Development of a Security Audit Framework for an Organization

MD. MAHABUB UJJAMAN
Student ID: 012103009

A Thesis

in

The Department

of

Computer Science and Engineering

Presented in Partial Fulfillment of the Requirements

For the Degree of Master of Science in Computer Science and Engineering

United International University

Dhaka, Bangladesh

February, 2018

Approval Certificate

This thesis titled **"Development of a Security Audit Framework for an Organization"** submitted by Md. Mahabub Ujjaman, Student ID: 012103009, has been accepted as Satisfactory in fulfillment of the requirement for the degree of Master of Science in Computer Science and Engineering on February, 2018.

Board of Examiners

1.

_____ Supervisor

Mohammad Mamun Elahi
Assistant Professor
Department of Computer Science & Engineering (CSE)
United International University (UIU)

2.

_____ Head Examiner

Dr. Salekul Islam
Associate Professor & Head of the Dept.
Department of Computer Science & Engineering (CSE)
United International University (UIU)

3.

_____ Examiner-I

Mohammad Moniruzzaman
Assistant Professor
Department of Computer Science & Engineering (CSE)
United International University (UIU)

4.

_____ Examiner-II

Dr. Hasan Sarwar
Professor
Department of Computer Science & Engineering (CSE)
United International University (UIU)

5.

_____ Ex-Officio

Dr. Mohammad Nurul Huda
Professor & Coordinator – MSCSE
Department of Computer Science & Engineering (CSE)
United International University (UIU)

Declaration

This is to certify that the work entitled "**Development of a Security Audit Framework for an Organization**" is the outcome of the research carried out by me under the supervision of Mohammad Mamun Elahi, Assistant Professor, Department of Computer Science & Engineering (CSE), United International University (UIU), Dhaka, Bangladesh.

_____

Md. Mahabub Ujjaman, Student ID: 012103009
Department of Computer Science & Engineering (CSE)
United International University (UIU)

In my capacity as supervisor of the candidate's thesis, I certify that the above statements are true to the best of my knowledge.

_____

Mohammad Mamun Elahi
Assistant Professor
Department of Computer Science & Engineering (CSE)
United International University (UIU)

Abstract

Now-a-days in the modern organizations, Information and Communication Technologies are used to support the organizations' activities. To manage the quality of the organization processes, audit processes are implemented.

Auditing Information Systems Security is difficult and becomes crucial to ensure the daily operational activities of organizations as well as to promote competition and to create new business opportunities. With a large number of parameters in the global standards, managing a conceptual security framework to manage and audit Information System Security especially for small to medium companies in Bangladesh is really cumbersome and a daunting process to follow. The purpose of this work is to propose a security audit framework for small to medium level organizations based on the ISO/IEC_JCT1 standards, to assist organizations to better manage their In-formation Systems Security.

To evaluate the proposed framework, some questionnaires were prepared and testing results of the effectiveness of IT Governance and Security controls mechanism based on the framework were shown to prove the efficacy of the approach. The framework should help an organization to minimize vulnerabilities, ensure smooth and transparent governance and protect information assets.

Acknowledgement

I would like to start by expressing my deepest gratitude to the Almighty Allah for giving me the ability and the strength to finish the task successfully within the scheduled time.

This thesis has been prepared to fulfill the requirement of MSCSE degree. I am very much fortunate that I have received sincere guidance, supervision and co-operation from various persons.

I would like to express my heartiest gratitude to my supervisor, Mr. Mohammad Mamun Elahi, Assistant Professor, United International University, for his continuous guidance, encouragement, and patience, and for giving me the opportunity to do this work. His valuable suggestions and strict guidance made it possible to prepare the thesis report.

Finally, my deepest gratitude and love to my wife for her support, encouragement, and endless love.

Terminologies Used

DC	Data Center
DRS	Disaster Recovery Site
BCP	Business Continuity Plan
ISP	Information Security Policy
IT SSC	I T Security Steering Committee
CAB	Change advisory board
DRP	Disaster Recovery Policy
VA	Vulnerability Assessment
PT	Penetration Testing
SDLC	System Development Life Cycle
IM	Information management
MAF	Management Accountability Framework
MITS	Management of Information Technology Security
ERM	Enterprise Risk Management
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
IAF	internal audit function's
ISMS	Information security management system
VAPT	Vulnerability Assessment and Penetration Testing
QMS	quality management system
PQA	Product quality assurance
PMF	Project management framework
CIO	Chief Information Officer
ITIL	Information Technology Infrastructure Library
CAB	Change Advisory Board
RFC	Request for Change
BCM	Business Continuity Management
ISACA	Information Systems Audit and Control Association
MAF	Management Accountability Framework

Table of Contents

LIST OF TABLES

LIST OF FIGURES

Chapter 1
INTRODUCTION

1.1 Introduction

Information technology (IT) development methodologies may be described as another support of rationalist, positivist, functionalist hegemony. The major methodologies of the Classical Systems Life Cycle, Structures Systems Development, Data Modeling and Object Oriented Analysis are briefly reviewed in terms of their ubiquitously quoted evolution and maturation and the benefits they purport to offer IT specialists and managers, general management and user groups. This paper argues that, while it has traditionally been the case that such methodologies be compared on a case by case basis, it is time to step back from the traditionally reductionist, positivist approaches of IT. IT methodological development is considered here from a critical, anti-positivist perspective. It is suggested that qualitative research methodologies be employed to assist in creating a new IT development epistemology to spare us from further IT implementation disasters.

1.2 Problem Statement

The primary purpose of the audit framework is to assess the effectiveness and efficiency of security measures and their compliance with an IS(Information Security) Policy and Operational Standards. Developing an Audit Framework to identify an organization's strength against the IT security threats as well as building up good IT governance policy is a very cumbersome work. The objectives follow an organization's Information Technology Security and include the following assurances [21], [22], [23]:

• A management control framework exists;

• An effective security program is in place;

• Security education and training is adequate;

• Information/communications is appropriately classified and protected;

• An effective personnel screening program is enforced;

• Security breaches are dealt with;

• Physical safeguards are in place for the protection of personnel and assets;

• Contingency management has been developed;

• Security requirements are met in contract management; and

• Threat and risk assessments are conducted on a regular basis and prior to major system, application and telecommunication changes.

The main objective of this work is to develop a simplified and effective security audit framework, especially for the small to medium level companies in Bangladesh. The purpose of this Framework is to clearly establish an organization's role in protecting its information assets, and communicate minimum expectations for meeting these requirements. Fulfilling these objectives enables an organization to implement a comprehensive system-wide Information Security Program. The scope of this Framework includes all information assets governed by an organization.

All personnel and service providers who have access to or utilize assets of the company, including data at rest, in transit or in process shall be subject to these requirements. This Framework applies to all information assets operated by the organization.

1.3 Theoretical Background and Related Works

An Information Security Framework assists in the protection of information assets. The challenges of running an information security program can be overwhelming. There are so many areas to address eg. Encryption, application security, disaster recovery. Then there is the complication of compliance with regulatory requirements such as HIPAA, PCI DSS, COBIT etc. [21]

Now-a-days, there is a huge number of frameworks and tools in practice for IT audit in the global industry. In the context of Bangladesh, for small and medium level organizations, there is a need for suitable tools or framework such that they can easily measure their scale of security level and take appropriate measures as well. For this, we

have taken steps to develop a framework with a limited and accommodate more appropriate elements like mentioned below:

a) In ‘Management of Information Technology (IT), there are lots of elements to strengthen the security audit framework:

The IT Governance Institute's definition is: "... leadership, organizational structures and processes to ensure that the organisation's IT sustains and extends the organisation's strategies and objectives” [28].

Also, we need to accommodate the appropriate and relevant elements, which are suitable for the small and medium organizations in the contest of Bangladesh to sustain against the security threats and proper management like: IT security steering committee (ITSC), IT Strategy, Security Awareness Training, Segregation of Duties Matrix, IT Human Resource Policies and Employee Satisfaction Surveys

We have to also define Business Continuity Plan, Risk Assessment, Disaster Recovery Testing and IT Help Desk Activities. Finally, we take some efficient points to summarize the change management elements along with eg. Change Advisory Board, Change Management Procedures, Configuration and Release Management and User Acceptance Testing Sign-offs.

In Physical Security and Environmental Controls, we propose the basic elements like Physical Access Control and Security Procedures and Data Center & Disaster Recovery Site - Environmental Controls. In Security of Information Systems, we emphasis on IT Policy and Procedures and IT Policy Revision Control. In System Development, we have sorted IT Project Management, System Design, Software Testing, Quality and Project Assurance and Project Documentation. In Network Security Review, we take the elements like System Risk Assessment, Internet Access Policy, Vulnerable Assessment & Penetration Testing and Security Architecture Monitor and Approval. In Control Assurance, here we mentioned IT Risk Assessment, IT Audit Function and IT Internal Control Assessment

1.4 Methodology and Approach

The audit followed a generic approach to Management of Information Technology Security (MITS) compliance developed by the audit team. MITS components were aligned with four Management Accountability Framework (MAF) components of an organization and they are Accountability, Risk Management, Governance or stewardship and Staff. A planned methodology is inserted in the Appendix A.[22]

1.5 Organization of The Thesis

This study shows how a realistic Security Audit Framework can help an association to understand the IT security Risk, Impact and appropriate measure in the respective field. The organization of this thesis is as follows. Chapter 1 provides a brief description regarding methodology and approach. Chapter 2 introduces main elements of the Security Audit Framework or model in detail. We first describe the model elements that our audit framework is built on, as well as provide a breakdown view on how to do go forward as well. We also determine the severity level, scoring the points, Risk as well as impact and recommendation. Chapter 3 provides a brief description on the proposed methodology and approach. We describe and provide in a chart regarding Action and Impact vs Risk. Finally, we define a Risk rating strategy and projected a Security Audit Framework. In Chapter 4, we assessment data in three organization especially on Banking and non-banking organizations in Bangladesh based on a sample questioner. After that we fill up the result sheet based on the questioners in the proposed framework and yielding a graphical presentation with chart. Chapter 5 concludes the report with some future work directions.

Chapter 2

Elements of IT Security Audit Framework for an organization

2.1 Management of Information Technology (IT)

2.1.1: IT Steering Committee (IT-SC)

Introduction:

The role of the IT steering committee is to aim to ensure that the IT projects are proceeding to plan, to ratify any scope changes which increase budget or timescale, to ensure that the project remains focused on the achievement of its objectives, to champion the project within their areas of business, to ensure that the resources required are made available to the project and to resolve issues outside the scope of the immediate project management.

The IT Steering Committee will provide overall direction to the project and be the ultimate forum within the project for ratifying critical project decisions. Generally, the composition of IT steering may have several roles (as mentioned below), however it is a management decision to finalize ITSC composition: [1],[5]

- Program Sponsor / Owner (e.g. Managing Director or CIO)
- Project Board (Project Team);
- Executives (e.g. DMDs);
- Senior User (s) (e.g. Function Heads);
- Project Manager(s);
- Project Office (PMO);
- Head of IT; and
- IT Experts

Further, ITSC should meet on regular basis to cover significant IT projects, discuss IT strategy, operational changes and other IT issues, for example system availability and performance. Minutes of meeting should also be documented and circulated to all the

ITSC members in timely manner. ITSC meetings must not delay project activity, but should be seen as a catalyst by:

- Acting as a deadline for actions;
- Setting future deadlines;
- Identifying and unblocking problems; and
- Assigning responsibilities.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no ITS- SC
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

If the committee is not in place and regularly meetings are not held between IT and business representatives, there is a risk that this may lead to lack of accountability and members not taking interest / ownership in decisions. Further, the Organization may also face following risks:

- Communication gap may increase between IT and the business and important business and

- IT issues may not be appropriately addressed;
- Not integrating all aspects of IT resources into an efficient, and unified effort; and
- Inefficient IT performance.

Recommendation

It is recommended that IT steering committee should be in place, which meets on periodic basis to discuss IT related issues. IT steering committee charter should be documented and the committee should include representatives from IT and all critical business segments/functions in the Organization

2.1.2: IT Strategy

Introduction:

The purpose of the IT strategy is to provide guidance for developing, managing and measuring the IT infrastructure and systems that support the business in achieving its goals. The IT strategy should therefore take into account how IT will enable the business strategy. With today's environment of ever-changing technology and increasing competitiveness, the IT strategy needs to provide for the possibility of unexpected changes in business direction, but should also be sufficiently specific to serve as a basis for communication and performance measurement. It should include the platforms and systems to be deployed & supported and migration strategies for deployment.

