



**Daffodil**  
*International*  
**University**

## **Internship on Information System Audit**

### **Submitted By:**

Maruf Hasan Rudro

ID: 183-35-2588

Section – A (27<sup>th</sup> Batch)

Department of Software Engineering

Daffodil International University

### **Supervised By:**

Tapushe Rabaya Toma

Assistant 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**

Summer – 2022

## APPROVAL

### APPROVAL

This Internship titled on "IT Audit", submitted by Maruf Hasan Rudro (ID: 183-35-2588) 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




-----  
Chairman

**Dr. Imran Mahmud**  
Head and Associate Professor

Department of Software Engineering

Faculty of Science and Information Technology  
Daffodil International University



-----  
Internal Examiner 1

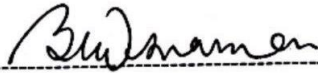
**Tapushe Rabaya Toma**

Assistant Professor

Department of Software Engineering

Faculty of Science and Information Technology

Daffodil International University

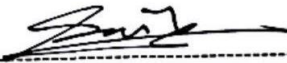


-----  
Internal Examiner 2

**Khalid Been Badruzzaman Biplob**  
Lecturer (Senior)  
Department of Software Engineering

Faculty of Science and Information Technology

Daffodil International University



-----  
External Examiner

**Md. Tanvir Quader**  
Senior Software Engineer  
Technology Team  
a2i Programme

## **DECLARATION**

I hereby declare that this internship report is my original and unique report for my Bachelor of Software Engineering program, and that it was advised by my esteemed supervisor mam. All sources of information that were used in this internship report have been duly credited. I also declare that this project or any part of this is unique and has not been submitted elsewhere for the award of any degree.

### **Submitted To**

---

Ms. Tapushe Rabaya Toma  
Assistant Professor  
Department of Software Engineering,  
Daffodil International University.

### **Submitted By**

---

Maruf Hasan Rudro  
ID: 183-35-2588  
Department of Software Engineering,  
Daffodil International University.

## **DEDICATION**

I dedicate this work to Allah almighty, who is also my creator, my unwavering ally, and my source of inspiration, wisdom, and understanding. He has been my source of power throughout this programme, and I have only been able to fly on His wings. My mother, who has consistently encouraged me and made sure I give everything I have to finish what I have started, is also honored in this work. My teachers and friends, who have both been strongly impacted in every way by this journey, deserve my gratitude.

I appreciate it. I can't express how much I care for each and every one of you. God, we thank you.

## ACKNOWLEDGEMENT

Firstly, me expressing my heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year internship successfully.

I'm really grateful and wish my profound my indebtedness to **Ms. Tapushe Rabaya Toma**, Assistant Professor, Department of SWE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of "*Internship*" to carry out this thesis. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete this internship.

I would like to express my heartiest gratitude to Dr. Imran Mahmud, Head Department of SWE, for his kind help to finish my internship and also to other faculty member and the staff of SWE department of Daffodil International University.

I would like to thank my entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

## **ABSTRACT**

Auditing and consulting for information systems (IS) has grown in popularity among recent graduates and students. Described in this report is my role as an IS auditor at ACNABIN Chartered Accountants. There are 10 partners overall in this firm. My internship is being completed under the guidance of our esteemed partner Sir Muhammad Aminul Haque, FCA, and I was under the direction of our esteemed director Mr. A.N.M. Shakawath Hossain. CISA, and still running my internship with this company, having started it on September 05, 2022. In this report, I'll go over each and every task I learned to do during my internship and put it into practice.

## TABLE OF CONTENTS

APPROVAL .....	ii
DECLARATION .....	iii
DEDICATION.....	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
2.4 Core Services: .....	3
2.5 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: .....	5
3.4 Internship Outcome .....	6
3.4.1 Contribution to the organization .....	6
3.4.3 Problems and difficulties during the internship .....	6
3.5 Audit procedure followed by ACNABIN .....	6
3.6 Audit Procedure.....	7
3.6.1 Documents requisition: .....	8
3.6.2 Requisition List:.....	8
3.6.3 Audit Format:.....	10
3.6.4 Documents Analysis: .....	14
3.6.5 Audit Report .....	22

