



Daffodil
International
University

Internship on Information System Audit

Submitted By:

Md. Asibur Rahman

ID: 182-35-2509

Section – A (26th Batch)

Department of Software Engineering

Daffodil International University

Supervised By:

Mr. Md. Maruf Hassan

Associate Professor, Department of software Engineering

Daffodil International University

This Internship report has been submitted in fulfillment of the requirements for the Degree of Bachelor of Science in Software Engineering.

Department of Software Engineering
DAFFODIL INTERNATIONAL UNIVERSITY

Spring - 2022

APPROVAL

APPROVAL (Room- 610)

This Internship titled on “**Information System Audit**”, submitted by **MD. Asibur Rahman (ID: 182-35-2509)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS



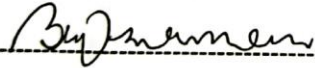
Dr. Imran Mahmud
Head and Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Chairman



Md. Shohel Arman
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 1



Khalid Been Badruzzaman Biplob
Lecturer (Senior)
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2



Md. Tanvir Quader
Senior Software Engineer
Technology Team
a2i Programme

External Examiner

DECLARATION

I hereby declare that this internship report is my original report for my Bachelor of Software Engineering program, and it was written by me with the assistance of my esteemed supervisor sir. All sources of information that were used in this internship report have been duly credited.

Furthermore, I confirm that this report is created only for my academic purpose not for any other means and I would like to assume full responsibility for any errors contained in this report.




Md. Asibur Rahman

ID: 182-35-2509

October, 2022

APPROVAL

This internship report titled “Internship on Information System Audit” by Md. Asibur Rahman, ID: 182-35-2509, Batch: SWE-26 has been approved for submission to the Department of Software Engineering, Daffodil International University, in fulfillment of the requirements for the degree of Bachelor of Science and Engineering.



MD. Maruf Hassan

Associate Professor

Department of Software Engineering

Daffodil International University

ACKNOWLEDGEMENT

First, I would like to show my gratitude to the almighty Allah (SWT) for granting me his blessing throughout these years and giving me the strength to complete my B.Sc. in Software Engineering.

I had the honor of learning under Mr. Md. Maruf Hassan sir, my respected supervisor, and I am grateful for his guidance and encouragement. His great knowledge allowed me to broaden my views and make significant progress. His keen eyes and constant support influenced me greatly with the positive motivation to work in the practical sector of the industry. His endless patience, Studious steering, continual encouragement, energetic support, constructive criticism, and valuable recommendation has attained me in my present position.

I would like to show my heartiest feelings to Dr. Imran Mahmud, Associate Professor and Head, Department of Software Engineering, Daffodil International University for his kindness and proper support for my internship. Additionally, I want to show my gratitude to all the faculties, employees and staffs for their continuous support.

I would also like to show my warmest gratitude to my course mates who supported me through these four years.

Finally, I would like to give thanks and show my gratitude to my parents and sibling for the support and patience they have shown.

ABSTRACT

Information System (IS) audit and consultancy has become a popular approach among fresh graduates and students. This report consists of a description of my work as an IS auditor in ACNABIN Chartered Accountants. This firm has 10 partners in total. I am completing my internship under our honorable partner sir Muhammad Aminul Haque, FCA and I was supervised by our honorable director Mr. A.N.M. Shakawath Hossain CISA, I have completed my internship program in this firm from 14th of February, 2022 to 14th of August, 2022. In this report I will describe each and every work that I have learnt and implemented during my internship program.

TABLE OF CONTENTS

APPROVAL	ii
DECLARATION	iii
APPROVAL	iv
ACKNOWLEDGEMENT	v
ABSTRACT	vi
TABLE OF CONTENTS.....	vii
1. INTRODUCTION	1
1.1 Objective:	1
1.2 Motivation:.....	1
1.3 Internship Goals:	1
2. COMPANY INFORMATION.....	2
2.1 Introduction about the Firm:	2
2.2 Vision:.....	2
2.3 Mission:	2
2.2 Core Services:.....	2
2.3 Organizational Structure:.....	3
3. WORKING PROCEDURE	4
3.1 Introduction:	4
3.2 Overview:	4
3.2.1 Types of IT Audit	4
3.3 Major Clients:.....	6
3.4 Audit Procedure	6
3.4.1 Documents requisition:.....	7
3.4.2 Requisition List:	8
3.4.3 Audit Format:	9
3.4.4 Documents Analysis:	13
3.4.5 Audit Report.....	21
IT Audit report of XYZ Company	22
4. CONCLUSION.....	55
REFERENCES	56

1. INTRODUCTION

1.1 Objective:

An internship program is meant to gain some real life industry experience based on the learnings of the related fields that has been learnt during the university course completion. It finds out our strength and weakness that can be very much impactful in our career. It helps us to learn how to be a perfect team player. It flourishes our soft skills and help us to get ready for the industry. It enriches our presentation and communication skills also. We also learn how to adopt new technologies while working in a project. In an internship program, we work with a bunch of industry experienced experts where we can get benefited also.

I have completed my 6 months internship program at ACNABIN Chartered Accountants as an IT Audit Intern. This internship report covers all the working experience that I have gained during my 6 months internship period.

1.2 Motivation:

As I am a student of the Department of Software Engineering (Major in Cyber Security), Daffodil International University, I have decided to gain some industry experience based on my learnings for these four years. The primary reason to do the internship is to know cybersecurity in depth with industry best practices. Because it is not possible to cover everything and get industry experience in boundaries of academic curriculum. Another reason of choosing internship it helps me to face real life challenges like facing internal and external audit and doing consultancy with renowned organizations.

I have completed “Information System Audit & Assurance Course” under major in cybersecurity. That’s why I have chosen ACNABIN Chartered Accountants where I can work independently as an external and internal IS auditor.

1.3 Internship Goals:

1. Conducting IT audits through different cybersecurity framework.
2. Doing cybersecurity consultancy.
3. Doing validation according to the framework requirements.
4. Provide report of the final assessment.
5. Knowing sensible data concerning security Audit and Assurance.
6. Gain information regarding IT tools and software that is vastly used in the industry.
7. Develop analytical and technical skills.
8. Develop professional skills with ethics and values.

2. COMPANY INFORMATION

2.1 Introduction about the Firm:

ACNABIN is one of the largest accounting firms relying on Baker Tilly International as a free institutional sub-firm in Bangladesh providing Security, Tax, Business Advisory Management, Information Systems Audit and Security ensuring the highest quality. Initiating the process in 1985, the law firm has been one of the most competent and trusted law firms for business networks and associated partners. At ACNABIN, we measure performance based on the value our customers and partners demand. Approximately 500 professionals with diverse knowledge and skills work continuously in all business areas to serve our valued customer base.