A successful IT strategy should have the following characteristics:[5]

- Be driven by the business strategy;
- Manage, leverage and integrate IT people, processes and technologies which exist within functional silos to integrate them into the overall IS strategic plan;
- Support long and short-term objectives without compromising ongoing operations;
- Demonstrate flexibility to accommodate business change;
- Address all layers of the infrastructure, processes, procedures and policies and identify the required organizational structure required to fulfill the strategy;
- Have a resilient foundation on which others can depend;

- Embrace technology, third parties, partnerships, the organization, structure and human capital; and
- Take into account the demands and requirements of various stakeholders and provide a solution which responds to service requirements while advancing IT forward.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no IT Strategy
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

In the absence of a formalized IT strategy, there is a risk that future IT investments in hardware and software may not be those that best meet ORGANIZATION's medium to long term business objectives. Without effective planning, the business potentially faces the following risks:

- Use of existing resources may be less than optimal;
- Not integrating all aspects of IT resources into an efficient, unified effort;
- Inefficient IT performance and performance management;
- Investment in IT may not be aligned with the business strategy and does not support business objectives;

- Over funding a non-critical area or under funding a critical area;
- Lost revenue opportunities due to inability of IT to meet business needs; and
- Inability to launch new products and services on time.
- Recommendations
- The Organization should formally document IT Strategy (Long term and short term), driven from the business plan and approved by the board.

2.1.3: Security Awareness Training

Introduction:

One of the greatest threats to information security could actually come from within a company or organization. Inside 'attacks' have been noted to be some of the most dangerous since these people are already quite familiar with the infrastructure. It is not always disgruntled workers and corporate spies who are a threat.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  **High**

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no policy and practice for security Awareness Training
1	There is no policy but practice at times for security Awareness Training
2	Developing a policy and practice at times for security Awareness Training
3	Developed and practice at times
4	Do not maintain strictly
5	Formal documental and strictly follow

Risks / Impacts

Failure to comply with regulatory requirements may expose the Organization to the reputation risk and the risk of penalties from the regulatory bodies.

Further, lack of security awareness programs and trainings pose multiple threats including social engineering threats.

Recommendations

The Organization should develop a comprehensive security awareness training program that yields measurable results. Through security awareness trainings, responsibilities are made clear and process ownership is established.

Further, management should arrange training sessions or refresher courses should be conducted on periodic basis, to update existing and new employees about security management policies and procedures.

2.1.4: Segregation of Duties Matrix [ISACA]

Introduction:

Segregation of Duties helps to implement a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. It makes sure that personnel are performing only authorized duties relevant to their respective jobs and positions.

For reference, management may consider following segregation of duties control matrix indicating which positions in IT should be separated and which require compensating controls when combined. [4], [24]

A Chart of IT Segregation of Duties Matrix is given below:

IT Segregation of Duties Matrix													
	Control Group	Systems Analyst	Application Programmer	Help Desk Manager	End User	Data Entry	Computer Operator	Database Administrator	Network Administrator	System Administrator	Security Administrator	Systems Programmer	Quality Assurance
Control Group		X	X	X		X	X	X	X	X		X	
Systems Analyst	X			X	X		X			X			X
Application Programmer	X			X	X	X	X	X	X	X	X	X	X
Help Desk Manager	X	X	X		X	X		X	X	X		X	
End User		X	X	X			X	X	X			X	X
Data Entry	X		X	X			X	X	X	X	X	X	
Computer Operator	X	X	X		X	X		X	X	X	X	X	
Database Administrator	X		X	X	X	X	X		X	X		X	
Network Administrator	X		X	X	X	X	X	X					
System Administrator	X		X	X		X	X	X				X	
Security Administrator		X	X			X	X					X	
Systems Programmer	X		X	X	X	X	X	X		X	X		X
Quality Assurance		X	X		X							X	
X– Combination of these functions may create a potential control weakness													

Table-1 : Chart of IT Segregation of Duties Matrix

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  **Medium**

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no policy and procedures regarding Segregation of Duties Matrix
1	There is a draft but not complete policy and procedures regarding Segregation of Duties Matrix
2	Process not followed in a formal way
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

Due to inadequate segregation of duties, ORGANIZATION is exposed to the following risks:

- In appropriate subversion of critical processes;
- Data manipulation, malicious or unintentional damages and loss of data integrity;
- Non-compliance with external requirements for segregation of materially significant systems and business processes; and
- Financial loss and reputational damage.

Recommendations

Management should ensure the effective and efficient functioning of business-critical systems and processes and a detailed exercise should be carried out to review the existing user access privileges. A segregation of duties matrix should be documented for the

existing roles in IT department, clearly eliminating all conflicting roles and responsibilities.

2.1.5: IT Human Resource Policies

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  Medium

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks

Score/Weight	Weight Description
0	There is no policy and procedure regarding IT Human Resource
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

In the absence of IT Human Resource policies, the Organization may face following risks:

- Employee turnover and its associated cost may increase;
- Policy leads to internal and external equity which may be disturbed; and
- Employee satisfaction, motivation and loyalty within employees may decrease.

Recommendations

Management should document IT Human Resource Policies as mentioned in the observation. As skill requirements for IT personnel require specialized interview questions

and retention of IT skilled staff is critical for business, separate HR policies should be documented that are specific for IT department.

Further, informal metrics should be in place such as employee retention/turnover by IT functional area and IT staff headcount as a percent of total staff. Further, the management should consider documenting procedures that take into account personal circumstances of staff affect the work.

2.1.6: Employee Satisfaction Surveys

Introduction:

Employee satisfaction surveys provide management with the knowledge and tools to build positive employee relations and a positive work environment. Employee attitudes, burnout tendencies, passion factors, loyalty, workplace climate and competitive intelligence are key indicators for employee retention, satisfaction, and productivity.

Effective businesses focus on creating and reinforcing employee satisfaction to get the most out of their human capital. Properly constructed employee satisfaction surveys provide the insights that are foundational to creating and reinforcing pleasurable work environments.[6]

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  **Low**

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no policy and procedure regarding Employee Satisfaction Surveys
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

In the absence of periodic HR employee satisfaction surveys, there is a risk that system deficiencies and employee needs are not identified or channelized.

Recommendations

Management should introduce the process for conducting employee satisfaction surveys so that employee's level of satisfaction towards IT and its systems can be measured. The management should perform this process on periodic basis and appropriate actions are taken on the results obtained.

2.2 Continuity of Systems

2.2.1: Business Continuity Plan (BCP)

Introduction:

Business Continuity Management (BCM) is the development; implementation and maintenance of policies, strategies and programs to assist an entity manage a business disruption event, as well as build entity resilience. It is the capability that assists in preventing, preparing for, responding to, managing and recovering from the impacts of a business disruption event.[7], [8]

Disruption-related risks may be infrequent, but have severe consequences for critical services, and are not able to be resolved by routine management. Disruption-related risks include physical and non-physical events such as natural disasters, pandemics, significant loss of utilities, financial crises, accidents, and incidents that threaten our reputation. An effective framework equips us to:

- Ensure services that are critical to our objectives continue despite the occurrence of a potentially disruptive event
- Stabilize the effects of a disruptive event and return to normal operations and a full recovery as quickly as possible
- Capitalize on opportunities created by the disruptive event.[9]

This adaptive capability builds high level resilience, and: • increases security awareness

- minimizes financial effects and effects on service delivery targets
- Improves understanding of functions and opportunities for improvement
- Enhances stakeholder confidence
- Protects corporate assets and reputation
- Strengthens relationships with emergency response partners.

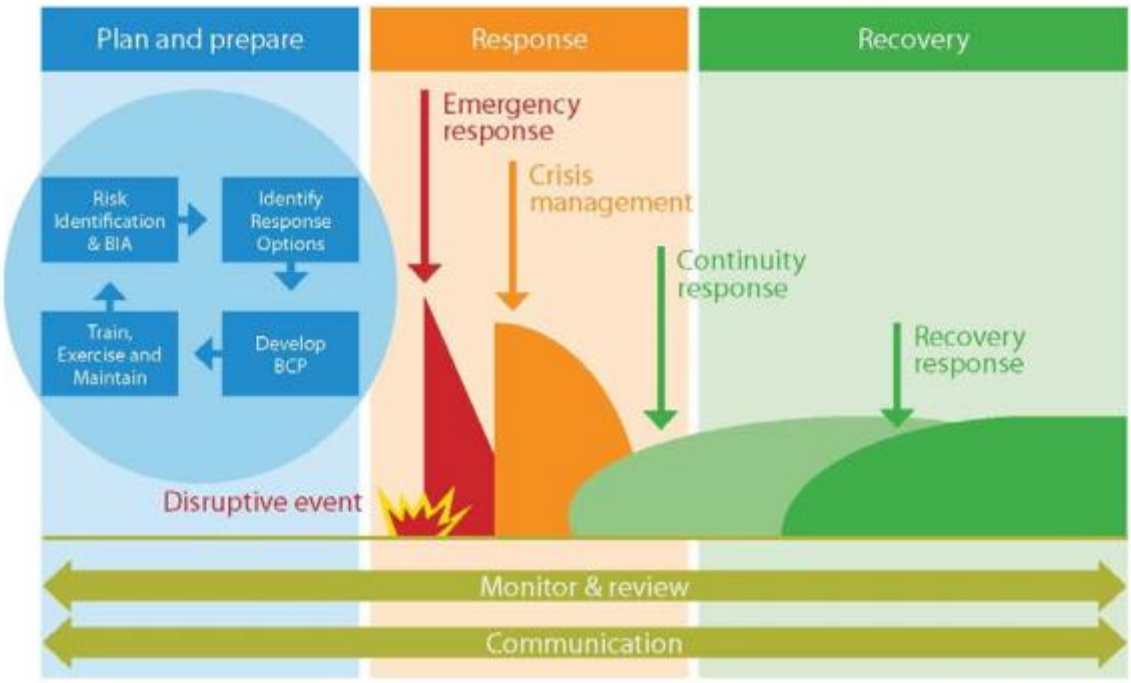

Figure-1: Relationship between the activities in managing BCP related task and risk

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no policy and procedure regarding Business Continuity Plan (BCP)
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

In the absence of approved and up to date BCP, the management may not be able to enforce the policy on the organization wide basis.

Without comprehensive, up to date BCP, there is a risk that in the event of a disaster or prolonged disruption / outage of some kind Organization may be unable to continue the operation of business critical processes and functions and recover key IT systems within an acceptable timeframe that allows the business to continue to meet its business goals.

Recommendations

A business continuity management process should be implemented to minimize the impact on the Organization and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

The consequences of disasters, security failures, loss of service, and service availability should be subject to a business impact analysis. Business continuity plans should be developed and implemented to ensure timely resumption of essential operations. Information security should be an integral part of the overall business continuity process, and other management processes within the Organization.

Following steps may be considered by the management in this regard:

- Establish a Business Continuity Management (BCM) Process or Function, including resilience strategies, recovery objectives, business continuity and crisis management plans and including obtaining management support and organizing and

managing the formulation of the function or process either in collaboration with, or as a key component of, an integrated risk management initiative;

- Identify the impacts resulting from disruptions and disaster scenarios that can affect the Organization and techniques that can be used to quantify and qualify such impacts. Identify time- critical functions, their recovery priorities, and inter-dependencies so that recovery time objectives can be set;

- Determine the events and external surroundings that can adversely affect the Organization and its resources (facilities, technologies, etc.) with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. Provide cost-benefit analysis to justify investment in controls to mitigate risks;

  - Determine and guide the selection of possible business operating strategies for continuation of business within the recovery point objective and recovery time objective, while maintaining the Organization's critical functions;
  - Develop and implement procedures for response and stabilizing the situation following an incident or event, including establishing and managing an Emergency Operations Centre to be used as a command centre during the emergency;
  - Formally document the skill set required to support the business continuity roles and responsibilities in the Organization. Further, the Organization may consider incorporating business continuity roles and responsibilities in respective job descriptions of business/IT personnel;
  - Design, develop, and implement Business Continuity and Crisis Management Plans that provide continuity within the recovery time and recovery point objectives;
  - Prepare a program to create and maintain corporate awareness and enhance the skills required to develop and implement the Business Continuity Management Program or process and its supporting activities;
  - Pre-plan and coordinate plan exercises, and evaluate and document plan exercise results.
  - Develop processes to maintain the currency of continuity capabilities and the plan

document in accordance with the Organization's strategic direction. Verify that the Plan will prove effective by comparison with a suitable standard, and report results in a clear and concise manner;

- Test the BCP on periodic basis (at least annually), review and audit by the internal audit department to ensure its appropriateness. It is important to minimize the economic impact of extended business disruptions in the event of disaster or contingency;
- Develop, coordinate, evaluate, and exercise plans to communicate with internal stakeholders (employees, corporate management, etc.), external stakeholders (customers, shareholders, vendors, suppliers, etc.) and the media (print, radio, television, internet, etc.); and
- Establish applicable procedures and policies for coordinating continuity and restoration activities with external agencies (local, state, national, emergency responders, defense, etc.) while ensuring compliance with applicable statutes or regulations.

2.2.2: Risk Assessment

Introduction:

The goal of a security assessment (also known as a security audit, security review, or network assessment), is to ensure that necessary security controls are integrated into the design and implementation of a project.