3.7 Consultancy Audit (ISO 27001 implementation) .....	23
3.7.1 Induction.....	23
3.7.2 Scope .....	23
3.7.3 Control objectives and controls .....	23
3.7.4 Benefits.....	24
3.8 Compliance Audit.....	24
3.8.1 Introduction .....	24
3.8.2 Major IT Compliance Regulatory frameworks .....	25
3.8.3 Audit Report .....	26
3.9 IT Audit Future .....	27
4. Benefits of the Internship .....	28
5. CONCLUSION.....	29
REFERENCES .....	30



# 1. INTRODUCTION

## 1.1 Objective:

The goal of an internship programmer is to gain practical experience in the workplace based on knowledge acquired during university course work in related subjects. It exposes our strengths and weaknesses, which might have a significant impact on our career. It teaches us how to work as a great team. It develops our skills and experience and aids in our industry readiness. It improves both our communication and presenting skills. Working on a project also teaches us how to accept new technology. Opportunity to work alongside several professionals with years of expertise in the field, we may both grow from internship programmers.

I am in a period where I'll complete 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 3 months internship period.

## 1.2 Motivation:

I have chosen to obtain some industry experience based on what I have learned over the past four years as a student at Daffodil International University's Department of Software Engineering (Major in Cyber Security). The main objective of the internship is to gain in-depth knowledge about cybersecurity best practices. because it is impossible to learn about everything and gain knowledge of the industry within the confines of an academic education. The ability to tackle real-world issues including internal and external audits and consulting work with prominent firms is another reason I chose an internship.

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. Executing IT audits utilizing various cybersecurity frameworks.
2. Consulting in cybersecurity.
3. Implementing validation in accordance with framework specifications.
4. Provide a report on the evaluation's conclusion.
5. Being aware of relevant information on security audit and assurance.
6. Learn more about the IT software and technologies that are widely utilized in the sector.
7. Improve your technical and analytical abilities.
8. Develop moral and ethical professional qualities.

## 2. COMPANY INFORMATION

### 2.1 Introduction about the Firm:

One of the biggest accounting firms in Bangladesh, ACNABIN is a free institutional sub-firm of Baker Tilly International, offering the highest calibers in security, tax, business advisory management, information systems audit, and security. The legal firm started the procedures in 1985, and since then, business networks and related partners have recognized it as one of the most qualified and trustworthy law offices. At ACNABIN, we gauge success in accordance with the demands of our partners and clients. In order to support our loyal customer base, 500 professionals with a variety of abilities and skills work continually in all business sectors.

Baker Tilly International sponsors ACNABIN, a company that goes beyond merely increasing appreciation. to appreciate the demands of the client. We make long-distance arrangements in addition to quickly satisfying demands. Respond to client requirements and proactively handle prospective obstacles.

ACNABIN was established in February 1985 with the goal of improving our reputation by assisting clients in succeeding. He has developed through time into one of Bangladesh's most significant and recognized contract accounting organizations. The Baker Tilly Internal fundamental principles act as a foundation of our culture.

1. Providing a positive example.
2. To provide dependable, high-quality services.
3. Flow of information and moral behavior.
4. To promote the formation of a community based on cooperation and civic responsibility. We are passionate about helping our clients, while at the same time developing our people's potential.

### 2.2 Vision:

By becoming your Trusted Business Advisor, we go beyond the conventional auditor-client relationship.

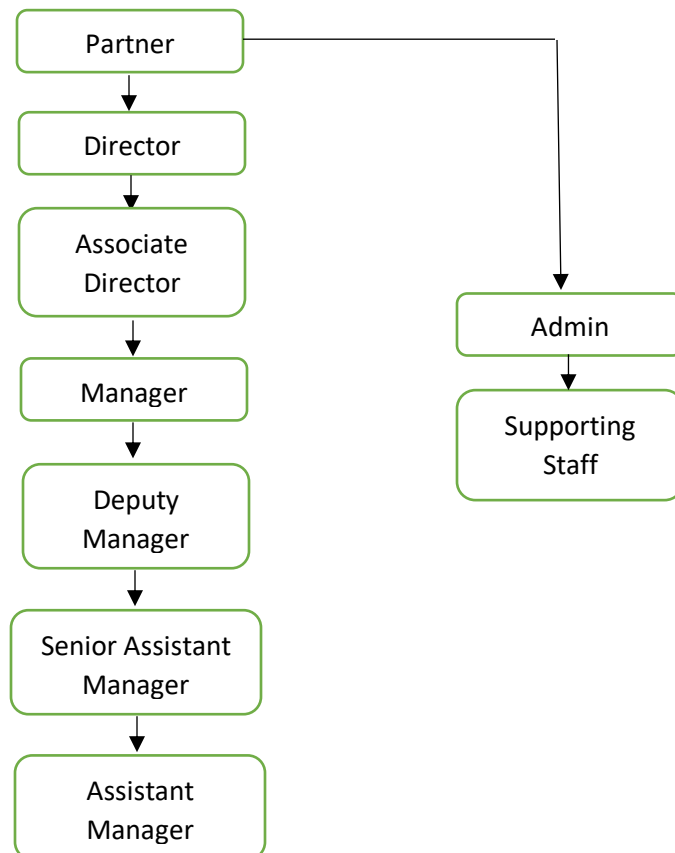
### 2.3 Mission:

We uphold the most stringent client confidentiality standards. It is necessary for the upkeep of trust and the fragile and competing nature of proprietary information. On such foundational ideas, we have established our success. We make every effort to gain and maintain client trust.

## 2.4 Core Services:

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

## 2.5 Organizational Structure:



**Fig – 1:** Organogram Chart of ACNABIN CA

### **3. WORKING PROCEDURE**

#### **3.1 Introduction:**

This section will highlight the projects and learnings I made while working as both an IT auditor and cybersecurity specialist during my internship at ACNABIN Chartered Accountants.

Mr. A.N.M. Shakawath Hossain, CISA, CISO, the Director of IT at ACNABIN Chartered Accountants, has been supervising me during this time.

#### **3.2 Overview:**

I've performed eight IT audits for eight different clients during the course of my internship, including banks, non-banking financial institutions, manufacturing organizations, hospitals, and electricity generating companies and groups 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:**

The purpose of internal auditing is to offer value and enhance an organization's operations. It is an impartial, unbiased assurance and consulting activity. By applying a standardized, analytical approach to assessing and enhancing the efficacy of risk mitigation, control, and governance procedures, it helps an organization in achieving its objectives.

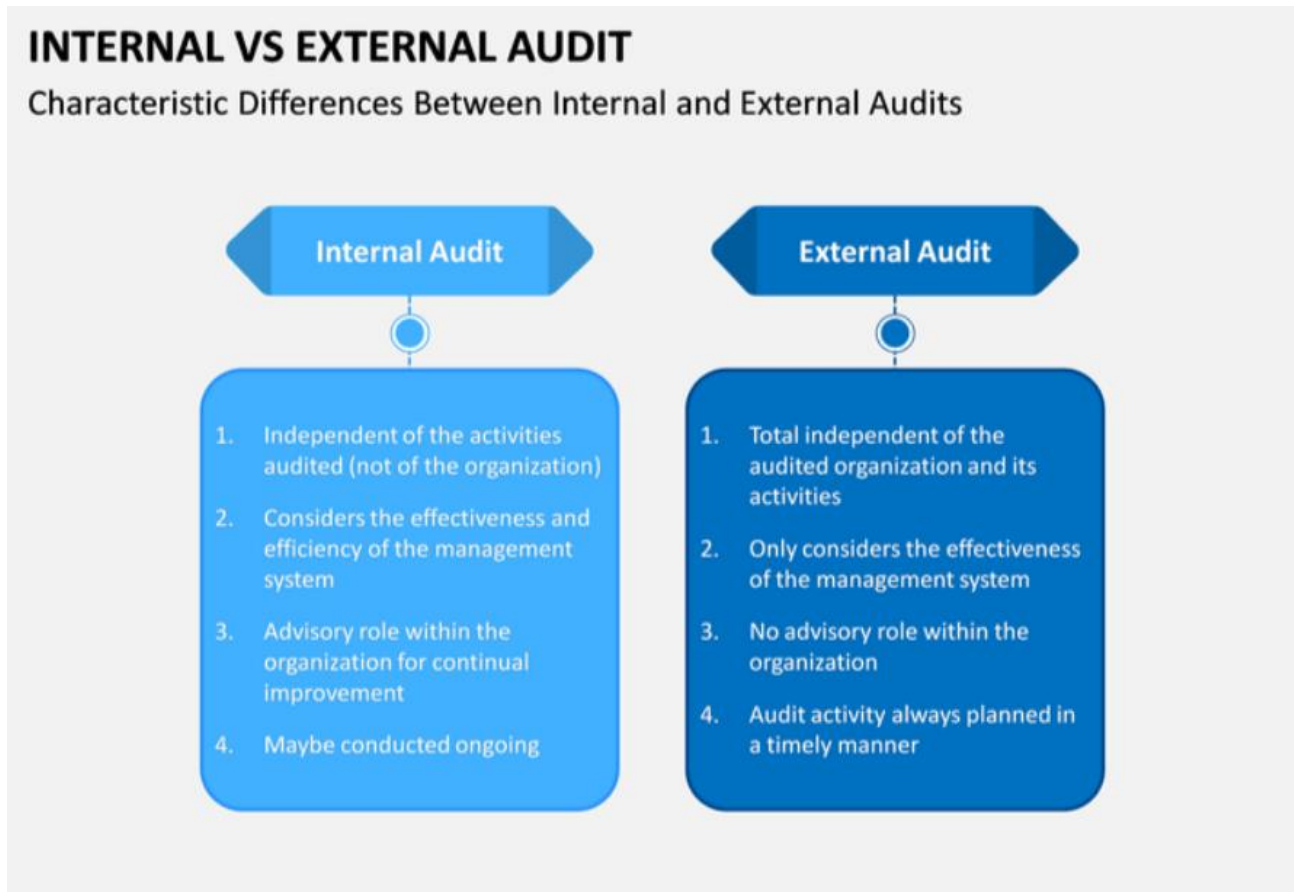
##### **3.2.1.2 External IT Audit:**

An examination carried out by an unbiased accountant is known as an external audit. The primary goal of this kind of audit is frequently certify an entity's financial statements. Certain lenders and investors, as well as all publicly-held companies, want this accreditation.

The objectives of an external audit are to determine:

- The completeness and correctness of the client's financial statements;
- If the client's financial statements have been prepared in compliance with the applicable conceptual framework for financial reporting; and

- Whether the client's accounting information correctly depict its financial condition and results.



**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 Infrastructure Finance Fund Limited (BIFFL)
  - North West Power Generation Company Limited.

2. Internal IT Audit -
  - Walton Hi-Tech Industries Ltd. PLC

I'm also doing an ISO 27001 implementation Project at Walton Hi-Tech Industries Ltd. PLC.