ACNABIN is a sponsored business of Baker Tilly International that focuses on more than just truly raising appreciation. To understand what the customer needs. We not only meet fast requirements, but also make long-distance arrangements. Respond to customer needs and proactively address future challenges.

ACNABIN was founded in February 1985 with a mission to continually enhance our reputation by helping our clients succeed. In the long term, he has grown to be one of the most important and reputable contract accounting firms in Bangladesh. Our culture is driven by the Baker Tilly Internal core values:

1. To lead by example
2. To deliver quality services with integrity
3. To communicate openly, to act ethically
4. And to foster a community built around civic responsibilities and teamwork.

We are passionate about helping our clients, while at the same time developing our people's potential.

2.2 Vision:

We go beyond the traditional auditor and client relationship by becoming your Trusted Business Advisor.

2.3 Mission:

We adhere to the strictest principles of client confidentiality. The sensitive and competitive nature of proprietary information and the maintenance of trust-demands it. We have built our success on such principles. We do our utmost to earn and keep client trust.

2.2 Core Services:

- IT Audit
- Audit and Assurance

- Tax and Legal Advice
- Advisory
- Cyber security consultancy
- ISO 27001 implementation.

2.3 Organizational Structure:

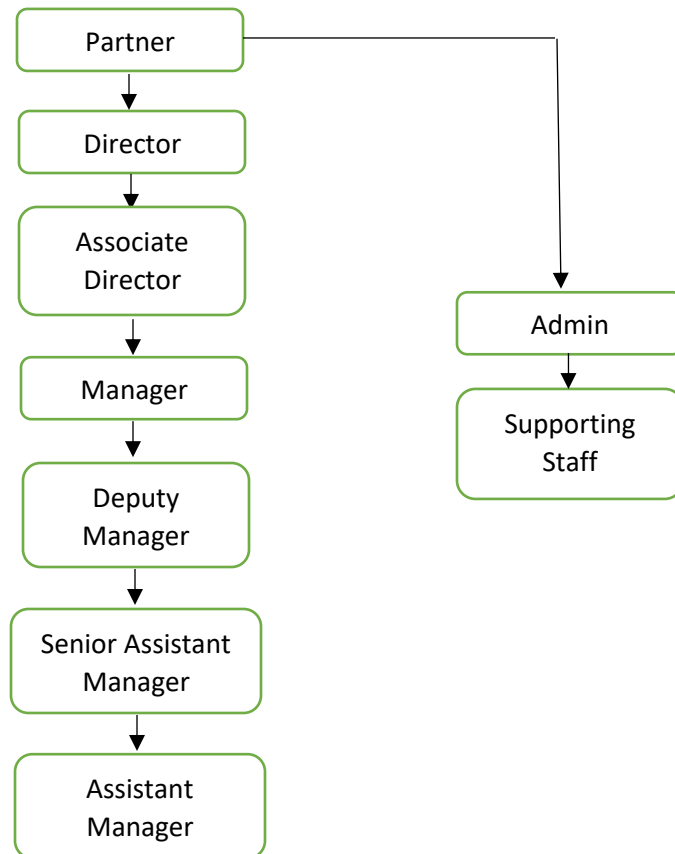


Fig – 1: Organogram Chart of ACNABIN CA

3. WORKING PROCEDURE

3.1 Introduction:

This portion will reflect my works and experiences that I have gathered during my internship period in ACNABIN Chartered Accountants as an IT auditor and cybersecurity consultant.

During this period I have supervised by Mr. A.N.M. Shakawath Hossain, CISA, CISO the Director of IT at ACNABIN Chartered Accountants.

3.2 Overview:

During this internship period, I have conducted eight IT audit in eight different clients which includes Banks, Non-Banking Financial Institutes, Manufacturing Company, Hospitals and Power generation companies and group of companies.

3.2.1 Types of IT Audit

There are two types of audits that is conducted by our firm. I have completed several projects that are following:

1. Internal Audit.
2. External Audit.

3.2.1.1 Internal IT Audit:

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

3.2.1.2 External IT Audit:

An external audit is an examination that is conducted by an independent accountant. This type of audit is most commonly intended to result in a certification of the financial statements of an entity. This certification is required by certain investors and lenders, and for all publicly-held businesses.

The objectives of an external audit are to determine:

- The accuracy and completeness of the client's accounting records;
- Whether the client's accounting records have been prepared in accordance with the applicable accounting framework; and
- Whether the client's financial statements present fairly its results and financial position.

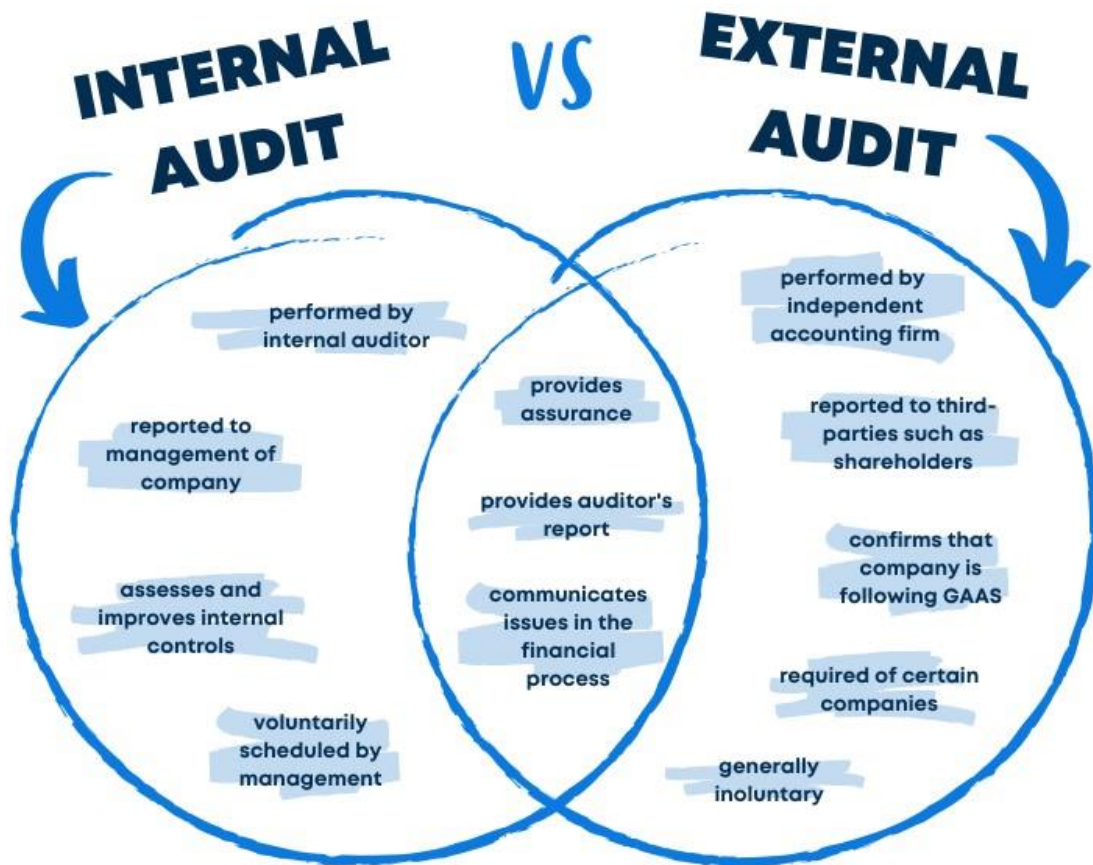


Fig – 2: Internal & External Audit

3.3 Major Clients:

My major clients in which I have completed both external and internal IT audits are:

1. External IT Audit -
 - Bangladesh Bank
 - Sonali Bank Limited
 - Grameen Bank
 - Woori Bank Bangladesh
 - Bangladesh Infrastructure Finance Fund Limited (BIFFL)
 - North West Power Generation Company Limited.
2. Internal IT Audit -
 - Walton Hi-Tech Industries Ltd. PLC
 - Ispahani Islamia Eye Hospital Ltd.
 - Ispahani Tea Ltd.

I have also done an ISO 27001 implementation Project at Walton Hi-Tech Industries Ltd. PLC.

3.4 Audit Procedure

Every Business is now associated with several IT infrastructure. Business processes has been so easy nowadays with the support of IT.

In an IT audit, in both external and internal, we place some documents requisition regarding ICT security compliance. After receiving those documents, we assess them and check the compliance. Then we find out the non-compliances and report to the management.

Here are my working steps:

1. Arrangements

The auditor will review previous audits and expert letters in your area. Auditors also research relevant policies and decisions and establish key audit programs to follow.

2. Warning

The Internal Audit Manager's workplace will notify the relevant department or department faculty of the upcoming audit and its basis when the first meeting is scheduled.

3. Commencement of meeting

This meeting includes all staff involved in the audit of the administrative and supervisory authorities. As with the audit program, we also discuss the motivations and objectives of the audit. Audit programs may be modified based on the data collected during this session.

4. Hands-on

This step includes testing to be performed and discussion with the employees in charge.

5. Write a report

Write a report after completing the practical training. The report includes areas such as audit objectives and scope, key fundamentals, findings and recommendations for revision or improvement.

6. Board Response

A draft audit report will be submitted to the audited area's administrative agency for consideration and comment on the proposals. The Board's response should include an action plan for the change.

7. Closing Session

This session will be held at the Office of Officers. Audit reports and board responses are evaluated and discussed. This is the ideal opportunity for questions and clarifications. The impact of other auditing methods not covered in the previous report will be reported at this meeting.

8. Distribution of Final Audit Report

After the final meeting, the final audit report containing the executives' responses is distributed to the audit department, the president, senior management, the CFO, and the CWRU's external accounting firm.

9. Follow-up

Approximately four months after the submission of the audit report, the audit management department will conduct a follow-up investigation. The reason for this check is to determine if corrective action has been taken.

In this chapter, I will briefly describe my whole working procedures and experience that I have gained throughout the internship program.

3.4.1 Documents requisition:

In an IT audit, the documents requisition is placed based on the following areas:

- Governance and strategy
- Data security
- Risk management
- Training and awareness
- Legal, regulatory and contractual requirements
- Policies and information security management system
- Business continuity and incident management
- Technical IT security controls

- Physical security controls
- Third-party management
- Secure development

3.4.2 Requisition List:

We ask for these documents for an IT Audit:

SL#	Document Required for IT Audit
1	"ICT Security Policy".
2	Organogram chart of ICT department including job description, segregation of duties and fallback plan.
3	Organogram for ICT support unit.
4	Scheduled roster for ICT personnel
5	Internal and/or external IS audit report (Last Three (03)).
6	Information Security Training documents for last period, copy of yearly training plan, List of participants.
7	Incident/Problem management log
8	Assessment of the risk
9	Identification of mitigation control
10	Remedial plan to reduce the risk
11	Approval of the risk acknowledgement from the owner of the risk
12	IT based/enabled product list [marked recently launched (if any) product], list of upcoming products.
13	List of software (in house and purchased).
14	Document of change procedure for IS (Documentation about –Necessary change details in production environment, Audit log of changes)
15	User Acceptance Test (UAT) for changes
16	Inventory list of all ICT assets
17	Software licenses (OS, DB, Anti-Virus, MS Office, etc.)
18	Operating procedure (Operating procedure for the users, Scheduling process, system start-up, close down, restart, recovery process.)
19	Handling of exception condition.
20	Secure disposal policy
21	Active Directory and password control policy
22	Audit trail report including user ID, authorizer ID and date-time stamp for System for a particular period of time
23	Network design document (should contain protocols and security features)
24	Email and internet usage policy
25	Outsourced software documentation
26	Business Continuity Plan
27	Backup and restore log
28	Disaster Recovery test report, list of available software in DR site.
29	SLA with software vendor, connectivity provider and with other vendors

30	Documentation about—Total Bandwidth used, No of Fiber communication link with vendor name, Network security devices
31	Annual fire testing report
32	User Creation Policy and procedures (Domain, Email, Software etc)
33	User deletion/deactivation Policy and procedures (Domain, Email, Software etc)
34	Software Design & Development related documents
35	List of security solution (Firewall, Anti-virus, SIEM, PAM etc)
36	Firewall and any other security solutions Report
37	Antivirus Dashboard Report
38	Software testing related documents
39	Role base access control list
40	List of computer/software users and their privilege
41	Server and Network utilization report in regular interval

3.4.3 Audit Format:

Based on my experience, I have conducted IT audits in the following format:

General Information:

Date	
Name of the Application/ System/DB/Network Device	
Description	
Classification	
Owner	
Custodian	
Location	
IP Address	
DNS Name	
Asset ID	

Details Information:

Area	Status	Comments
Logical Access Path		
Physical Access Path		
Remote Access		
Risk & Controls		
Risk Assessment		
List of IT Controls		
User Management		
User Management Policy		
User Creation Process		

List of All Active Users with Access Privilege		
List of Newly Created Users (Audit Year)		
No. of new user reviewed		
List of Deleted User (Audit Year)		
No of Deleted User Reviewed		
User Review		
Segregation of Duties (SoD)		
Password Management		
Password Policy		
Minimum Length of Password		
Password Complexity		
Password Expiry Period		
Remember Password		
Minimum Days		
No of wrong password input		
Password Lock Period		
Backup & Restore		
Backup Policy		
Recovery Point Objective (RPO)		
Recovery Time Objective (RTO)		
Backup Frequency		
Backup Log		
Backup Medium		
Backup Labelling		
Backup Store		
Frequency of Backup Restoring		
Backup Restore Log		
Change Management		
Change Management Policy		
Change Process		
Change Request Log (Audit Period)		
No. of Changes		
No. of Change Reviewed		
Impact of Changes		
Authorization of Changes		
Testing of Changes		
Approval of Change		