A properly completed security assessment should provide documentation outlining any security gaps between a project designs and approved corporate security policies. Management can address security gaps in three ways: Management can decide to cancel the project, allocate the necessary resources to correct the security gaps, or accept the risk based on an informed risk / reward analysis.[10]

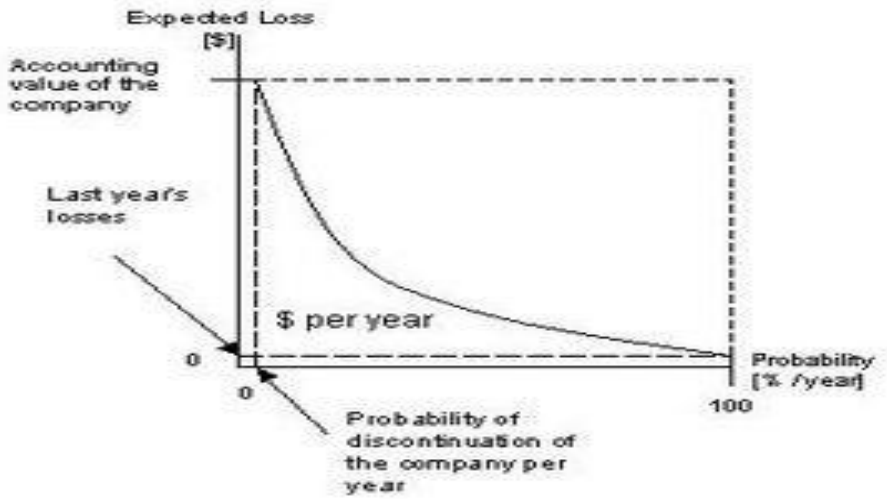

Figure-2: The Risk assessment from a financial point of view.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no policy and procedure regarding Risk assessment
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

Due to absence of formal risk assessment process, there is risk that the Organization may

not be able to correctly identify and analyze the types of risk that may impact the Organization.

The Organization may not be able to anticipate the risk of interruptions to business activities and processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Recommendations

Risk assessment is an important step in documenting a comprehensive BCP. Risk assessment should be designed to identify and analyze the types of risk that may impact the Organization. Assessment should be performed by a group representing various Organization functions and support groups. Following recommendations should be considered by the management in conducting the risk assessment exercise:

- Using available information about known or anticipated risks, the Organization should identify and review risks that could possibly impact the business, and rate the likelihood of each. A Risk Assessment matrix can aid identification of risks and prioritization of mitigation/planning strategies;
- Understanding the risks the Organization is facing in terms of likelihood and impact in time, including an identification and prioritization of critical business processes;
- Identifying all the assets involved in critical business processes;
- Ensure that there is an appropriate balance between threat prevention planning and measures and business continuity planning and measures. The cost of implementing preventive and/or recovery and restoration measures should be balanced against the business and operational impact of the outage. as well as its likelihood of occurrence; and
- Ensure that business continuity plans and arrangements include all resources necessary to support critical business functions (e.g., office work space and technology, furniture, voice and data communications, supplies and services, and people resources). The resources required to restore critical business activities need to be continually monitored and redefined. The introduction of new office

technologies, such as imaging and workflow redesign may render manual recovery fallback procedures unworkable.

2.2.3: Disaster Recovery Testing

Introduction:

Disaster recovery planning is the process of creating a document that details the steps your business will take to recover from a catastrophic event. Many businesses take the time to create a disaster recovery plan, but then leave it to sit on a shelf collecting dust, never reviewed or updated.[1][24]

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no policy and procedure regarding DRS testing
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

In the event of a disaster such as loss of primary site, the Organization may not be able to

recover desired level of computing power within a certain tolerable timeframe. This could result in excessive downtime and hence financial and reputational risks. Without continual testing, existing arrangements and procedures become outdated, and incapable of being successfully and efficiently activated.

Further, the risk in continually testing components of a recovery plan in isolation is that there may be procedures which do not integrate well or that are missed between business unit and technology testing.

Recommendations

It is recommended that comprehensive and complete disaster recovery testing should be conducted by the Organization. All systems including the core Organization system, alternate delivery channels, networks, card system etc should be tested and operated from the Disaster Recovery Site, at least on annual basis. It is important that testing be as comprehensive as possible. [1], [11]

Following recommendations should be considered by the management regarding BCP/DRP testing:

- The first step in testing should be the setting of goals and expectations. An obvious goal is to determine whether a certain crisis response process works and how it can be improved. Other less obvious goals can be to test capacity (as in the case of a call-in or call-out phone system, for instance), to reduce the time necessary for accomplishment of a process (for example, using repeated drills to shorten response times), and to bring awareness and knowledge to the general employee population about the BCP / DRP;

2.2.4: IT Help Desk Activities

Introduction:

The help desk staff and supporting IT staff may not all work from the same location. With remote access applications, technicians are able to solve many help desk issues from another work location or their home office. While there is still a need for on-site support to

effectively collaborate on some issues, remote support provides greater flexibility.

A typical help desk can effectively perform several functions. It provides a single (or multiple) point of contact for users to gain assistance in troubleshooting, get answers to questions, and solve known problems. A help desk generally manages its requests through the use of software such as issue tracking systems

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  Medium

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no Help Desk Activities
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

The help desk is often quoted as a vulnerable point for social engineering attacks. A social engineer is a con man. He or she is someone who wants to take advantage of a person's helpfulness and use it to advance his strategy. At the same time, the helpdesk is a key area to preventing security incidents (for both Social Engineering and monitoring security policy). Absence of setting up documented benchmark for queries action resolution for help desk service, the Organization may find difficulties to establish a proven resolution for individual problem and incident. It will be also difficult to identify an incident and

whether it is a threat.

Recommendations

It is recommended the Organization should establish a policy and procedure for the help desk in light of security management. The management may follow and get idea from the industry standard guideline of ITIL and ISO 27001. We also recommend that the management should setup a single point of helpdesk contact so that incidents and problem may be segregated and prioritized. [1],[2]

2.3 Change Management

2.3.1: Change Advisory Board

Introduction:

CAB – known formally as the Change Advisory Board, is a group of people who are tasked with evaluating changes to the IT environment. It can be as simple as an email distribution list, or as formal as a Chairman-led, take-minutes, raise-your-hand-to-speak board. The culture and the business needs of the organization determines what's appropriate. [1],[5]

The CAB is comprised of technical staff and key decision makers. There's no set rules for who's on CAB. The Change Manager ensures the right people with the right information, knowledge, and background are there to effectively review each change.

It's not uncommon for Subject Matter Experts to be called in to help review and advice on specific Change Requests because of the nature of the Change. (i.e. Senior Network engineer for router changes.)

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no Change Advisory Board
1	Follow some sectors
2	Yet to documented

3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

In the absence of formal program change advisory board the Organization is exposed to the following risks:

- Unauthorized changes made to programs can go unnoticed;
- Changes made may not meet the exact user requirements;
- Untested programs in the production environment, therefore unreliable changes in the system resulting in incorrect operation and loss of data integrity; and
- Lack of accountability for changes made to system.

Recommendation

Change Advisory Board (CAB) should put in place which, comprise individuals at an appropriate level and should make decisions regarding the impact of the change and estimating required resources. The CAB should comprise individuals at appropriate levels within the Organization and change should be dealt with according to business priority.
The Change advisory board (CAB) delivers support to the Change Management team by approving requested changes and assisting in the assessment and prioritization of changes. This body is generally made up of IT and Business representatives that include:[24],[1]

- Business Representative,
- Change Manager,
- User managers and groups,
- Technical experts,
- Possible third parties and customers (if required).

All changes should be initiated through the agreed change management channel, as Change Advisory Board. Any Request for Change (RFC) should be circulated in advance to allow the CAB members whether to attend in person, send a representative, or communicate via the Change Manager.

The CAB fulfills its purpose primarily by executing the following strategies:

- Implement a standard, repeatable, predictable, and transparent Framework change advisory process;
- Remain focused on statewide business needs based on and in relation to business needs;
- Place greater emphasis and priority on required aspects of the Framework; and
- Act in accordance with legislative direction as stipulated in statute.

Specific roles and responsibilities should be assigned to members of the Change Management team and Change Advisory Board.

For effective decision-making, the Change Advisory Board (CAB) should comprise individuals at an appropriate level and should make decisions regarding the impact of the change and estimating required resources. All changes should be dealt with according to business priority.

Division of roles is important to ensure that changes to business functionality are properly authorized by CAB. Further, periodic CAB meeting should be held. Meeting notes should be documented and circulated to all CAB members.

2.3.2 Change Management Procedures

Introduction:

Every IT landscape must change over time. Old technologies need to be replaced, while existing solutions require upgrades to address more demanding regulations. Finally, IT needs to roll out new solutions to meet business demands. As the Digital Age transforms many industries, the rate of change is ever-increasing and difficult for IT to manage if ill prepared.

The Information Technology Infrastructure Library (ITIL) provides a set of best practices for change management that makes it easier for IT professionals to roll out and prioritize changes efficiently, without negatively impacting customers or agreed-upon service levels. To stay competitive and avoid the stress of implementing changes without direction, it's important to understand these guidelines. [1],[5],[13]

Work Flow:

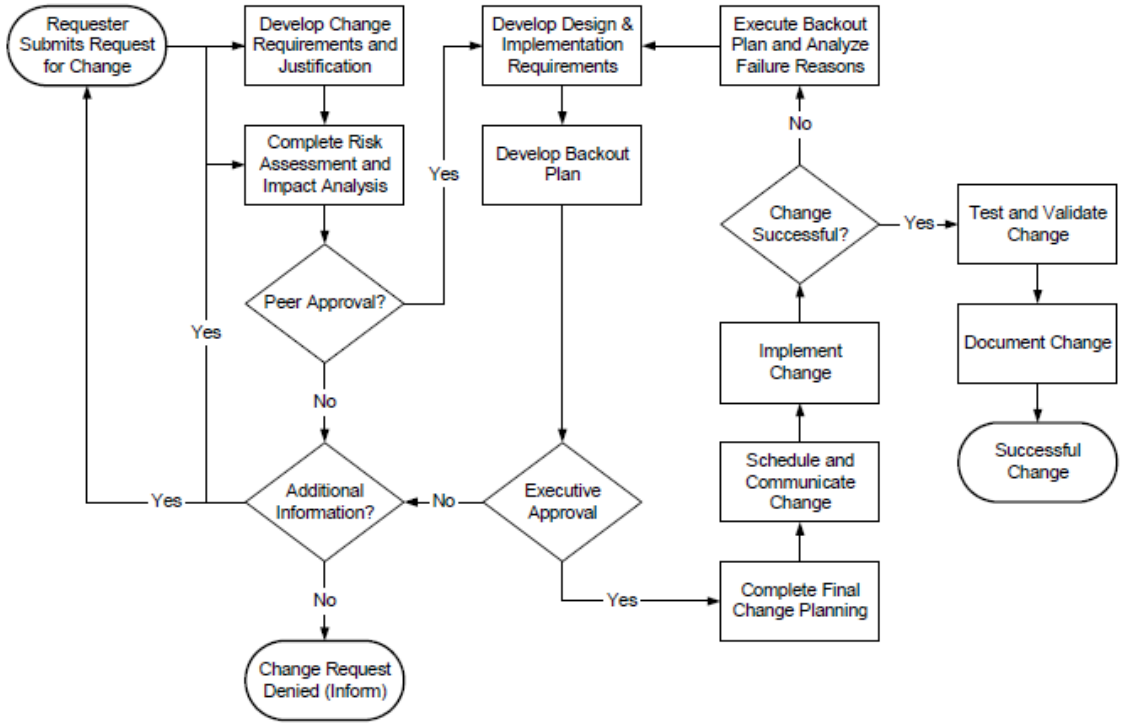

Figure-3: Basic Change management Work Flow:

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Score/Weight	Weight Description
0	There is no Change Management Procedures
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Put a Tick (√) marks:

Risks / Impacts

If change management procedures are not documented, following risks may be faced:

- There may be the risk of implementing changes without following effective practices including planning, changes prioritization, categorization and regular change management reporting;
- Lack of formal documented impact assessment may lead to the risk that incorrect decisions may be made as to whether a change is viable or not. Further it will be difficult to ensure that management have fully considered the pros and cons of any new change or that management has accepted the impact of the new change; and
- Procedures for aborting and recovering from unsuccessful changes may not be identified.

Recommendations

Management should document comprehensive change management procedures and ensure the implementation is consistent and applicable to all IT systems. Further, the change

management policy in IT policy should also address the following change management areas:

- Impact assessment/analysis;
- Prioritization of changes;
- Regular Change Management reporting; and
- Fallback Plans.

2.3.3: Configuration and Release Management

Introduction:

Release management. Release management is the process of managing, planning, scheduling and controlling a software build through different stages and environments; including testing and deploying software releases in a proper method.

Categories include

- Programs/Projects
- Services
- Systems
- Hardware
- Software
- Documentation
- Environment
- People
- Data

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  Medium

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no Configuration and Release Management
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

In the absence of formal configuration management procedures, Organization may be exposed to the following risks: [1],[5]

- Updated hardware configurations not recorded; and
- Software versions and configurations not maintained including operating systems and applications.

