidents
f. It is necessary to do periodic testing to identify the causes of Information security incidents and make a corrective action plans to reduce the related risks.
g. Incident management strategies also comply with the regulatory requirements of CERT-In/IDRBT/RBI regarding cyber security incidents.[2]

H. Data Security Measures:

The Data Security Policies & Procedures should be adhering to the PCI-DSS standards. Some Proactive measures may be checked which are:

a. The Servers & Data Centers must be protected by adequately firewalls, Anti-viruses and Intrusion prevention system which controls by the stringent access control list that must be taken care by IT team.
b. To check that the Database server and the client's server are protected from internal and external threats, internal vulnerability and external penetration testing should be carried out from a hacker's perspective.
c. The website which used to collect data should be deployed with strong encryption & decryption mechanism and Black box testing approach can be used for websites vulnerability and threat assessments.
d. The server should be hosted under biometric access control with CCTV monitoring.
e. Database Access should be allowed only Database Administration or the concerned person.
f. Banks which are outside the city or may be at far from the central banks should have a secondary alternates, servers & Back up storage system so that at any incident the business operations can be shift & continued from the secondary ones till the primary would get work. It is recommended that the alternate resources should be planned within 25 km range of the banks.
g. **Fitness Check list**

Table: 2

Security Policy		
Existence of IS Policy	Yes/No	Yes = 1 , No = 0
When was the last reviewed conducted	1. Quarterly 2. Half Yearly 3. Annually	
XReason For Last Review	1. Periodic 2. Incident 3. Infrastructure Changes	Periodic=3, Incident = 2, Infrastructure changes = 1
Owner of Security policy	1. Board of Directors 2. Security Committee 3. CISO	Board of Directors = 3 Security committee =1 CISO = 2
IS committee meeting frequency	1. Quarterly 2. Half Yearly 3. Annually	Quarterly = 3 Half yearly = 2 Yearly = 1
Roles & Responsibility Defined to every Committee members	Yes/No	
Whether IT Governance management/ committee is separated from Management	Yes/No	
Medium of Communication	1. Email 2. Intranet 3. In-house Periodic Training	Intranet = 3 Email = 2 In house periodic training = 1
Security policy has been define according to guidelines of ISO27001, COBIT and RBI circular.	Yes/No	
Designated Owner has been assigned to Policy and procedure	Yes/No	
What Interval of time external Audit conducted	1. Quarterly 2. Half Yearly 3. Annually	Quarterly = 3 Half yearly = 2 Yearly = 1
Assets Accountability		
Information asset has been distinguished	Yes/No	
Maintenance of Inventory database	Centrally/Locally	Centrally =2, Locally = 1
Existence of another database inventory for Disaster Recovery	Yes/No	
Updating process for assets of inventory database exist	Yes/No	
Human Resource Security		
IS awareness training program exist	Yes/No	
Backhand verification process for the recruitment	1. In-house 2. Out sourced	In-house = 2 Outsourced = 1
Third Part Security/Vendor Management		
Third party onsite security audit prior to outsourcing	Yes/No	
Periodic checking of third party access provided	Yes/No	
Backhand Verification Program	1. SLA Review 2. Third Party Audit	Third Party Audit = 2 SLA Review = 1
CISO reviews the controls related to third party contracts	Yes/No	
Physical Security		
Security measures has be taken to protect physical access	1. Electronic Access Control (Access card) 2. Biometric	Electronic Access Control (Access