User Acceptance Testing (UAT)		
Segregation of Duties (SoD)		
Hardening		
Configuration Management Policy		
Written & Approved Configuration		
Periodic Configuration Review		
Patch Management Policy		
Patch Deployment Process		
Patch Testing before Deployment		
Last Patch Deployment Date		
Written & Approved List of Ports & Services with Business Justification		
Periodic Review of Ports & Services		
Incident/Problem Management		
Incident/Problem Management Policy		
Incident/Problem Management Process		
Incident/Problem Log		
No. of Incident		
No. of Changes Reviewed		
Root Cause Analysis		
Trend Analysis		
BIA/BCP/DRP		
Business Impact Analysis		
Business Impact		
Business Continuity Plan		
BCP Test		
Disaster Recovery Plan		
Disaster Recovery Test		
Log Management		
Log Management Policy		
Log Retention Period		
Log Review		
Audit Trail Log		
Audit Trail Log Review		
Medium of Log preserve		
Location of the Log		

Security		
Data Retention Policy		
Data Retention Period		
Secure Disposal Policy		
Anti-Virus/End-point Security		
Last Signature Update Date		
VAPT		
Internal Audit Report		
Vendor Management		
Vendor Management Policy		
Vendor Selection Process		
Name of the Vendor		
AMC/SLA		
Vendor Audit		

Logical Access Path:

Physical Access Path:

Remote Access Path:

User Creation Process:

Patch Deployment Process:

Change Process:

Incident/Problem Management Process:

Risk Register:

Risks	Risk Category	Risk Rating	Control	Comments

Control Register:

Control	Description	Effectiveness	Comments

Sample Size

Testing manual controls (=non-automated controls)

The number of samples to test when testing a manual control depends mainly on two factors – the frequency/population of the control and the risk related to the control: Sample size table:

Frequency of control	Number of items to test		
	High	Medium	Low
Annual	1		
Quarterly	2		
Monthly	4	3	2
Weekly	10	7	5
Daily	30	25	20
Multiple times per day	45	30	20

3.4.4 Documents Analysis:

ICT Security Policy:

In any kind of organization, manufacturing company, Bank, NBFI or multinational company who has implemented IT infrastructure for their business purpose should have an approved and documented ICT Security policy in place.

Generally, an ICT Security Policy must consider the following factors:

- Defining an overall organizational approach to organizational security
- Laying out user access control policies and security measures
- Detecting compromised assets such as data, networks, computers, devices, and applications
- Minimizing the adverse impacts of any compromised assets
- Protecting an organization's reputation for information security
- Complying with applicable legal requirements from standards and regulatory bodies.
- Protecting sensitive client data.
- Establishing frameworks through which to respond to questions and complaints about cybersecurity threats such as malware, ransomware, and phishing
- Limiting access to information to users with a legitimate need for it.

Organogram chart of ICT department including job description, segregation of duties and fallback plan:

The definition of an org chart or "org chart" is a diagram that shows a report or relationship hierarchy. The most common use of organizational charts is to show the structure of a company, government, or other organization.

Matrix Organization Structure of Multinational Company

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

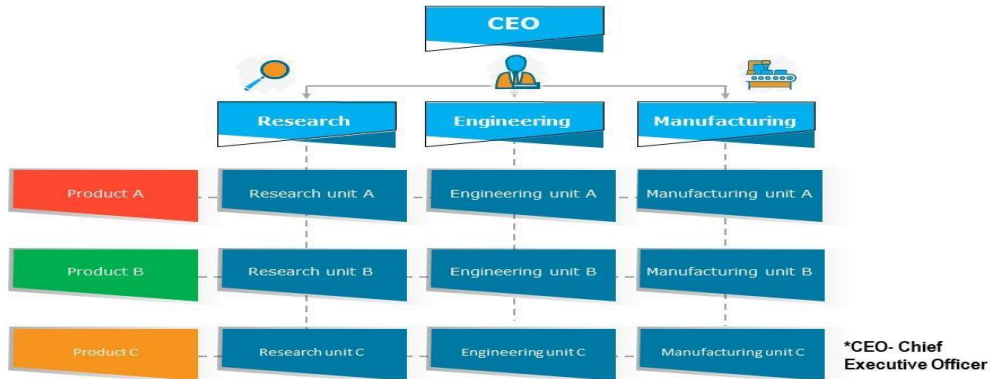


Fig – 3: Organogram Chart of a multinational Company

Incident/Problem management log:

Any kind of incidents that happens in the organization that is related to ICT security, must be kept in a separate register to assess the risk of that incident.

Assessment of the risk:

There are several risks that can breach the CIA standard of an organization. The company/organization should assess the risk based on the ISO 27001 security framework in a regular basis.

Risks should be identified and rated in three categories:

1. High
2. Medium
3. Low.

The respective company/organization should set the matrix for risk rating based on their business criticality.

Identification of mitigation control:

Risk can never be eliminated. But it can be mitigated. After assessing the risks, an organization must find out the mitigation control to mitigate the risk.

Approval of the risk acknowledgement from the owner of the risk:

In a company/organization there are several risks that are connected to several departments of that company. The respective heads of those companies are responsible for those risks. They are the risk owners.

After assessing the risks, an approval is mandatory from the risk owners regarding the acknowledgement of the risks.

IT based/enabled product list:

This list contains all information of all the ICT assets that are being used by the employees of the company.

This part should contain the following contents:

- Office
- Cost Centre
- Type
- Brand Name
- Product Model
- Product Serial
- User Name
- Dept.
- Location
- Supplier
- Invoice
- Owner
- Custodian
- Asset ID
- Asset Classification.

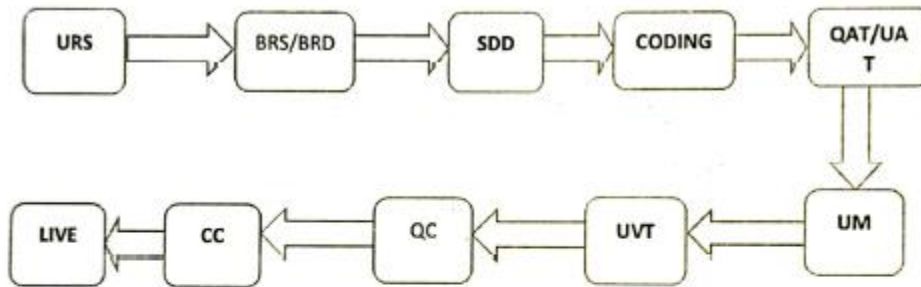
List of software (in house and purchased):

A list of software should be maintained by the company that must be approved by the management. That includes both in house and purchased software.