Further in the absence of a comprehensive release management for source control and versioning, it may not be possible to keep track of changes made to the system, and if required, rollback to a previous functional version may not be possible.

Recommendations

It is recommended that ORGANIZATION should utilize automated Configuration Management function tools that are used to automatically record and change configuration settings. These tools help to streamline IT operations and make it easier for IT systems to be more consistent with one another.

2.3.4 User Acceptance Testing Sign-offs

Introduction:

UAT stands for User Acceptance Testing. We know what testing is, acceptance means approval or agreement. The user in the context of a software product is either the consumer of the software or the person who requested it to be built for him/her (client).

This is typically the last step before the product goes live or before the delivery of the product is accepted. UAT is after the product itself is thoroughly tested (i.e after system testing).

Users or client – This could be either someone who is buying a product (in the case of commercial software) or someone who has had a software custom built through a software service provider or the end user if the software is made available to them ahead of time and when their feedback is sought. [1],[5]

Number	Acceptance Requirement	Critical		Test Result		Comments
		Yes	No	Accept	Reject	
1	The system must execute to end of job.	√				Payroll will not run in a production status until this requirement has been met.
2	The results of payroll must be correct.	√				Payroll will not run in a production status until this requirement has been met.

Figure-4: **User Acceptance Testing Template for Payroll system:**

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  Medium

Score Assessment of the element may consider by the following weighted values:
Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no User Acceptance Testing Sign-offs
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

Lack of user acceptance testing sign-offs may expose the Organization to the risk that new or changed programs may not operate as designed and may not meet the needs of the intended users.

Recommendation

It is recommended to sing-off every user after implementation of every change.

2.4 Physical Security and Environmental Controls

2.4.1: Physical Access Control and Security Procedures

Introduction:

Work on physical security mainly focuses on the physical protection of information, buildings, personnel, installations, and other material resources. Additionally, physical security covers issues related to processes prior criminal activities, espionage, and terrorism. What factors can develop into the biggest direct threats?[1],[14],[15]

- Staff – dismissal, strikes, illness.
- Sabotage and vandalism.
- Hardware failures.
- Natural disasters – tornadoes, earthquakes, floods, and tsunamis.
- Man-made disaster – terrorism, arson, bombings.
  Loss of access to electricity, air, and water.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no Physical Access Control and Security Procedures
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

In the absence of the formally documented procedures, emergency situations could not properly handled which would result in increased downtime and/or risk to the staff. In such circumstances, every IT personnel should act according to the procedure documented to overcome the issue in timely and proper manner.

Further, in the absence of formally documented escalation procedures, timely reporting of incident at an appropriate level would not be possible. Further, the damage containment activities may be delayed. If such situation occurs in data center all IT critical assets will be at high risk.

Recommendations

The above mentioned procedures should be developed and approved by the management to ensure continuity and consistency of data centre's physical security requirements. Procedures help improve quality and ensure consistency. The documentation should be current and accessible by all IT personnel.

2.4.2 Data Center and Disaster Recovery Site - Environmental Controls

Introduction:

Data center environmental control is a set of standard guidelines for maintaining temperature, humidity, and other physical qualities of air within a data center for the housed computing infrastructure to function optimally.

Air flow management addresses the need to improve data center computer cooling efficiency by preventing the recirculation of hot air exhausted from IT equipment and reducing bypass airflow.

There are several methods of separating hot and cold airstreams, such as hot/cold aisle containment and in-row cooling units. Overheating of data center equipment can result in reduced server performance or equipment damage due to hot exhaust air finding its way into an air inlet. Atmospheric stratification can require setting cooling equipment temperatures lower than recommended. Mixing the cooled air and exhausted air increases refrigeration costs.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no Data Center and Disaster Recovery Site - Environmental Controls
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

Absence ineffective environmental controls can cause serious damage to entity's operations, hardware, and human lives. In, the event of fire, there is a risk of serious damage to computers and other equipment. Further,

- Excess humidity can cause particles of silver to move away from connectors onto copper circuits, which cement the connectors into their sockets;
- Humid wall may lead to short circuit and fire; and
- Lesser humidity can cause static electricity.

Recommendations

Management should ensure to remove combustible material from the data center in DR site as well as near the tape library. Further, appropriate controls should be deployed for humidity controls which should be operated properly and monitored regularly.

2.5 Security of Information Systems

2.5.1 IT Policy and Procedures

Introduction:

Information Technology Services supports, empowers and advances the use of technology to sustain the organization's business operation, research and outreach mission. The Chief Information Officer (CIO) is dedicated to collaborating with the various departmental and units in providing a rich, integrated and secure electronic environment in which to educate employees, carry out secure, proper and conduct business.

The Information Security Policy will be supplemented by a suite of policies, processes, standards and procedures that will set out the expectations for information security within the organization, and will provide clear guidelines to staffs and other users of organizations information assets of their responsibilities for appropriate use and safety of these assets, and their legal obligations to comply with related statutory requirements

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no IT Policy and Procedures
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

If not guided by appropriate IT policy and procedures, the users of IT resources may be unaware of their responsibilities and work procedures, leading to the risk of:[24], [1],[5]

 Lack of security controls implementation within the Organization resulting from inadequate security awareness;

- Loss of confidential information;
- Damage and/or destruction of valuable IT information assets e.g. data, application and backups;
- Ad-hoc practices due to lack of standardization; and
- Lack of users' accountability towards systems security.

Recommendations

Management should develop framework for IT policy and procedures. Comprehensive IT procedures should be developed and approved by appropriate level of management.

Further, management could consider implementation of IT Security standard ISO 27001 and/or COBIT. Following are some IT policies and procedures which should be considered: **[1],[5],[16],[17]**

 Information Security:

- Information classification;
- Data ownership and Confidentiality;
- Logical access;
- Security incident detection and response;
- Information security administration;
- Incident detection and response;
- Personnel Security;
- Virus control;
- Information security training;

- Security awareness;
- Networks and communications;
- Internet and electronic communications security;
- Destruction of obsolete information;
- Information systems audit and control;
- Vulnerability assessment;
- Cryptography; and
- Firewalls & intrusion prevention/detection systems.

 Access Management and Data Center:

- Physical access to IT facilities;
- Data center access management procedures;
- Physical and environmental security procedures.

 Business Continuity:

- Business continuity plan;
- Backup and recovery procedures;

 Software / Solution Management:

- Software development methodology and Software development life cycle;
- Definition of business and functional aspects;
- Definition of technology capital expenditure;
- Critical supplier review process;
- Establishment of adequate contract;
- Reconciliation of software licenses; and
- Monitoring of compliance of contracts.

 Project Management:

- Project management procedures and project definition;
- Project classification;
- Project prioritization; and
- Project management framework (PMF) and standard infrastructure life cycle

(SILC).

- Change Management:
  - Comprehensive change control management procedures;
  - Pre-implementation; and
  - Post-implementation.

- Incident and Problem Management Procedures:

  - Problem management process standards;
  - Helpdesk and Process standards;
  - Escalation and notification;
  - Determination bypass and recovery;
  - Resolution;
  - Prevention and continuous improvement coordination; and
  - Ongoing self assessment.

- Resource Management:
  - Resource management policy and capacity planning;
  - Performance management system;
  - Service level management; and
  - Employee retention policy.

- Quality Management:
  - Approval of feasibility studies;
  - System validation;
  - Risk management standards;
  - Verification and acceptance testing;
  - Written acceptance criteria; and
  - Documentation standards.

- Contracting and Outsourcing:

- Third Party Service Management; and
- Ongoing vendor management.

2.5.2 IT Policy Revision Control

Introduction:

Version control is a system that records changes to a file or set of files over time so that you can recall specific versions later. For the examples in this book you will use software source code as the files being version controlled, though in reality you can do this with nearly any type of file on a computer. [18],[24],[5]

Nearly everyone in every organization has to manage multiple versions of one file or another. Contracts, benefit plan documents, router configurations, org charts, web content, accounting system scripts, software source files, even books. All are documents that someone else in your organization) change more than once

Version control is important for documents that undergo a lot of revisionand redrafting and is particularly important for electronic documents because they can easily be changed by a number of different users. These changes may not be immediately apparent.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  Medium

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no IT Policy Revision Control
1	Follow some sectors

2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

Due to absence of revision history of security policy, integrity of the security policy cannot be insured; further risk is involved due to revision control of security policy that updates in environment and security infrastructure cannot be incorporated.

Recommendations

Management should incorporate the revision control in Organizations security policy, proper updating process should be documented for following hierarchy for approvals of changes occurring in revision of security policy. Further, there should be formal procedures for the internal review to check the appropriateness of the implementation of information technology policy.

2.6 System Developments

2.6.1: IT Project Management

Introduction:

The process of creating and maintaining information systems is called systems development or systems analysis and design. This diagram shows that it involves all five components of an information system. In addition to technical knowledge, it requires business knowledge and management skill.[23],[1],[6]

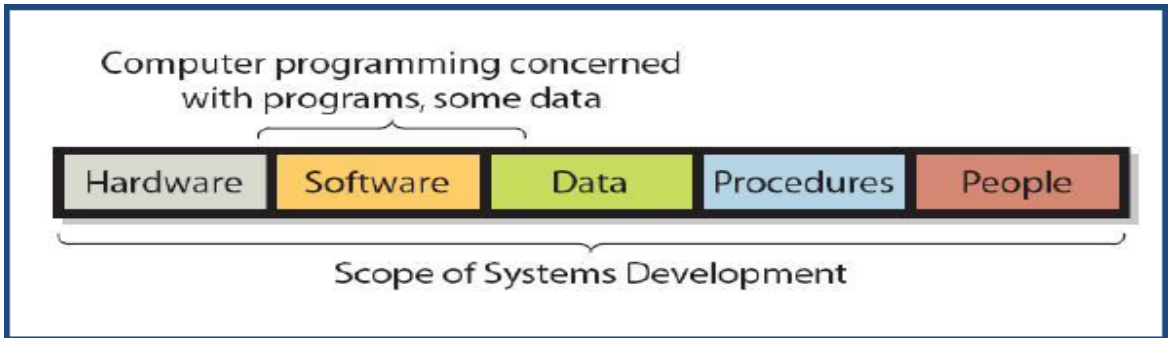

Figure-5: Systems Development vs. Program Development

The classical systems development life cycle (SDLC) process includes five phases as this diagram points out:

- System definition
- Requirements analysis
- Component design
- Implementation
- System maintenance (fix or enhance)

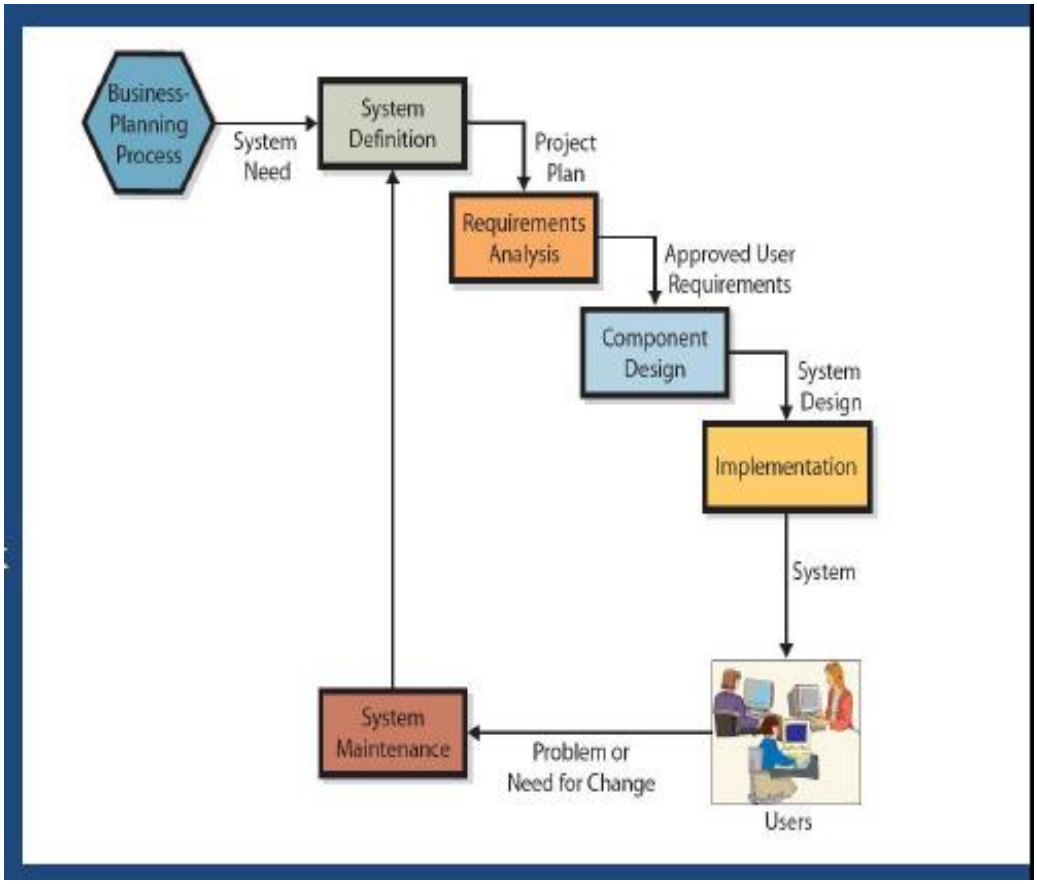

Figure-6: Phases in the SDLC

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no IT Project Management
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks/ Impacts

In the absence of formal IT project management methodology and guidelines, the Organization may face following risks:

- In appropriate project prioritization and misalignment of project objectives;
- Due to a dependency on another project, a project may be delayed and incur additional costs. Little or no contingency may be built into project deadlines, and may also result in project delays and additional costs;
- Clear reporting lines may not be established and project managers may not comply with methodologies or best practice;
- Projects may go ahead without a sufficient business case and feasibility being conducted;
- Project delays may incur costs in excess of what was budgeted for e.g. fees for legal advice, hardware and consulting;

- Insufficient planning may result in a system being implemented which is not able to meet requirements; and
- Projects may not record lessons they learned and other projects may make the same mistakes.