### **3.4 Internship Outcome**

#### **3.4.1 Contribution to the organization**

I was given the responsibility of conducting IT audits for Walton Ltd. while I was an intern at ACNABIN. I assisted team "Synergy" of the ACNABIN IT audit team there in gathering documentation for a bank IT audit. I was initially dispatched to a branch with a senior supervisor who had been appointed to that bank. Nevertheless, following an audit of three various banks. I was given the task by my director to develop an information system security policy because of this. In addition, I assisted the entire audit team in compiling papers for future audits, including incident reports, annual audit reports on their progress, and policies on risk management and IT system security. In addition, I had to speak with the senior officer directly of Walton in order to conduct additional compliance checks. Where I need to persuade and ensure the privacy of the documents, they are giving us.

#### **3.4.3 Problems and difficulties during the internship**

##### **Challenges for IT Auditor**

As an IT auditor I have faced some following challenges:

- The use of new technologies.
- The adoption of novel development strategies.
- Achieving the ideal balance between the soft skills possessed by audit teams (data analysts, ethical hackers, sociologists, fraud analysts, etc.), yet preserving the standard of audits completed.
- Data management and administration Cybersecurity and IT security.
- Staffing and skills issues Emerging technology and infrastructural developments - transformation, innovation, and disruption.
- Vendor and third-party management.

### **3.5 Audit procedure followed by ACNABIN**

There are mainly seven steps in the procedure that prescribed in Audit practice manual:

1. Identify overall goals;
2. Gather & evaluate initial information;
3. Assess general risks;
4. Assess account specific risk;

5. Develop efficient and effective audit plan program;
6. Conduct audit testing; and
7. Evaluate and communicate audit results.

### **3.6 Audit Procedure**

Today, every business is linked to various types of IT infrastructure. Today's business operations are incredibly simple because to IT.

We ask specific papers for an IT audit's compliance with ICT security standards, both internally and externally. We examine the documents and make sure they comply after collecting them. We then determine the non-compliances and notify management.

Here are the steps I take when working:

#### **1. Arrangements**

The auditor will examine prior audits and letters from local experts. Additionally, auditors create important audit initiatives and conduct relevant policy and decision-making research.