Document of change procedure:

Documentation about necessary change details in production environment should be maintained. Any change in the system should be done in an approved method to avoid breach of CIA standard. Audit log of changes must be kept also.

Here is a change procedure that is maintained by one of our clients:



URS: User Requirement Specification

BRS: Business Requirement Specification

SDD: Software Design Document

QAT: Quality Assurance & Testing

UM: User Manual

UVT: User Verification Test

QC: Quality Control

CC: Configuration Controller

Fig – 4: Document for Change procedure

User Acceptance Test (UAT) for changes:

After the necessary changes in the system, an UAT – User Acceptance Test must be conducted by the end user.

Software licenses:

Original licenses of OS, DB, Anti-Virus, MS Office, etc. must be kept and shared with the auditors. Unlicensed system would be a non-compliance for any organization/company.

Operating procedure:

A standard operating procedure for the users, scheduling process, system start-up, close down, restart, recovery process should be maintained.

Secure disposal policy:

Any company/organization must have a secure disposal policy for all their ICT assets. Because an out of life asset must be disposed in such a way that it can't be re used in any purpose.

Password control policy:

Any company/Organization should follow the following password guidelines to protect their system from data breach:

- Minimum length of 8 characters and maximum length of at least 64 characters if chosen by the user.
- Allow usage of ASCII characters (including space) and Unicode characters.
- Check prospective passwords against a list that contains values known to be commonly used, expected, or compromised.
- Limit consecutive failed authentication attempts on a single account to no more than 100.
- Allow "paste" functionality while entering a password.
- No complexity requirements.
- No password expiration period.
- Enforce multi-factor authentication (MFA).

Network design document:

A network design document should contain protocols and security features of the particular organization. It shows the whole network connectivity through cloud, database, servers, routers, firewall and end user computers.

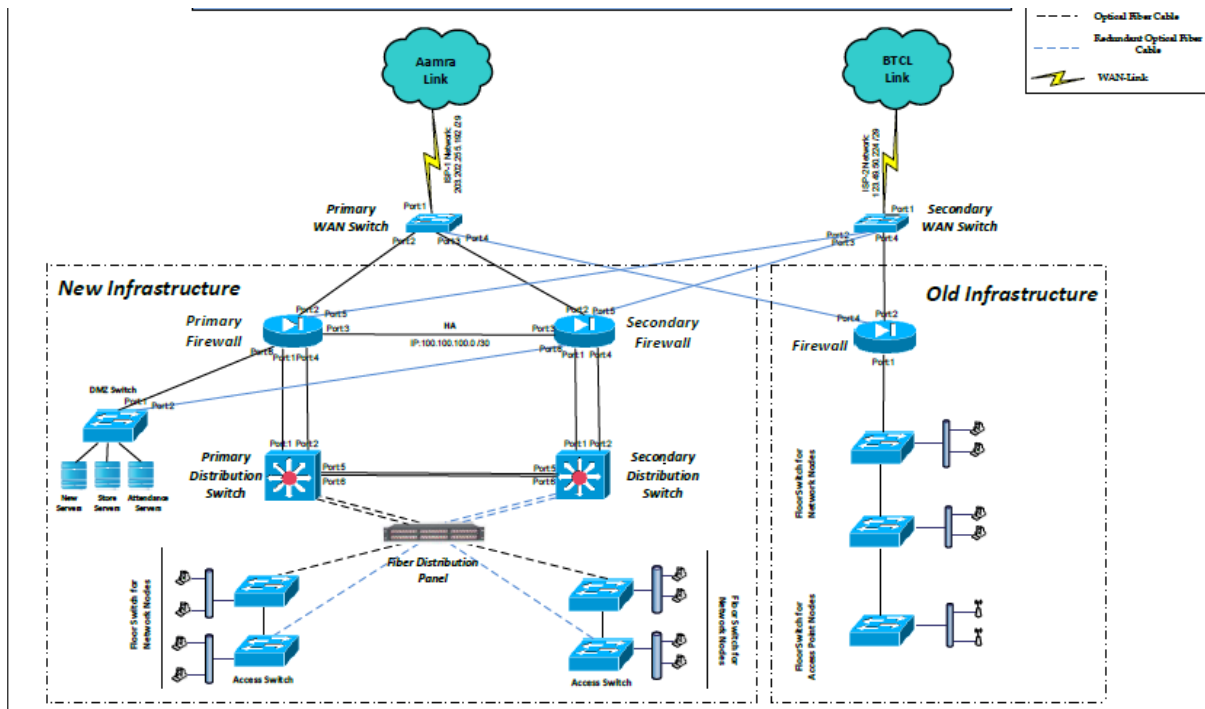


Fig 6: Network Design Document

Email and internet usage policy:

To ensure a secure email communication and prevent the system to get compromised by unauthorized emails and attachments, an organization/company must have a secure email and internet usage policy that should cover the following areas:

- Prohibition of personal use of corporate email.
- No Emailing Confidential or Proprietary Information.
- Guidelines for using attachments.
- A requirement that an employee use only approved e-mail providers.
- Policy for archiving mail. A guide to using auto responders.

Business Continuity Plan:

A business continuity plan (BCP) is a plan designed to ensure the continuity of business processes in the event of an emergency or disaster. Such emergencies or disasters may include fires or other instances in which business cannot be conducted under normal circumstances. Organizations should address all of these potential threats and develop a BCP to ensure continued operations should the threat materialize.

A business continuity plan includes:

- Organizational threat analysis
- List of major tasks required to keep the organization running
- Easy to find admin contact
- A map of where workers should go in the event of a disaster
- Sponsorship details page for your information and support of your club
- Collaboration between all parts of your club
- Feedback from everyone in your club purchase

When developing your BCP, you should identify threats that could impact your normal operations. The next step is to determine the major tasks required to continue operations. How many people do you need to keep your business running, and what tools and information do you need?

A list of managers and their contact information should be included in her BCP. These people should have each other's contact information at home. If it's not possible to get to the office, we need to be able to communicate with each other, both at home and remotely, so that we can plan for the return to work. This includes using data backups and disaster recovery plans.

Creating a BCP requires the involvement of many people. Creating a BCP is not the responsibility of one person.

Backup and restore log:

A company/organization must keep the backup of their data in a DR site. They need to restore their data also when needed.

SLA with software vendor, connectivity provider and with other vendors:

SLA stands for Service Level Agreement. A SLA must be documented for the both parties in case of any purchase or service. SLA is the mutual agreement for the purchased service with all conditions.