Recommendation

It is recommended that management should document and implement a formal IT project management methodology. Further, the IT security policy must be updated to include critical project management areas as part of solution development.

2.6.2: System Design

Introduction:

Systems design services firms plan and design computer systems that integrate computer hardware, software, and communications technologies. They help clients select the right hardware and software products for a particular project, and then develop, install, and implement the system

All five components require attention in the design phase:

- Hardware —Determine the specifications and evaluate alternatives against the requirements.
- Programs —Decide whether to use off-the-shelf software, off-the-shelf with alterations, or custom-developed software.
- Database —Convert the data model to a database design.
- Procedures —Design procedures for users, operations personnel, and for normal, backup, and failure recovery tasks.
- People —Design job descriptions for users and operations personnel. You may have to add new jobs or alter existing jobs.

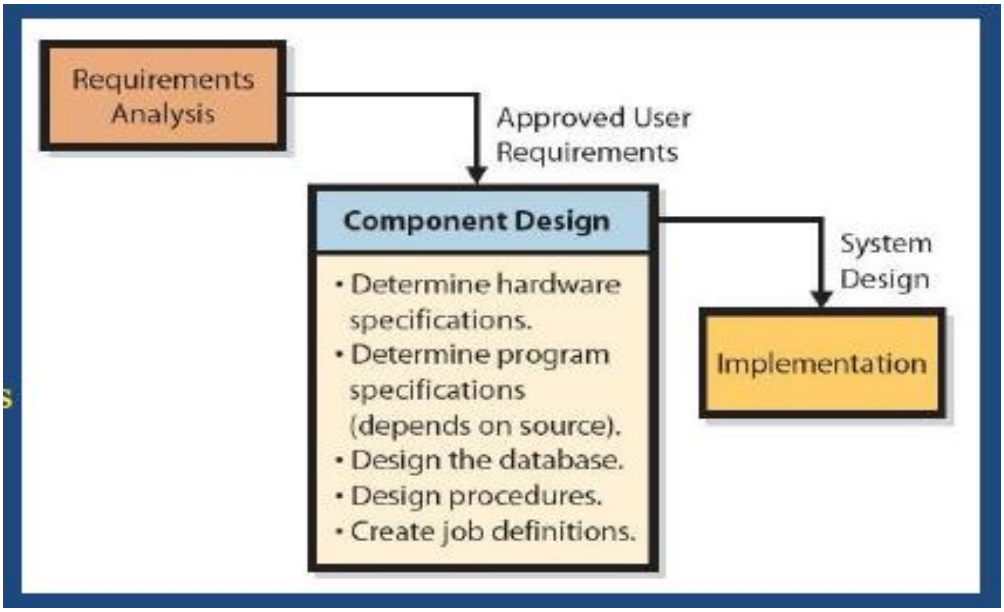

Figure-7: Implementation Phase

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no guideline for System Design
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

Without system design there is a risk of system failure because of the absence of capabilities like flexibility, scalability, performance, maintainability and testability which are suppose to consider during designing a system. Moreover in absence of system design it is difficult to indentify methods used to transactional data and what can and cannot be predicted about sound system performance.

Recommendations

IT project management team should document all system design of developed in-house software where process flow will clearly defined.

2.6.3: Software Testing

Introduction:

System testing begins by creating a test plan that spells out what actions users will take when using the new system. It includes testing normal actions and incorrect actions. Every line of program code should be executed to test error messages.
–Product quality assurance (PQA) personnel can construct a test plan with user advice and assistance. They can perform some of the testing and supervise users as they test the system.
–Users must be part of the test team and help develop test plans and test cases. Users must have the final say.
–Beta testing allows future system users to try the new system on their own in the last stage of testing.
Software testing involves the execution of a software component or system component to evaluate one or more properties of interest. In general, these properties indicate the extent to which the component or system under test

- meets the requirements that guided its design and development,
- responds correctly to all kinds of inputs,
- performs its functions within an acceptable time,

- is sufficiently usable,
- can be installed and run in its intended environments, and
- achieves the general result its stakeholders desire.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no system developed for Software Testing
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

In the absence of testing procedure there is a risk of disability to

- Discover effects;
- Avoid user detecting problems;
- Assure reliability of the software; and
- Detect a defect early, which helps in reducing the cost of defect fixing.

Recommendations

It is recommended to implement a procedure for software testing within SDLC process as well as document test report and submit to project manager.

2.6.4 Quality and Project Assurance

Introduction:

The focus of quality assurance is on the processes used in the project. Quality assurance ensures that project processes are used effectively to produce quality project deliverables. It involves following and meeting standards, continuously improving project work, and correcting project defects. [15],[1]

The following table identifies:

- The project processes subject to quality assurance.
- The quality standards and stakeholder expectations for that process.
- The quality assurance activity – e.g., quality audit or reviews, code review – that will be executed to monitor that project processes are properly followed.
- How often or when the quality assurance activity will be performed.
- The name of the person responsible for carrying out and reporting on the quality assurance activity.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is no process for Quality and Project Assurance
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it

4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

In the absence of a quality control and quality assurance process, following risks may be faced by the Organization:

- Lack of standard quality process within the development function;
- Reliance on security controls may not be established in newly developed systems; and
- Software bugs and defects may not be detected and corrected.

Recommendations

It is recommended that quality management system (QMS) should be established that provides a standard, formal and continuous approach regarding quality management that is aligned with business requirements. Further, an independent quality and project assurance team should be established, which should be responsible for exercising quality assurance and project control activities. This team will also be responsible to ensure that new programs meet user requirements, Organization's security policy requirements and business objectives.

2.6.5: Project Documentation

Introduction:

There's no doubt that project documentation is a vital part of project management. It is substantiated by the essential two functions of documentation: to make sure that project requirements are fulfilled and to establish traceability with regard to what has been done, who has done it, and when it has been done.

Documentation must lay the foundation for quality, traceability, and history for both the individual document and for the entire project documentation. It is also extremely

important that the documentation is well arranged, easy to read, and adequate.

Initiation	Planning	Execution	Control	Closure
Feasibility Report	Requirement Specification	Traceability Matrix	Change Management	Technical Document
Project Charter	Design Document	Issue Tracker	Test Document	Functional document
	Work Plan/Estimate			User Manual
				Transition/Rollout Plan
				Handover Document
				Contract Closure
				Lessons Learnt

Table-2: Project management usually follows major phases

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  Medium

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is not any process for Project Documentation
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

In absence of software documentation following risks can be identified:

- Software cannot be maintained;
- Users cannot train and they virtually cannot use the software; and
- New developers would have to re-invent the wheel in software development.

Recommendations

It is recommended to implement a process to update the documentation against each of developed software which includes:

- User Requirements Analysis;
- Management Plan;
- Software Quality Assurance Plan;
- Software Design Documents;
- Test Plan;
- System Documents;
- Test Report; and
- User Documents.

2.7 Network Security Review

2.7.1: System Risk Assessment[1],[16]

Introduction:

In real network environment, risks arise in some links can lead to changes in the others correlative risk domain which reduces the network security performance finally. Therefore, evaluating the risk transmission effect on network security has an important real significance

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is not any process for System Risk Assessment
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

Without conducting proper and documented risk assessment it may be difficult to identify and mitigate risks, ensure appropriate resource and fund allocation from senior management.

Recommendations

We recommend that the Organization should formally document procedure for performing network risk assessment and generate reports.

2.7.2: Internet Access Policy

Introduction:

Internet connectivity presents the organization with new risks that must be addressed to safeguard the facility's vital information assets.

These risks include:

Access to the Internet by personnel that is inconsistent with business needs results in the

misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet.

Additionally, the company may face loss of reputation and possible legal action through other types of misuse. All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate. Access to the Internet will be provided to users to support business activities and only on an as needed basis to perform their jobs and professional roles.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is not any process for Internet Access Policy
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

Using broadband which is not permitted by ORGANIZATION IT management is a violation of regulation. Using unsolicited connectivity is an exposure to various vulnerable websites and malicious source. P2P bit torrent is a source of malicious software. Employees are able to browse stock exchange website which is a violation of Organization's regulation.

Recommendations

We recommend that the management should monitor internet usage by employees. We also recommend that management should block systems USB ports and does not allow employees to use broadband connectivity. If internet service is required by the branches, IT division should provide them with independent wireless connectivity.

2.7.3: Vulnerable Assessment (VA) and Penetration Testing (PT)

Introduction:

Vulnerability Assessment and Penetration Testing (VAPT) are two types of vulnerability testing. The tests have different strengths and are often combined to achieve a more complete vulnerability analysis. In short, Penetration Testing and Vulnerability Assessments perform two different tasks, usually with different results, within the same area of focus.

Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to cause damage and those that cannot. Vulnerability scanners alert companies to the preexisting flaws in their code and where they are located. Penetration tests attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application. Penetration tests find exploitable flaws and measure the severity of each. A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system. Together, penetration testing and vulnerability assessment tools provide a detailed picture of the flaws that exist in an application and the risks associated with those flaws.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is not any process for Vulnerable Assessment and Penetration Testing
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

In the absence of a penetration testing / VA security assessment the Organization will not be able to identify security risks and vulnerabilities present in systems and networks. Moreover the potential risk and vulnerabilities would not be identified / mitigated thus leaving the systems and networks prone to attacks.

Recommendations

It is recommended that penetration testing / security assessment should be carried out by independent experts specifically contracted for this purpose. It can be useful in detecting vulnerabilities in the systems and networks, and for checking how effective the controls are in preventing unauthorized access due to these vulnerabilities.

2.7.4: Security Architecture Monitor and Approval

Introduction:

The biggest challenges that IT Security Department face is identifying the critical assets that makes an organization unique, locating these assets on the network, and building security defenses around them while maintaining functionality. This lack of knowledge has driven organizations to implement a "uniform protection" approach to security. With uniform protection, every system on the network is treated as equally important and must be equally monitored for malicious activity and signs of compromise.

The security architecture is one component of a product's overall architecture and is developed to provide guidance during the design of the product. It outlines the level of assurance that is required and potential impacts that this level of security could have during the development stages and on the product overall.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Severity Level  Medium

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is not any process for Security Architecture Monitor and Approval
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

Without separate Information Security division it may be difficult for The Management to design overall security architecture for Organization's head office and branches.

Recommendations

We recommend that ORGANIZATION management should consider dedicated division/personnel that will design and consolidate overall Information Security architecture and ensure IT security policy compliance.

2.8 Control Assurance

2.8.1: IT Risk Assessment

Introduction:

IT risk management can be considered a component of a wider enterprise risk management system.[24]

The establishment, maintenance and continuous update of an Information security management system (ISMS) provide a strong indication that a company is using a systematic approach for the identification, assessment and management of information security risks

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  High

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is not any process for IT Risk Assessment

1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

Lack of risk management or risk assessment procedures may leads to the following risks:

- IT risks and business risks managed independently and the impact of an IT risk on the business undetected or significant risks possibly missed;
- Irrelevant risks considered important or each risk seen as a single threat rather than in an overall context;
- Ineffective support for risk assessment by senior management or inability to explain significant risks to management; and
- Lack of cost control for risk management and/or loss of IT assets or confidentiality or integrity breach of IT assets.

Recommendations

Management should ensure that consistent approach for IT risk management is developed and followed, IT risks are effectively managed, and continuous evaluation of current IT risks and threats to the Organization is in place.

Further, organization wide risk assessment and management framework should incorporates a regular assessment of the relevant IT risks to the achievement of the IT and business objectives, forming a basis for determining how the risks should be managed and mitigated to an acceptable level. A logical and systematic risk assessment methodology must be employed including risk identification, measurement, action plan review, and the appropriate acceptance and communication of the remaining unaddressed risks.