#### **2. Warning**

When the initial meeting is set, the Auditing Manager's office will inform the pertinent department or departmental faculty about the impending audit and its foundation.

#### **3. Commencement of meeting**

All employees participating in the audit of the managerial and supervisory authorities are present at this meeting. We talk about the audit's objectives and goals in the same way that we did with the audit programmer. Depending on the data gathered during this session, audit programmers may need to be improved.

#### **4. Hands-on**

This stage involves talking with the responsible staff members and conducting the diagnostic procedures.

#### **5. Write a report**

After finishing the practical training, write a report. The report covers topics like the audit's purpose and scope, core aspects, findings, and recommendations for improvement.

#### **6. Board Response**

The administrative agency for the audited region will be given a preliminary audit report to review and comment on the recommendations. An implementation plan for the modification should be included in the Board's answer.

#### **7. Closing Session**

This meeting will take place at the officers' office. Board response and audit reports are reviewed and discussed. This is the appropriate time to ask questions and get more information. At this meeting, the results of additional accounting and auditing that were not included in the prior report will be provided.

### **8. Distribution of Final Audit Report**

Following the last meeting, the auditing, the presidency, senior executives, the CFO, and the CWRU's external chartered accountants receive a copy of the final audit document that contains the executives' responses.

### **9. Follow-up**

The audit organizational management will carry out a follow-up investigation about four months after the audit report's submission. This check is being done to see if immediate measures has been performed.

I'll give a brief overview of my entire working process and the experience I acquired through the internship period in this chapter.

#### **3.6.1 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

#### **3.6.2 Requisition List:**

We ask for these documents for an IT Audit:

<b>SL#</b>	<b>Document Required for IT Audit</b>
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

### 3.6.3 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		
<b>Risk &amp; Controls</b>		
Risk Assessment		
List of IT Controls		
<b>User Management</b>		
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)		

<b>Password Management</b>		
Password Policy		
Minimum Length of Password		
Password Complexity		
Password Expiry Period		
Remember Password		
Minimum Days		
No of wrong password input		
Password Lock Period		
<b>Backup &amp; Restore</b>		
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		
<b>Change Management</b>		
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)		
<b>Hardening</b>		
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		
<b>Incident/Problem Management</b>		
Incident/Problem Management Policy		
Incident/Problem Management Process		
Incident/Problem Log		
No. of Incident		
No. of Changes Reviewed		
Root Cause Analysis		
Trend Analysis		
<b>BIA/BCP/DRP</b>		
Business Impact Analysis		
Business Impact		
Business Continuity Plan		
BCP Test		
Disaster Recovery Plan		
Disaster Recovery Test		
<b>Log Management</b>		
Log Management Policy		
Log Retention Period		
Log Review		
Audit Trail Log		
Audit Trail Log Review		
Medium of Log preserve		
Location of the Log		
<b>Security</b>		
Data Retention Policy		
Data Retention Period		
Secure Disposal Policy		
Anti-Virus/End-point Security		
Last Signature Update Date		
VAPT		
Internal Audit Report		
<b>Vendor Management</b>		
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

### 3.6.4 Documents Analysis:

#### ICT Security Policy:

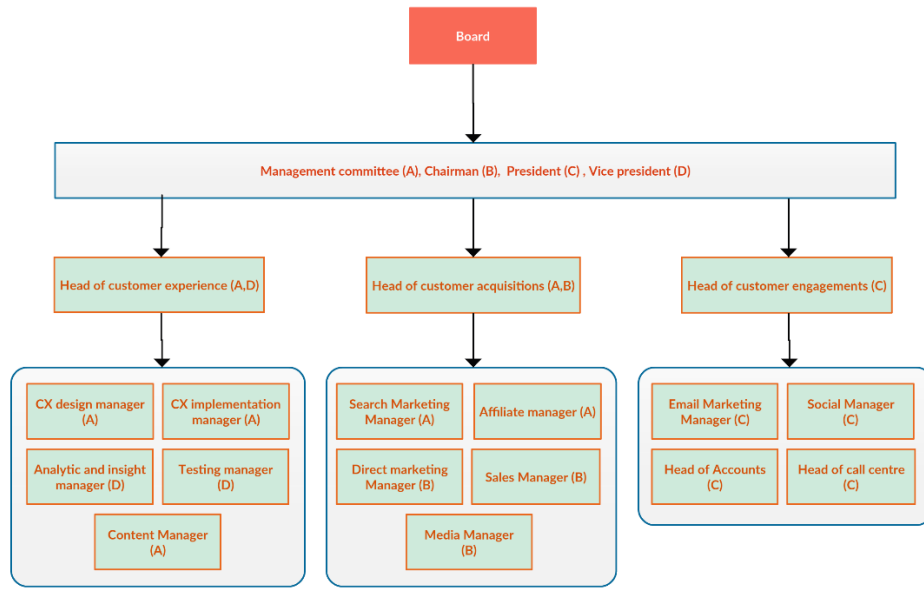
Any type of organization, including manufacturing firms, banks, non-bank financial institutions (NBFI), and multinational corporations, should have an authorized and established ICT security program in place.