	System 3. Security Guards 4. All of the above	card) = 3 Biometric System = 2 Security Guards = 1 All of the Above = 4
security controls differentiate vendor, equipment maintenance staff, Employee	Yes/ No	
Risk assessment has considered the natural threat	Yes/No	
Proper power supply (Generator, UPS) is available for Information processing facility	Yes/No	
Who check the details of Faults and corrective measures?	1. CISO 2. Data center head 3. IT Head	CISO = 2 Data center head = 3 IT Head = 1
Does exist an Information Diagram which include Location, IP address, and asset owner.	Yes/No	
IS Incident Management		
Whether the process ownership steps for orderly response to a security incident	Yes/No	
System monitoring / forensic investigation is established for proactive action is taken for security incidents	1. Audit Trail 2. Intrusion Prevention/Detection System 3. Log Correlation 4. Any other, Please Specify	Audit Trail = 1 Intrusion Prevention/Detection System = 2 Log Correlation = 3 Any other, Please Specify = 4
Effective Communication with, regulatory bodies, law enforcement authorities, information service providers and Telecommunication operators to get quick and specialist guidance obtained, in the event of a security incident	Yes/No	
How many times security policy review by CISO	1.Quarterly 2.Half Yearly 3. Yearly	Quarterly = 3 Half Yearly =2 Yearly = 1
Frequency of last security incident	1. Less than 3 2. 3- 10 incidents 3. More than 10	Less than 3 incidents = 3 3- 10 incidents = 2 More than 10 = 1
Communication and Operation Management		
Operating procedures implemented for critical processes	Yes/No	
Monitoring performance and declaration for upgrade requirements are done for proper processing power and storage	Yes/No	
VA/PT cycle is rendered for E commerce	Yes/No	
Controls for phishing attacks	Yes/No	
System Acquisition, Development and Maintenance		
Proper controls to mitigate the risk are identified ,in case of data corruption happen during internal processing	Yes/No	
cryptographic controls to protect Information	Yes/No	
Digital signatures For CIA of electronic document	Yes/No	
Access Controls		
Network access policy is define within the organization	Yes/No	
Control are define for authentic access and no access from external connection	1. Cryptography based Techniques 2. Hardware Token 3. Software Tokens 4. Any other	Cryptography based Techniques = 4 Hardware = 1 Software Tokens = 2 Any other = 3
Compliance		
Existence of procedures to justify compliance according to legal restrictions used for material	Yes/No	
all areas are considered for regular review to ensure compliance with	Yes/No	
Whether whole computer hardware is tested on regular intervals to avoid vulnerability	Yes/No	
Authorize compliance officer for the organization	Yes/No	

This Checklist can change/edited or manipulated according to the organization's size and their Business objectives. To ensure the Fitness level of the organization we categories its scores in three levels.

Table: 3

Scores is equals to or Less than 60	The Situation is critical and the Bank need to improve its IT operations immediately by mitigating all the critical risks issues
Scores is Between 61 and 80	The Fitness level is normal and can be better by applying absent controls in their business operations.
Scores is More than 80	The Fitness Level of their IT operations is good and keep maintain

V. CONCLUSION

The Bank would achieve a significantly enhanced security position by improving compliance with regulatory requirements, better-educated staff, less fragile workflows, and reduced liability exposure. Information security Governance is a part of Enterprise Governance that ensures the reliability and transparency of the processes of Banks for their stakeholders. So the used Technology in these financial institutions should be enhanced and upgraded on a regular basis with their continues fitness test reviews. These evaluation criteria and factors can be changed and added according to the bank's needs.

According to the above factors and IT domain one can develop a specific Framework by detailing and defining the core business processes of banks which will give the clear picture of their IT performance. Further we can also use it in our Educational Institutes, Colleges and SME's for defining their IT health.

VI. REFERENCE

[1]. White paper Regulatory Compliance & Business Continuity Planning, Inquest Corporation – Management Consulting Practice

[2]. Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds, Reserve Bank of India Department of Banking Supervision, Central Office

[3]. IT Governance Series: Information Security Governance for the Indian Banking Sector, Version 1.0, November 2011.An IDRBT Publication

[4]. Mario Spremic, Ph.D., CGEIT, Measuring IT Governance Performance: a Research Study on CobiT- Based Regulation Framework Usage, International Journal of Mathematics and Computers in Simulation

[5]. IT Governance Series---Organizational Strucuter for IT in the Indian Banking Sector, Version 1.0 May 2010 IDRBT

[6]. Guidance to achieve control objectives for successful IT Governance, Cobit Control Practices, digitaliser.dk/resource.