IT Risk Management Framework helps to establish a process that is aligned to Organization's risk management framework. Risk Assessment helps to assess on a

recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis.

2.8.2: IT Audit Function

Introduction:

The internal audit function's (IAF) role has evolved from traditional (accounting and financial control) to more strategic (governance). The business environment has changed as well, and nowadays relies considerably on information technology (IT). Only a few studies have investigated IT governance from a holistic perspective. Further, no study has closely examined IAF involvement in IT governance as a whole. This study uses a holistic approach to describe IAF involvement in IT governance and to explore the influence of IAF characteristics on this involvement. Survey results indicate that IAF involvement in IT governance structures, processes, and relational capabilities has not fully expanded. Also, IAF resources and IT audit experience, IT personnel and IT training/certification, and interaction between the IAF and board of directors committees influence IAF involvement in overall IT governance. These IAF characteristics influence each dimension of IAF involvement in IT governance differently. The overall results should be useful to internal auditors, senior executives, and board members seeking to enhance, assess, or make changes to their organization's IT governance

The results of IT Audit need not be restricted to IT governance activity; it is considered vital in corporate risk mitigation for organizations to undertake regular external IT Audit projects to ensure that executive supervision of technology activities are taken seriously.

It is generally considered best practice to undertake periodic external reviews of IT to consider efficiency, costs, and service levels, risk profile and business alignment. These may take the form of a broad IT Review, or specific compliance audit activities.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  Medium

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is not any process for IT Audit Function
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

Assurance that the confidentiality, integrity and availability of information systems and technology assets are adequately protected may not be obtained by the management in the absence of skilled and experienced IS auditors in the team.

Recommendations

Management should consider hiring IS audit resources which have computer sciences background and have IS audit related certifications such as CISA, CISM etc. and should have prior experience of IS auditing in any sector.

2.8.3: IT Internal Control Assessment

Introduction:

Internal control, as define is a process for assuring achievement of an organization's objectives in operational effectiveness and efficiency, reliable financial reporting, and compliance with laws, regulations and policies. A broad concept, internal control involves everything that controls risks to an organization.

It is a means by which an organization's resources are directed, monitored, and measured. It plays an important role in detecting and preventing fraud and protecting the organization's resources, both physical (e.g., machinery and property) and intangible (e.g., reputation or intellectual property such as trademarks). At the organizational level, internal control objectives relate to the reliability of financial reporting, timely feedback on the achievement of operational or strategic goals, and compliance with laws and regulations.

Based on the importance and objective of the organization, auditor may be categorized the severity level of this element. Here, we define the severity level of the element:

Severity Level  Medium

Score Assessment of the element may consider by the following weighted values:

Put a Tick (√) marks:

Score/Weight	Weight Description
0	There is not any process for IT Internal Control Assessment
1	Follow some sectors
2	Yet to documented
3	Informal process and follow it
4	Formal process to follow
5	Formal documental and strictly follow

Risks / Impacts

Lack of IT internal control assessment and appropriate link between internal controls and risks may lead to ineffectiveness of internal controls. Employees of the Organization may be incompliant towards internal controls.

Recommendations

Management should implement the process of IT Internal Control Assessment, which should be carried out on periodic basis. The objective of the internal IT control assessment is to provide management with a view of the design of the internal control structure, as

well as the implementation of that structure. Internal control assessment is the starting point for the creation of a control improvement plan, to identify specific actionable steps necessary to deter fraud in the Organization.

Further, there should be a process to link the internal controls to risks that are related to achievement of business and IT strategy so that control objectives can be accomplished.

Chapter 3

Proposed Methodology and approach

3.1 Introduction

The way of approach of our question will have a profound effect upon the way o construct our dissertation, so this section discusses the types of research that we might undertake for our dissertation. The use of literature and case studies is considered and the merits of primary research are debated and advice is given on the use of existing research data. We may not be fond of statistics, but the potential relevance of a quantitative approach should be considered and similarly, the idea of qualitative analysis and conducting our own research may defer valuable data. The possibilities of using quantitative and qualitative data are also discussed.

3.2 Actions and Impact vs. Risk

The approach provides useful analysis and reporting which helps detailed analysis of Business/IT System Controls Review of the application. It matches controls against risks based on a traffic light approach which identifies risks based on its potential impact and likelihood of its occurrence and controls based on its strengths and weaknesses.

Overall Risk Rating	Action Required / Possible Business Impact
High	**Action must occur very shortly. Possible business impacts are:** • May have detrimental impact on operations, functions, or brand. • May have significant, measurable impact on the business. • Possible decrease in the public's confidence in the organization.
Medium	**Action should occur within a reasonable time period. Possible business impacts are:** • May have significant impact on operations, functions, or brand. • May have measurable impact on daily operations. • Should not decrease the public's confidence in the organization.
Low	**Is generally not a priority but action should occur. Possible business impacts are:** • May have minimal impact on operations, functions, or brand. • A breach of this sensitivity level may result in the degradation of operations or ability to provide timely service

Table-3: Overall Risk Rating

3.3 Risk Rating

Further, for the overall conclusion on the state of control environment in the organization, following benchmarks to be considered:

Overall Report Ratings	
Satisfactory	Control environment/system functioning as intended. If findings are noted, they need control enhancements, whereas other issues may have been identified, which should be addressed within a reasonable time frame.
Satisfactory with Exceptions	Control environment/system functioning in an acceptable manner, but findings show there is a need for improvement. Either the volume or the relative significance of findings requires positive
Needed Improvement	Several significant findings or weaknesses in control environment/system were noted (or several weaknesses were noted that, when taken collectively, are considered significant). Immediate action should be taken to correct the control
Unsatisfactory	Control environment/system not functioning as intended. Findings indicate unacceptable exposure in several areas. The condition requires improvements with more than usual management involvement and monitoring until controls are

Table-4: Overall Report Ratings

3.4 Proposed Security Audit Framework for an organization vs Overall Assessment Results:

The following Model table provides summarized ranking of observations in the report with their risk ratings with major areas that needs to be focused:

S. No	Area of Review	Total No. of Findings	No. of High Level Findings	No. of Medium Level Findings	No. of Low Level Findings	**Remarks: (Satisfactory/Satisfactory with Exceptions/Needed Improvement/Unsatisfactory)**
Overall Results for Review of IT						
Overall Results						**Based on the control deficiencies, the overall control environment has number of weakness and can be termed as "Need Improvement".**
Area wise Results						
1	Management of IT					
2	Continuity of Systems					
3	Change Management					
4	Physical Security & Environmental Controls					
5	Security of Information Systems					
6	System Development					
7	Network Security					
8	Control Assurance					

Table-5: Proposed approach vs. Overall Assessment Results

Chapter 4

Assessment and Data analysis in three Organizations with Overall

Assessment Results.

Financial/Non-Financial organization: Sample Organization-A

QUESTIONNAIRE

Development of a Security Audit Framework for a Financial and Non-Financial organizations in Bangladesh.

Instructions: Answer all questions in the section that applies to you.
Tick where appropriate and write your responses in the spaces provided.

NB: *Information provided in this questionnaire will be treated with anonymity and confidentiality*

SL	Seq.	Name of the Items	Based on Findings/Observations: (Weight / Marks) Low to High Risk→ 1& 2→ Low, 3 & 4→Medium and 5→High				
			❶	❷	❸	❷	❺
	A	**Management of IT**					
1	1	IT security steering committee	1	2	3	4	❺
2	2	IT Strategy	1	2	3	4	❺
3	3	Security Awareness Training	1	2	3	❹	5
4	4	Segregation of Duties Matrix	1	2	3	❹	5
5	5	IT Human Resource Policies	1	2	❸	4	5
6	6	Employee Satisfaction Surveys	1	2	❸	4	5
	B	**Continuity of Systems**					
7	1	Business Continuity Plan (BCP)	1	2	3	❹	5
8	2	Risk Assessment	1	2	3	❹	5
9	3	Disaster Recovery Testing	❶	❷	3	4	5
10	4	Help Desk Activities	1	2	❸	4	5
	C	**Change Management**					
11	1	Change Advisory Board	1	2	3	4	❺
12	2	Change Management	1	2	❸	4	5
13	3	Configuration and Release	1	2	3	❹	5
14	4	User Acceptance Testing Sign-	1	2	❸	4	5
	D	**Physical Security and Environmental Controls**					
15	1	Physical Access Control and	1	2	3	❹	5
16	2	Review of Access Rights of	1	❷	3	4	5

17	3	Location Selection-Primary	1	2	3	❹	5
18	4	Disaster Recovery Site -	1	❷	3	4	5
19	5	Disaster Recovery Site -	1	2	3	❹	5
	E	**Security of Information Systems**					
20	1	IT Policy and Procedures	1	2	3	4	❺
21	2	IT Policy Revision Control	1	2	3	❹	5
22	**F**	**System Development**					
23	1	IT Project Management	1	2	3	4	❺
24	2	System Design	1	2	❸	4	5
25	3	Software Testing	1	2	3	❹	5
26	4	Quality and Project Assurance	1	❷	3	4	5
27	5	Documentation	1	2	3	❹	5
	G	**Network Security Review**					
28	1	System Risk Assessment	1	2	3	❹	5
29	2	Internet Access Policy	1	2	3	❹	5
30	3	Penetration Testing	1	2	3	4	❺
31	4	Packet Analysis	1	2	❸	4	5
	H	**Control Assurance**					
32	1	IT Risk Assessment	1	2	3	4	❺
33	2	IT Audit Function	1	2	❸	4	5
34	3	IT Internal Control Assessment	1	❷	3	4	5

Table-6: Assessment questionary-1

Details of Survey Result: Sample Organization-A

S.No	Area of Review	Total No. of Findings	No. of High Level Findings	No. of Medium Level Findings	No. of Low Level Findings	Remarks: (Satisfactory/Satisfactory with Exceptions/Needed Improvement /Unsatisfactory)
Overall Results for Review of IT						
Overall Results		34	7 20%	21 62%	4 12 %	Satisfactory with Exceptions
Area wise Results						
A	Management of IT	6	2	4	1	Satisfactory with Exceptions
B	Continuity of Systems	4	0	3	1	Satisfactory
C	Change Management	4	1	3	0	Satisfactory
D	Physical Security & Environmental Controls	5	0	3	2	Satisfactory
E	Security of Information Systems	2	1	1	0	Satisfactory
F	System Development	5	1	3	1	Satisfactory
G	Network Security	4	1	3	0	Satisfactory
H	Control Assurance	3	1	1	1	Satisfactory

Table-7: Survey Result of assessment questionary-1

Survey Result: Sample Organization-A:

A: Detail Survey result:

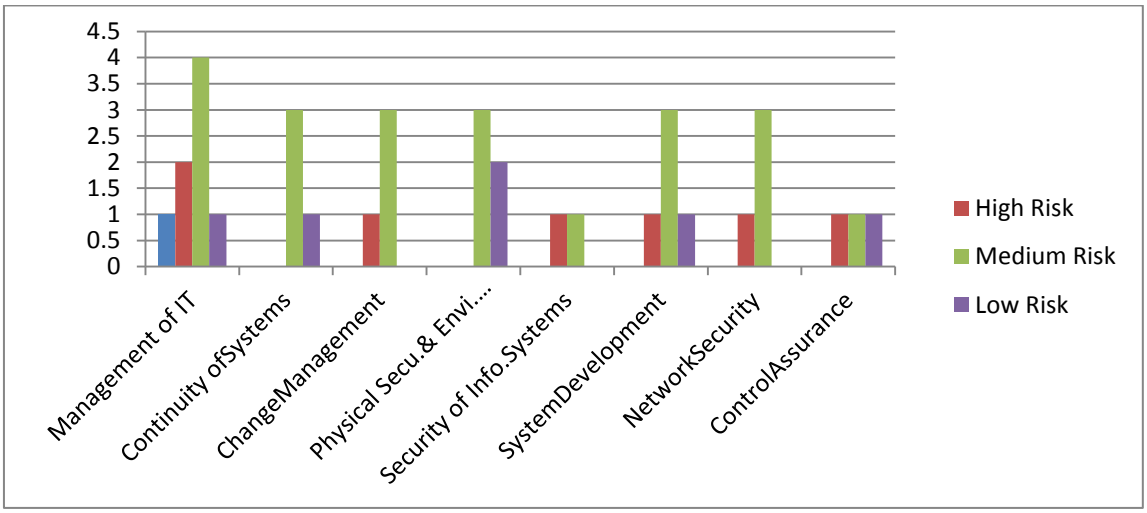

Figure-8: Survey result for assessment questionary-1

In the detail survey result and as per the column chart, it shows that the number of High, Medium and Low Risk for Management of IT is two, three and one, for Continuity of System the number is zero, three and one and so one. In this chart, the overall security level indicates low to medium in range. For high risk, it shows average to low in six cases and there is no high risk in two instance.