It is important for businesses and consumers alike to set accurate service level agreements (SLAs) for specific products to ensure smooth operations and support. As Naomi Karten explains in her work on creating service level agreements: It serves an important purpose as a communication and dispute resolution tool and as a general expectations management document.

Typical SLA content -

To create a well-organized service level agreement, there are six main components that should be included in this excellent template.

1. Contract overview -

The contract summary provides details such as a general description of who is involved, effective/expiration dates, and other details covered by each SLA.

2. Goals and targets -

The next section we need to cover is goals and objectives. The purpose of the agreement is outlined here, including the possibility of reaching mutual agreement.

3. Stakeholder -

This section defines the parties involved in the contract. For example, an IT service provider and his IT customer.

4. Periodic review -

Periodic reviews should be mentioned and should outline the effective/expiration dates and parameters associated with the review period for her particular SLA.

5. Service contract -

Next is probably the biggest part of the service level agreement, called the service contract. It contains many important components for which service providers are responsible. Topics in this section are:

- Scope of services. Deal with the specific services provided by the contract. B. Phone Support.
- Customer requirements, including payment details at agreed intervals.
- Service provider requirements are also part of the service agreement and cover areas including defining response times for service-related incidents.
- Service premise. Here we discuss logging changes to the service and how they are communicated to stakeholders.

6. Service management -

The final part of the service level agreement deals with service management. This section covers both service availability and service requests. A clear SLA provides information on phone support availability, service request response times, and remote support options.

Whether creating a service level agreement or simply ignoring it, maintaining a good relationship between service providers and service consumers involves many, if not all, of the above sections and subsections.

User Creation & Deletion Policy and procedures:

Any company/organization must have a proper user creation policy and procedures for their Domain, Email, and Software etc.

Following contents should be considered for an access control policy:

1. Introduction
2. Business Requirement for Access Control
3. Access Control Policy
4. Access to networks and network services
5. User Access Management
6. User Registration
7. Privileged Access Management
8. Management of Secret authentication information of users
9. Removal of Access Rights
10. Review of User Access Rights
11. System and Application Access Control
12. Information Access Restriction
13. Secure Log-on Procedures
14. User Password Management
15. Password Use
16. Session Time-out

Software Design & Development related documents:

When developing a software, some documentations must be in place regarding the requirements of the system software like Software requirement specifications diagram, Use cases, UI/UX design documents, Class diagrams, Entity relationship diagram, Data flow diagram etc.

We need to collect them and assess as per the requirement and business needs of the company.

3.4.5 Audit Report

After analyzing all the documents I have to prepare an audit report which includes the following headings:

1. Observation heading
2. Risk Rating
3. Root cause
4. Potential Risk
5. Recommendation
6. Management Response

Here I have attached a sample IT audit report:

IT Audit report of XYZ Company

1. Absence of ICT Security Policy.

Observation

XYZ COMPANY doesn't have any ICT Security Policy.

Risks

- Does not demonstrate the senior management's commitment to maintaining a secure IT environment.
- Does not ensure the entire organization to do a more effective job of securing the company's information assets.
- Organization may fail to manage the organization's ICT risks.

Recommendation

Company should take necessary steps to develop an IT security policy in comply with organizations mission and vision.

Management Response

2. Segregation of Duties (SoD) is not implemented.

Observation

XYZ COMPANY has not implemented segregation of duties.

Risks

- There may not be proper oversight and review to catch errors.
- Fraud or theft could not be prevented.

Recommendation

XYZ COMPANY should implement Segregation of duties (SoD) to have proper oversight to catch errors.

Management Response

3. Job description is not approved.

Observation

During the course of our audit at XYZ COMPANY, we observed that the ICT department has documented a Job description which is not approved yet. They aren't maintaining the fallback plan also.

Risk

- Performance appraisal may not be conducted properly.
- Accountability may not be established.
- Proper training may not be given and succession planning may not be done rightly.

Recommendation

Management should ensure that Job Description is documented and approved as well as communicated to the employees.

Management Response

4. No ICT support unit is formed.

Observation

No ICT support unit for ICT support by the XYZ COMPANY management.

Risks

- Immediate support could not be ensured for critical incidents.
- Organization may fail to manage ICT risk.

Recommendation

XYZ COMPANY should implement Segregation of duties (SoD) to have proper oversight to catch errors.

Management Response

5. Incident/Problem management log is not maintained.

Observation

IT team of XYZ COMPANY resolving problems when a user informing them over phone, email or any other medium. IT team resolves those issue. Problems and solutions are not recorded.

Risk

- Security breaches and weakness may not detect early or quickly.
- Relevant parties may not notify instantly when a breach or incident has occurred.
- May not prevent the damage of reputational or brand image.

Recommendation

The problem management system should have -

- A process to log the information system related problems.
- A process of workflow to escalate any problem to a concerned person to get a quick, effective and orderly response.
- Problem findings and action steps taken during the problem resolution process shall be documented.
- A trend analysis of past problems shall be performed to facilitate the identification and prevention of similar problems.
- Process shall be established to review and monitor the incidents.

XYZ COMPANY should record all the problems and solutions to effectively and efficiently manage the IT services.

Management Response

6. Does not perform the ICT risk assessment

Observation

ICT risk is the business risk. Cybersecurity or Information security begins with the ICT Risk Assessment. This is the starting point of cybersecurity implementation.

XYZ COMPANY does not perform the ICT risk assessment.

Risks

- Without knowing the risk XYZ COMPANY can't implement the accurate security control in right place. The outcome of the risk assessment demonstrate the justification of the implemented controls.
- Without risk assessment organization may not be able to determine which controls they should implement and when.
- Management may be in dark about the current security posture of the organization and the consequence, if the controls are not implemented.
- Management may not allocate budget for the security implementation.
- The flaws or vulnerabilities of the systems may not discover early and hence organization may not be able to take proper security measures to protect their systems as well as the organization

Recommendation

XYZ COMPANY should perform the ICT risk assessment.

Management Response

7. Absent of Change Management policy and procedure

Observation

We did not find change management policy and procedure in XYZ COMPANY.

Risk

- Without proper change management the changes on software, network, and system configuration may not satisfy the business need and the company may face business loss, reputational loss as well as financial loss.
- Organization may be detect the unauthorized changes on software, network & system configuration.

Recommendation

Company shall prepare and follow change management policy and procedure properly for their ICT operations.

Management Response

8. User Acceptance Test (UAT) is not performed for change management.

Observation

During the course of our audit, we have observed that User acceptance test (UAT) is not performed for any kind of changes in the system. Users confirm their changes over the phone or email with their supporting vendors.