B) Overall Survery Result and assessment:

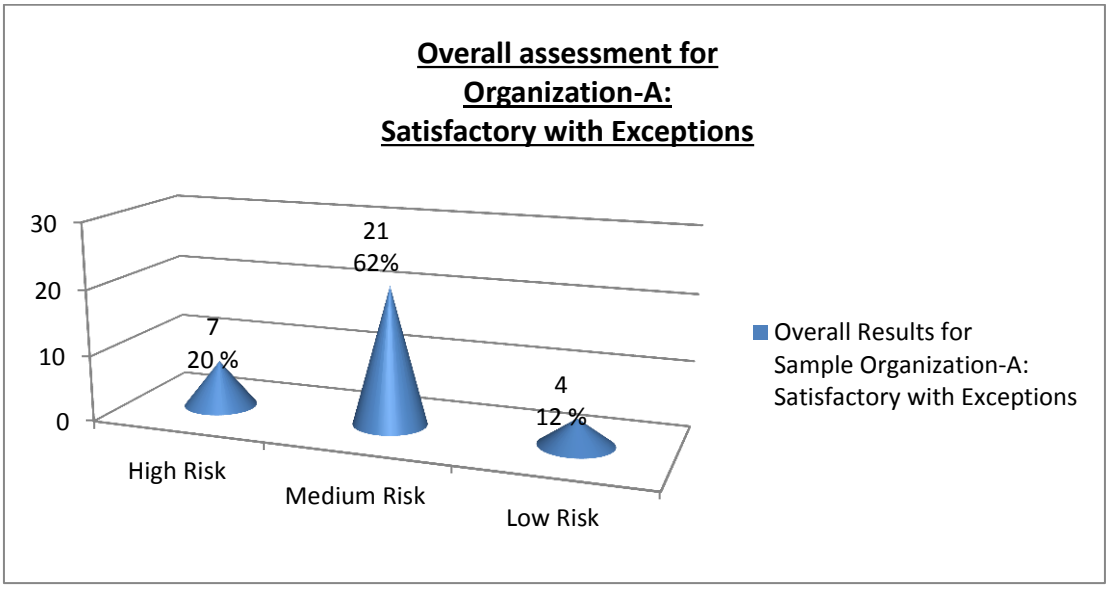

Figure-9: Overall for assessment questionary-1

In the chart, it shows that low risk is 4%, medium risk is 62% whereas high risk is 12% only. For this there need to take further steps and precautions for dropping the high and medium risks in acceptable level. Therefore, we may consider the overall security level in a "Satisfactory level with Exceptions".

Financial/Non-Financial organization: Sample Organization- B

QUESTIONNAIRE

Development of a Security Audit Framework for a financial and Non-Financial organization in Bangladesh**.**

Instructions: Answer all questions in the section that applies to you.
Tick where appropriate and write your responses in the spaces provided.

NB: *Information provided in this questionnaire will be treated with anonymity and confidentiality*

SL	Seq.	Name of the Items	Based on Findings/Observations: (Weight / Marks) Low to High Risk→ 1& 2→ Low, 3 & 4→Medium and 5→High				
			❶	❷	❸	❷	❺
	A	**Management of IT**					
1	1	IT security steering committee	1	2	3	4	❺
2	2	IT Strategy	1	2	❸	4	5
3	3	Security Awareness Training	1	2	❸	4	5
4	4	Segregation of Duties Matrix	1	2	3	❹	5
5	5	IT Human Resource Policies	1	❷	3	4	5
6	6	Employee Satisfaction Surveys	❶	2	3	4	5
	B	**Continuity of Systems**					
7	1	Business Continuity Plan (BCP)	1	2	❸	4	5
8	2	Risk Assessment	1	2	3	❹	5
9	3	Disaster Recovery Testing	❶	❷	3	4	5
10	4	Help Desk Activities	1	2	❸	4	5
	C	**Change Management**					
11	1	Change Advisory Board	1	❷	3	4	5
12	2	Change Management	1	2	❸	4	5
13	3	Configuration and Release	1	2	3	❹	5
14	4	User Acceptance Testing Sign-	1	2	❸	4	5
	D	**Physical Security and Environmental Controls**					
15	1	Physical Access Control and	1	2	3	❹	5
16	2	Review of Access Rights of	1	❷	3	4	5
17	3	Location Selection-Primary	1	2	❸	4	5
18	4	Disaster Recovery Site -	1	❷	3	4	5
19	5	Disaster Recovery Site -	1	2	3	❹	5
	E	**Security of Information Systems**					
20	1	IT Policy and Procedures	1	2	3	4	❺

21	2	IT Policy Revision Control	1	2	3	**4**	5
22	**F**	**System Development**					
23	1	IT Project Management	1	**2**	3	4	5
24	2	System Design	1	2	**3**	4	5
25	3	Software Testing	1	2	3	**4**	5
26	4	Quality and Project Assurance	1	**2**	3	4	5
27	5	Documentation	1	2	3	**4**	5
	G	**Network Security Review**					
28	1	System Risk Assessment	1	**2**	3	4	5
29	2	Internet Access Policy	1	2	3	**4**	5
30	3	Penetration Testing	1	2	3	**4**	5
31	4	Packet Analysis	1	2	**3**	4	5
	H	**Control Assurance**					
32	1	IT Risk Assessment	1	2	3	**4**	5
33	2	IT Audit Function	1	2	**3**	4	5
34	3	IT Internal Control Assessment	1	**2**	3	4	5

Table-8:- Assessment questionary-2

Details of Survey Result: Sample Organization-B

S.No	Area ofReview	Total No. of Findings	No. of High Level Findings	No. of Medium Level Findings	No. of Low Level Findings	Remarks: (Satisfactory/Satisfactory with Exceptions/Needed Improvement /Unsatisfactory)
Overall Results for Review of IT						
Overall Results		34	2 6 %	20 59 %	12 35 %	**Satisfactory**
Area wise Results						
A	**Management of IT**	6	1	3	2	**Satisfactory**
B	**Continuity of Systems**	4	0	3	2	**Satisfactory**
C	**Change Management**	4	0	2	2	**Satisfactory**
D	**Physical Security & Environmental Controls**	5	0	3	2	**Satisfactory**

E	**Security of Information Systems**	2	1	1	0	**Satisfactory**
F	**System Development**	5	0	3	2	**Satisfactory**
G	**Network Security**	4	0	3	1	**Satisfactory**
H	**Control Assurance**	3	0	2	1	**Satisfactory**

Table-9:- Survey Result of assessment questionary-2

Survey Result: Sample Organization-B:

A: Detail Survey result:

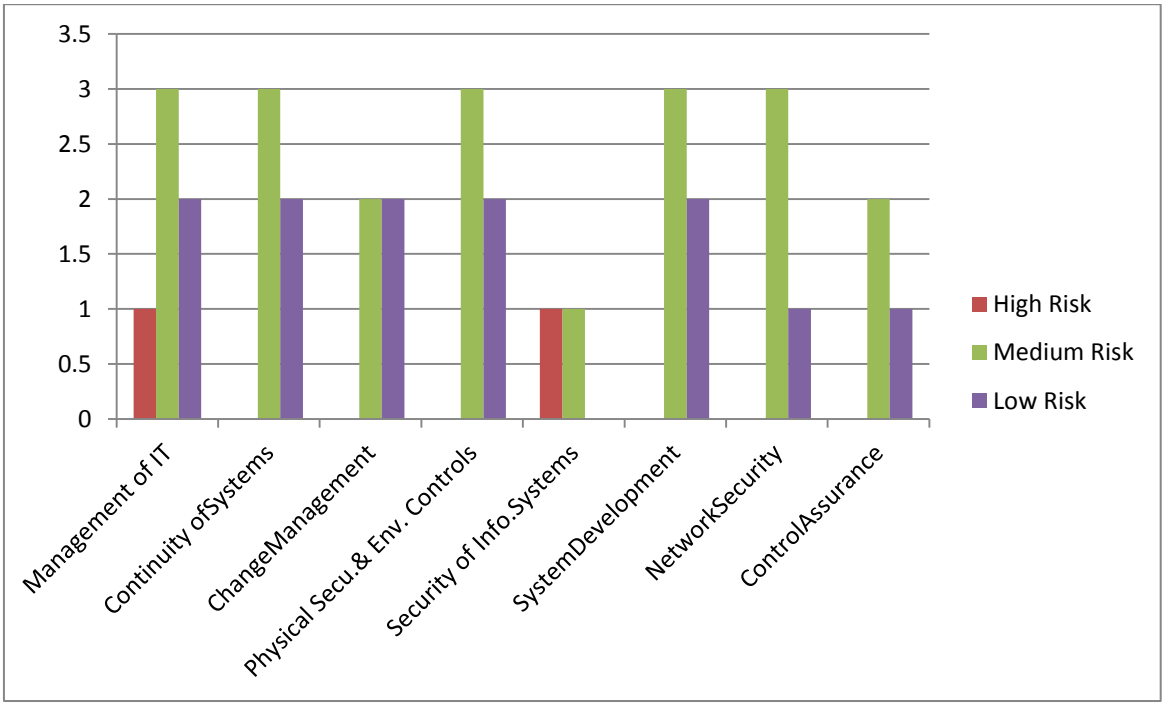

Figure- 10: Survey result for assessment questionary-2

In the detail survey result and as per the column chart, it shows that the number of High, Medium and Low Risk for Management of IT is one, three and two, for Continuity of System the number is zero, three and tow and so one. In this chart, the overall security level indicates low to medium range. For high risk, it shows average to low in three cases and there is no high risk in six instance.

B) Overall Survery Result:

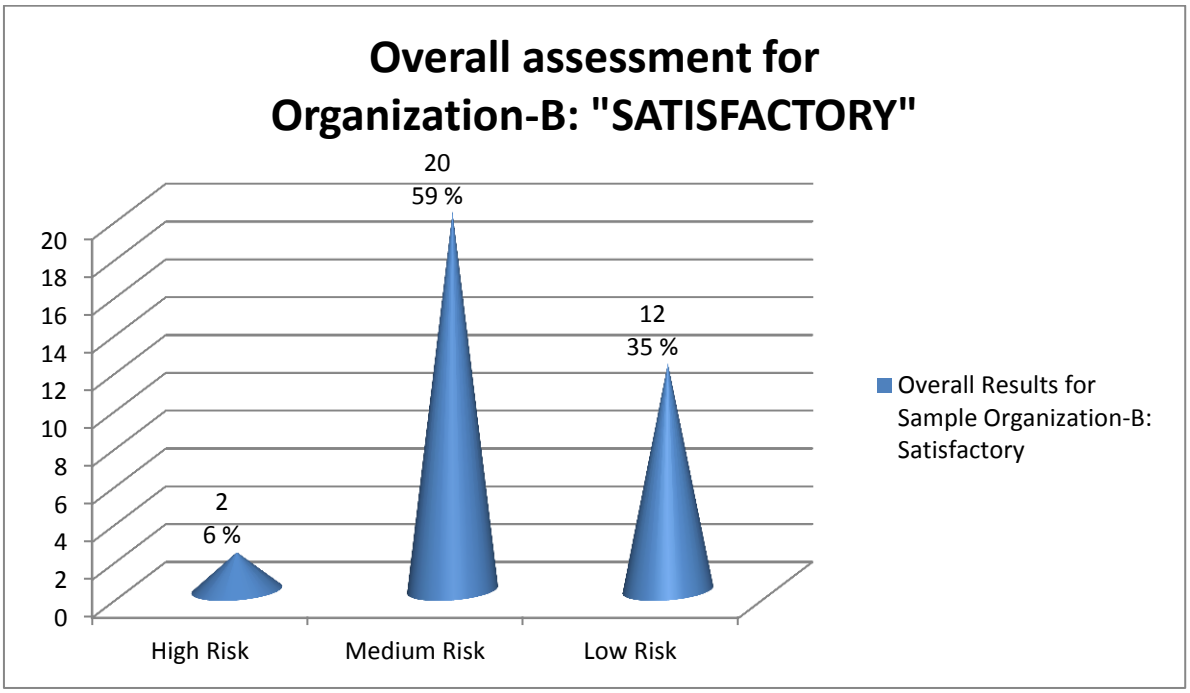

Figure- 11: Overall for assessment questionary-2

In the chart of IT security framework, it shows that low risk is 35%, medium risk is 59% whereas high risk is 6% only. For this, there need to take further steps and measures for dropping the medium risks in an acceptable level and for high risk, an organization may adopt the high risk considering business growth or feasibility. Therefore, we may consider the overall security level in a “Satisfactory”.

Financial/Non-Financial organization: Sample Organization- C

QUESTIONNAIRE

Development of a Security Audit Framework for a financial and Non-Financial organization in Bangladesh**.**

Instructions: Answer all questions in the section that applies to you.
Tick where appropriate and write your responses in the spaces provided.

NB: *Information provided in this questionnaire will be treated with anonymity and confidentiality*

SL	Seq.	Name of the Items	Based on Findings/Observations: (Weight / Marks) Low to High Risk→ 1& 2→ Low, 3 & 4→Medium and 5→High				
			❶	❷	❸	❷	❺
	A	**Management of IT**					
1	1	IT security steering committee (ITSSC)	1	2	3	4	❺
2	2	IT Strategy	1	2	3	4	❺
3	3	Security Awareness Training	1	2	❸	4	5
4	4	Segregation of Duties Matrix	1	2	3	❹	5
5	5	IT Human Resource Policies	1	2	3	❹	5
6	6	Employee Satisfaction Surveys	❶	2	3	4	5
	B	**Continuity of Systems**					
7	1	Business Continuity Plan (BCP)	1	2	3	4	❺
8	2	Risk Assessment	1	2	3	4	❺
9	3	Disaster Recovery Testing	1	2	3	❹	5
10	4	Help Desk Activities	1	2	3	❹	5
	C	**Change Management**					
11	1	Change Advisory Board	1	2	3	4	❺
12	2	Change Management Procedures	1	2	3	4	❺
13	3	Configuration and Release Management	1	2	3	❹	5
14	4	User Acceptance Testing Sign-offs	1	2	❸	4	5
	D	**Physical Security and Environmental Controls**					
15	1	Physical Access Control and Security	1	2	3	4	❺
16	2	Review of Access Rights of Data Center	1	2	3	4	❺
17	3	Location Selection-Primary Data	1	2	3	4	❺
18	4	Disaster Recovery Site - Physical	1	2	3	❹	5
19	5	Disaster Recovery Site - Environmental	1	2	3	❹	5
	E	**Security of Information Systems**					
20	1	IT Policy and Procedures	1	2	3	4	❺
21	2	IT Policy Revision Control	1	2	3	❹	5

22	**F**	**System Development**					
23	1	IT Project Management	1	2	3	4	**5**
24	2	System Design	1	2	**3**	4	5
25	3	Software Testing	1	2	3	**4**	5
26	4	Quality and Project Assurance	1	**2**	3	4	5
27	5	Documentation	1	2	3	**4**	5
	G	**Network Security Review**					
28	1	System Risk Assessment	1	2	3	4	**5**
29	2	Internet Access Policy	1	2	3	**4**	5
30	3	Penetration Testing	1	2	3	**4**	5
31	4	Packet Analysis	1	2	**3**	4	5
	H	**Control Assurance**					
32	1	IT Risk Assessment	1	2	3	4	**5**
33	2	IT Audit Function	1	2	3	4	**5**
34	3	IT Internal Control Assessment	1	**2**	3	4	5

Table-12: Assessment questionary-3

Details of Survey Result: Sample Organization-C

S.No	Area ofReview	Total No. of Findings	No. of High Level Findings	No. of Medium Level Findings	No. of Low Level Findings	Remarks: (Satisfactory/Satisfactory with Exceptions/Needed Improvement /Unsatisfactory)
Overall Results for Review of IT						
Overall Results		34	15 44 %	16 47 %	3 9 %	**Unsatisfactory**
Area wise Results						
A	**Management of IT**	6	2	3	1	**Needed Improvement**
B	**Continuity of Systems**	4	2	2	0	**Unsatisfactory**
C	**Change Management**	4	2	2	0	**Unsatisfactory**
D	**Physical Security & Environmental Controls**	5	3	2	0	**Unsatisfactory**
E	**Security of Information Systems**	2	1	1	0	**Unsatisfactory**
F	**System Development**	5	1	3	1	**Satisfactory with Exceptions**
G	**Network Security**	4	1	3	0	**Satisfactory with Exceptions**
H	**Control Assurance**	3	2	0	1	**Unsatisfactory**

Table-13: Survey Result of assessment questionary-3

Survey Result: Sample Organization-C:

A: Detail Survey result:

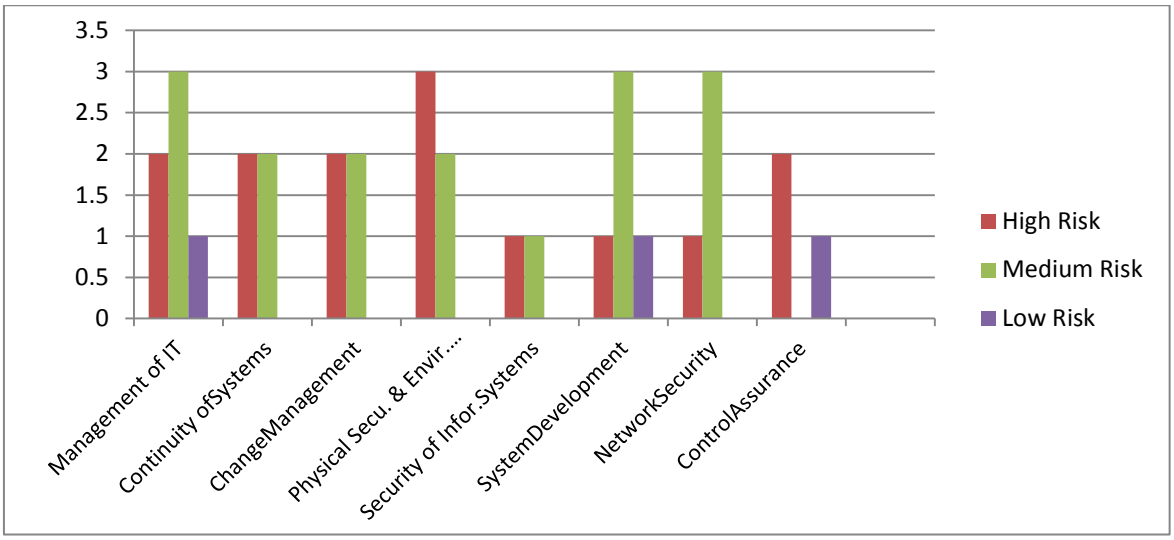

Figure-12: Survey result for assessment questionary-3

In the detail survey result and as per the column chart, it shows that the number of High, Medium and Low Risk for Management of IT is two, three and one, for Continuity of System the number is two, two and zero and so one. In this chart, the overall security level indicates medium to higher range. For high risk, it shows average too high in all cases and which is alarming and is not acceptable at all.

B) Overall Survery Result:

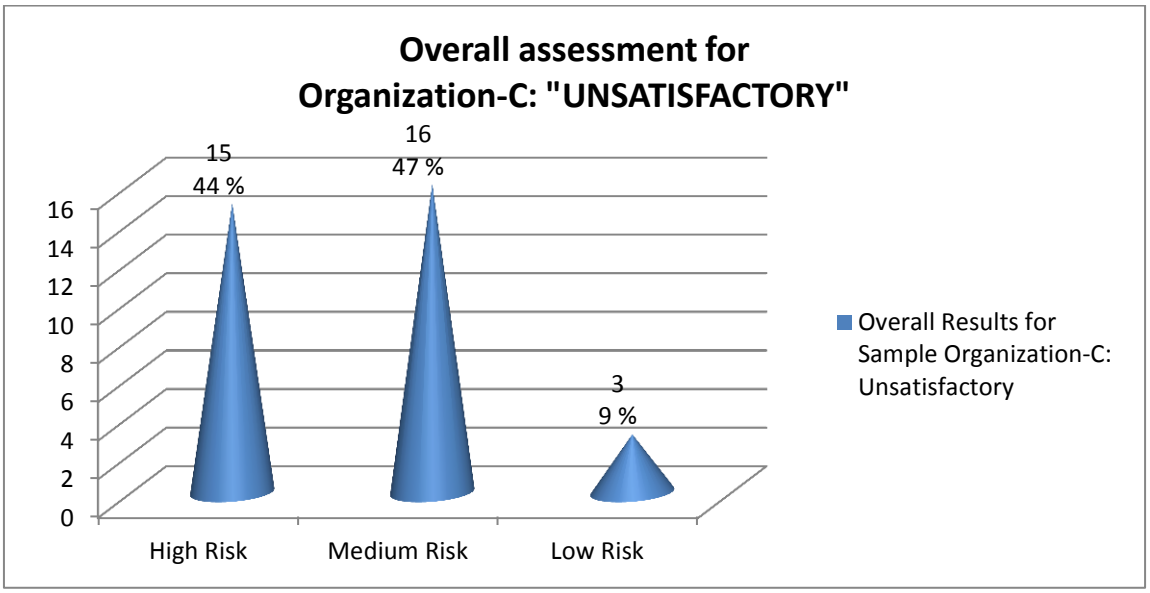

Figure-13: Overall for assessment questionary-3

In the chart of IT security framework, it shows that low risk is 9%, medium risk is 47% whereas high risk is 44% only. It is alarming and for this there need to take immediate steps and measure for dropping the high risks and in an acceptable level for an organization. Therefore, we may consider the overall security level in an "Unsatisfactory level".

Chapter-5

Conclusion and Future work

Many components of the internal control framework are in place. There are key areas where improvements are required. The concerns of the organization have undertaken initiatives and steps in establishing a comprehensive IT security access internal control framework. We recognize the effort undertaken in this regard.
In order to address the areas requiring improvements, the participation of managers and management across the Office is needed as improvements affect all the Sectors and Divisions.
A focused effort is required in:

- Formalizing and strengthening IT security policies and procedures into a main IT security program
- Establishing a security risk management process at an operational level consistent with Enterprise Risk Management (ERM) practices and polices
- Strengthening the IT security procedural framework between Services Security Unit, and Infrastructure Technology Services & other IM/IT groups.
- IT awareness program should be taken place in both employees and customer, ensuring security as a whole.

References:

[1] “Guideline on ICT Security-For Banks and Non-Bank Financial Institutions by Bangladesh Bank”, May, 2015, Version 3.0

[2] "Chapter 5: COBIT as a Framework for Enterprise Governance of IT". Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5 (2nd ed.). Springer. pp. 103–128. ISBN 9783319145471. Retrieved 24 June 2016.

[3] "ISACA Releases COBIT 5: Updated Framework for the Governance and Management of IT" (PDF). Provitivi, Inc. 18 May 2012. Retrieved 23 Jan 201

[4] "COBIT 5 for Information Security". ISACA. Retrieved 24 June 2016

[5] Lingo, Steve. "A Communications Audit: The First Step on the Way to Unified Communications". The XO Blog. Retrieved 17 Jan 2016

[6] “ISO/IEC 27000”:2016

[7] WCIT-2010 “Human resources management main role in information technology project management”, Hamid Tohidi a* Islamic Azad University, South Tehran Branch, Tehran, Iran

file:///C:/Users/mu022501/Desktop/1-s2.0-S1877050910005260-main.pdf

[8] “SATISFACTION, CITIZENSHIP BEHAVIORS, AND PERFORMANCE IN WORK UNITS: A META-ANALYSIS OF COLLECTIVE CONSTRUCT RELATIONS” Authors-DANIEL S. WHITMAN,DAVID L. VAN ROOY,CHOCKALINGAM VISWESVARAN, First published: 18 February 2010

[9] Rouse, Margaret (April 2006), “Building with modern data center design in mind”, retrieved 23 September 2015

[10] ANAO, “Business Continuity Management, Building resilience in public sector entities, Better Practice Guide” , June 2009

[11] AS/NZS 5050:2010 “Business continuity - Managing disruption-related risk”

[12]”The security Risk Assement Handbook”, Doglus J Landoll, 2006

[13]”Principles of incident response and disaster recovery”, ME Whitman, HJ Mattord, A Green - 2013

[14] “ITSMTRANSITION”, Greg Sanker, greg.sanker@itsmtransition.com

[15] “Evergreen Systems”, Inc. 2007

[16]Uropien Center Bank, “ECB-PUBLIC” 2017

[17] “ITO Security Services”, January 2011 V0.2

[18] “Springer Nature” ,© 2017 Springer International Publishing AG. Part of Springer Nature.

[19] Jiayuan Lu, Coll. of Inf. Sci., Nanjing Aduit Univ. Nanjing, Nanjing, China, Date of Conference: 20-22 Aug. 2010

[20] Steven M Bragg, Published Online: 26 SEP 2015

[21] Ernst & Young ,”Insights on governance, risk and compliance”, February 2013

[22] “Risk assessment and internal controls: continuing challenges for auditors INTERNATIONAL AUDITING PERSPECTIVES An International Accounting, Auditing & Ethics initiative”, © ICAEW 2015

[23] IIARF RESEARCH REPORT, “Evaluating Internal Control Systems A Comprehensive Assessment Model (CAM) for Enterprise Risk Management”, Carolyn Dittmeier, CIA, CRMA Paolo Casati, CIA, CRMA, 2014

[24] “Theoretical Framework of the Public Audit”, Assist. Prof. Dr. Mehmet Alpertunga Avci, 2015

[25] “Report of the Information and Communication Technology (ICT) Division – Information Technology Security Audit”, Yokon Executive Council office, Government Internal Audit service, Fiscal Year (2014 – 2015)

[26] “Internal Audit Report on IT Security Access”, Office of the Superintendent of financial institute Canada, January 2010

[27] “ISACA THE RISK IT FRAMEWORK”, https://www.isaca.org

[28] "Board Briefing on IT Governance, 2nd Edition" (PDF). IT Governance Institute. 2003. Retrieved June 24, 2014.