Risk

- Changed functionalities may not perform properly.
- System may perform ineffectively due to inappropriate changes.
- Organization may face business loss, reputational loss as well as financial loss.

Recommendation

Company shall prepare and follow the User Acceptance test (UAT) properly for the changes in ICT operations.

Management Response

9. Secure Disposal Policy does not exist.

Observation

Simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file.

There is no policy and procedure exists to securely dispose ICT assets.

Risks

- Harmful for environment.
- Sensitive information may be disclose to unauthorized person(s).

Recommendation

XYZ COMPANY should develop data disposal policy and special tools must be used to securely erase data prior to equipment disposal.

Management Response

10. Absence of Password control policy and procedures

Observation

At present there is no password policy and procedures exists in XYZ COMPANY. Users using their password as per their will. In some cases we observed XYZ COMPANY using easily guessable password.

Risk

In cybersecurity context the first line of defense is a strong password. Using easily guessable passwords will put anyone at substantial risk of being hacked and having their identities stolen.

Recommendation

The company should develop password policy and procedure and should enforce this policy among the users of the IT systems.

Management Response

11. Absence of Business Continuity Plan (BCP) and Procedures

Observation

Business continuity planning (BCP) is the process involved in creating a system of prevention and recovery from potential threats to a company.

There is no Business Continuity Plan (BCP) and Procedures exists to operate the business during the disaster.

Risks

- Without having the BCP organization can't ensures that personnel and assets are protected and are able to function quickly in the event of a disaster.
- Without proper BCP, organization may not be operable during a disaster.

Recommendation

XYZ COMPANY should prepare Business Continuity Plan (BCP) and procedure.

Management Response

12. Does not perform Business Impact Analysis (BIA)

Observation

Business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency.

XYZ COMPANY does not perform the Business Impact Analysis (BIA) for ICT services.

Risks

Without BIA organization may not able to determine the most crucial business functions.

Recommendation

XYZ COMPANY should perform Business Impact Analysis (BIA).

Management Response

13. Absence of Disaster Recovery Plan (DRP)

Observation

A Disaster Recovery Plan (DRP) is a business plan that describes how work can be resumed quickly and effectively after a disaster.

XYZ COMPANY does not have any policy and procedures to resume their business after a disaster.

Risks

Without having an approved DRP the organization may not be able to resume business with enough data and system functionality to allow a business to operate on time.

Recommendation

XYZ COMPANY should develop Disaster Recovery Plan (DRP) as per business needs.

Management Response

14. Recovery Time Objective (RTO), Recovery Point Objective (RPO) not clearly define

Observation

The Recovery Time Objective (RTO) is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. RTO is determined by the cycle owner during a business impact analysis (BIA). This includes identifying a selection period for replacement or manual workarounds.

A recovery point objective (RPO) is characterized by a business continuity plan. This is the specified maximum period during which information (exchange) may be lost by an IT administrator due to a significant event.

XYZ COMPANY does not define the Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Risks

Without predefined RTO and RPO business may not be able to recover business after a disaster or disruption within business required time and tolerable data loss.

Recommendation

The company should clearly define the RPO and RTO based on Business Impact Analysis (BIA).

Management Response

15. Does not have Data Retention Policy

Observation

The data retention policies within an organization are a set of guidelines that describes which data will be archived, how long it will be kept and other factors concerning the retention of the data.

XYZ COMPANY don't have any data retention policy.

Risk

Without the clear data retention policy the organization may not archive the data as per organizational need or regulatory compliance.

Recommendation

The company shall prepare data retention policy as per there /regulatory requirements.

Management Response

16. Absence of Server or end user computers, network devices hardening policy and procedures

Observation

Currently the XYZ COMPANY does not have any policy and procedures for server or end user computers, network devices hardening.

Risk

- If not harden properly the system may consume more power, may require more processing speed and memory which may lead to financial loss.
- The unnecessary software, if not removed from the system it consumes more disk space as well as process power
- The unnecessary/inactive users of the system expose greater risk to brute-force attack.

Recommendation

The company shall develop a server/computer hardening procedures and should adhere with the policy.

Management Response

17. Does not have Log Maintenance policy

Observation

Currently XYZ COMPANY's don't have any log maintenance policy.

Risks

Without having log maintenance policy organization may not preserve log for required duration and may not be able to detect unusual activity and will not be able to perform forensic investigations.

Recommendation

The company should develop log maintenance policy and strictly follow that.

Management Response

18. Incomplete Inventory List of ICT Assets

Observation

XYZ COMPANY does not maintaining an inventory list for the ICT assets which should contain the hardware related information, software, database, data, purchase date, warranty period, owner, custodian etc.

Risks

- Without an inventory, some system components could be forgotten and be inadvertently excluded from the organization's configuration standards.
- Out of dated hardware, firmware in general are easy to breach. Without the expiry date on Assets inventory organization may fail to detect out of dated hardware, firmware.
- Detection of hardware warranty in case of hardware failure are not possible without recording warranty period on assets inventory.
- Without knowing the configuration of a server, hardware or devices it's very difficult to upgrade the system.

Recommendation

XYZ COMPANY should prepare a full ICT inventory as per Information Security Management System (ISMS) recommendation.

Management Response

19. Absent of Assets Classification

Observation:

XYZ COMPANY doesn't classify their ICT Assets.

Risks:

- Without classification of the asset XYZ COMPANY may not be able to reduce the Risk and cost of over- or under-protecting information resources in linking security to business objectives
- Information may be misused.
- XYZ COMPANY may not assess:
 - The level of access controls that should be applied to each information asset.
 - The importance of the information asset.
 - The extent and depth of the security controls.

Recommendation:

XYZ COMPANY must classify their ICT Assets as per organizational need.

Management Response:

20. Poor Asset Management

Observation:

An asset is defined as an item of value. Asset management is based on the idea that it is important to identify, track, classify and assign ownership for the most important assets to ensure they are adequately protected. Knowing what you have, where it is, how important it is, and who's responsible for it are all important pieces of puzzle.

XYZ COMPANY doesn't following proper ICT asset management.

Risks:

- Asset may not be classified based on the organization's data classification and handling policy.
- May not identify or assign the right person responsible for approving the access rights and access levels.
- Confidentiality, integrity and availability may not be ensure.
- Segregation of Duties (SoD) may not be ensure.
- Information may be misuse.

Recommendation:

XYZ COMPANY must implement Asset management process as per industry standard.

Management Response:

21. Data ownership and classification does not defined

Observation

During the course of our audit at XYZ COMPANY, we observed that ownership of data has not been formally documented for ensuring data integrity and data security of their applications/Software and area of the system(s). Formal documentations and procedures of classified and sensitive information are not in place for classifying, marking, handling, processing, or otherwise protecting the information.

Risk

Due to the absence of documented process owners with the responsibility for ensuring data integrity and data security of their particular application /area of the system(s) may lead to the following risk:

- Insufficient security measures for the systems and Data.
- Business process owners may not be held accountable for data protection and business process owners' not taking responsibility for data.

Recommendation

Data ownership and classification should be clearly defined.

Management Response

22. Does not have Portable Device Usages Policy and Procedures

Observation

Company's employees can use pen drive, portable hard disk to transfer files and these devices are not encrypted.

Risks

- Though the portable hard drive is unencrypted anyone can access the stored data on drive.
- The data can be breach if any one lost the drive. It may cause financial/ reputation/ confidentiality losses.

Recommendation

Company should develop portable device usages policy and strictly follow the policy.

Management Response

23. Individual Users can Install / download software

Observation

Individual users are able to download or install software on their desktop or laptop computer.

Risk

Many times free or pirated software comes bundled with other unwanted, harmful programs including spyware, viruses, or even Trojan horse programs.

Recommendation

Individual user should not install or download software application and/or executable file to any desktop or laptop computer without prior authorization.

Management Response

24. Pirated windows and office applications are being used by the employees.

Observation

During the course of our audit, we have observed that the management have purchased 30 genuine windows, 80 antivirus and 30 MS office license for some of their users. But there are many users who are using pirated copies of these software.

Risk

- Many times free or pirated software comes bundled with other unwanted, harmful programs including spyware, viruses, or even Trojan horse programs.
- Pirated copies may expire anytime and can crash the windows.
- Data loss can take place.

Recommendation

The management should ensure licensed software for all of their employees.

Management Response

25. Absence of handling of exception condition policy and procedure.

Observation

During the course of our audit, we have observed that no policy or procedure is maintained for handling exception condition.

Risk

- Proper procedure may not be ensured in case of any exception conditions.
- Timely response may not be established in exception condition.
- Company may face organizational, reputational and financial loss.

Recommendation

XYZ COMPANY should follow an exception handling procedure to ensure timely response.

Management Response

26. No directory service is implemented.

Observation

During the course of our audit, we have observed that XYZ COMPANY management have not implemented any directory service yet.

Risk

Without directory service BIFFL may not ensure the user management, resource management as well.

Recommendation

XYZ COMPANY should implement directory service.

Management Response

27. Absence of audit trail log.

Observation

During our audit we did not find any audit trail log for the software (Tally, CFS) using by XYZ COMPANY ICT team.

Risk

- Without audit trail log data integrity may not ensure.
- Accountability may not be ensured.

Recommendation

The management should maintain audit trail log.

Management Response

28. Absence of email and internet usage policy.

Observation

During the course of our audit, we found that the XYZ COMPANY management did not document and approved any email and internet usage policy.

Risk

- Malicious emails cannot be identified.
- Unauthorized file transfer can take place.
- Opening corrupted files can affect the whole system.
- System can get compromised.

Recommendation

XYZ COMPANY management should document an approved email & internet usage policy.

Management Response

29. Backup is only taken in an external hard drive.

Observation

During the course of our audit, we have observed that the IT department is using an external hard drive for backup.

Risk

- Data loss can take place.
- Confidentiality, integrity and availability of data cannot be ensured.
- Sensitive data may disclose to unauthorized parties.

Recommendation

The XYZ COMPANY management should not keep the backup in an external hard drive.

Management Response

30. Absence of approved user creation and deletion policy.

Observation

During the course of our audit, we have observed that the XYZ COMPANY management does not maintain any approved user creation and deletion policy and procedure for newly created and deleted users.

Risk

Without having documented and approved user creation and deletion process, inappropriate person may get access to the system and users may removed from the system without following proper process.

Recommendation

XYZ COMPANY management does document and approve user creation and deletion policy and procedure.

Management Response

31. Software testing is not performed.

Observation

During our audit period we have observed that the IT department does not perform software testing.

Risk

- Software bugs cannot be identified and fixed timely.
- Existing software bugs can hamper the company's critical works.

Recommendation

The management should perform both black box and white box testing for all of their software.

Management Response

32. Role based access control is not maintained.

Observation

During the audit period we have observed that XYZ COMPANY management does not maintain role based access control system.

Risk

- User role cannot be defined.
- One user may get unauthorized access.
- Unauthorized access cannot be identified.

Recommendation

XYZ COMPANY management should maintain the role based access control system.

Management Response

33. Privileged User Management is not implemented.

Observation

During the course of our audit, we have observed that the XYZ COMPANY management does not have implemented the privileged user management for their system users. They maintain the user access management in that way –

Software Privilege:

Stationery Requisition System:

- Super Admin -1
- Admin -7
- User- All employees without Driver, Helper, OSS etc.

Store Management System:

- Admin -Managed by vendor.
- User- Store department of Power Plants.

ERP Software:

- 8 users (all are Admin)

Task Management System:

- Admin- 1 (ICT Department)
- User- Procurement Division of Corporate Office.

CPF Management System:

- Super Admin – 1 (Managed by vendor)
- Admin-1 (A&F)
- User- All employees.

Risk

- User access cannot be identified.
- One can get access to the systems module that should not happen.

Recommendation

XYZ COMPANY authority should implement the privileged access management system.

Management Response

4. CONCLUSION

In this digital world, ICT Security has always been a top most discussed issue from both security and business perspectives. All types of companies, organizations, financial institutions are implementing ICT infrastructure to make their daily transaction easier and faster. A huge amount of data is stored in every minute to. These data needs security as most of them are very much confidential. IT audit is such a profession where I can ensure security compliances from business perspectives. I find my journey with ACNABIN Chartered Accountants as an IT Audit intern very much helpful for my personal and professional benefits. I am thankful to my firm for giving me this opportunity. This will help my career to boost up.

REFERENCES

- [1] *Advancing IT, audit, governance, risk, privacy & cybersecurity*. (n.d.). ISACA. Retrieved November 3, 2022, from <https://www.isaca.org/>
- [2] *COBIT*. (n.d.). ISACA. Retrieved November 3, 2022, from <https://www.isaca.org/resources/cobit>
- [3] *IS audit basics: The Core of IT Auditing*. (n.d.). ISACA. Retrieved November 3, 2022, from <https://www.isaca.org/resources/isaca-journal/past-issues/2014/is-audit-basics-the-core-of-it-auditing>
- [4] *ISACA portal*. (n.d.-a). Isaca.org. Retrieved November 3, 2022, from <https://www.isaca.org/bookstore/risk-it-and-risk-related/ritf2>
- [5] *ISACA portal*. (n.d.-b). Isaca.org. Retrieved November 3, 2022, from <https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko91EAC>
- [6] *ISO/IEC 27001 and related standards*. (2022). ISO. <https://www.iso.org/isoiec-27001-information-security.html>