In general, an ICT Information Security needs to take into account the following things:

- Formulating a comprehensive organizational strategy for organizational security
- Determining compromised assets, including data, networks, computers, devices, and applications; detecting compromised assets; and minimize the negative effects of any compromised assets.
- Preserving a company's standing in terms of information security
- Adhering to any appropriate legal demands made by standards and regulatory organizations.
- Safeguarding private client information.
- Creating procedures for responding to inquiries and grievances about cybersecurity dangers such malware, ransomware, and spoofing
- Restricting users' information accessibility to those who truly need it.

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

An organisational chart, sometimes known as an "org chart," is a graphic that displays a hierarchy of reports or relationships. Organizational charts are most commonly used to illustrate the structure of organizations, ministries, or other enterprises.



**Fig – 3:** Organogram Chart of a multinational Company

**Incident/Problem management log:**

To determine the risk of an event, a separate register must be kept for any ICT surveillance occurrences that happen in the organization.

**Assessment of the risk:**

The CIA standard of an organization can be violated in a number of ways. The business or organization needs to regularly evaluate the threat depending on the ISO 27001 security framework.

Risks should be identified and rated in three categories:

1. High
2. Medium
3. Low.

Based on how crucial their operations are to them, the appropriate corporation or company should define the vulnerability analysis matrix.

**Identification of mitigation control:**

Risk cannot be totally eliminated. However, it can be diminished. An organization needs to identify the risk mitigation control after analyzing the hazards.

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

There are a number of dangers in a company or an organization that are related to a number of its divisions. These risks are the respective owners of such organizations. Owners of the danger, they are.

The risk owners must approve the identification of the risks after the hazards have been evaluated.

**IT based/enabled product list:**

The details of every ICT asset used by the company's vision and mission are included in this list.

These items should be included in this section:

- 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):**

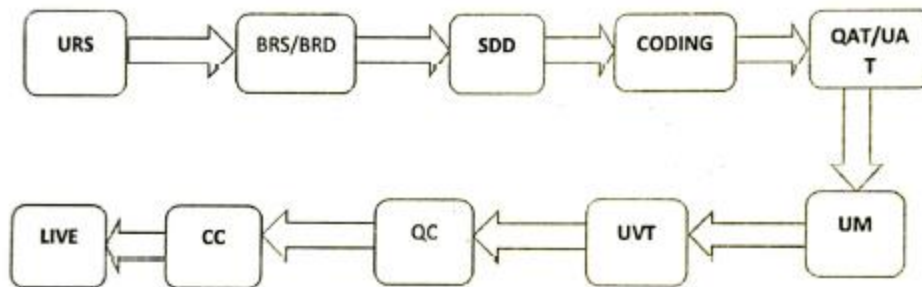
The business should have a registry of software that requires management approval. That applies to both internal and external software.

**Document of change procedure:**

It is important to retain documentation of the relevant modification information in the production environment. To prevent breaking CIA standards, all improvements to the system should be made through an approved procedure. A change audit log must be maintained as well.

Here is a modification protocol that one of our clients maintains:





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:**

An UAT - User Acceptance Test must be carried out by the end user assuming the essential process improvements.

**Software licenses:**

Original OS, DB, Anti-Virus, MS Office, and other licenses must be safeguarded and provided to the auditors. Any organization operating would be in violation if they used an unlicensed system.

**Operating procedure:**

It is important to establish a standard operating procedure for users, scheduling, system startup, breakdown, restart, and recovery.

**Secure disposal policy:**

For all of its ICT assets, any business or organization needs to establish a secure disposal policy. Because an asset that is no longer beneficial must be disposed of in a way that prevents its subsequent use for any reason.

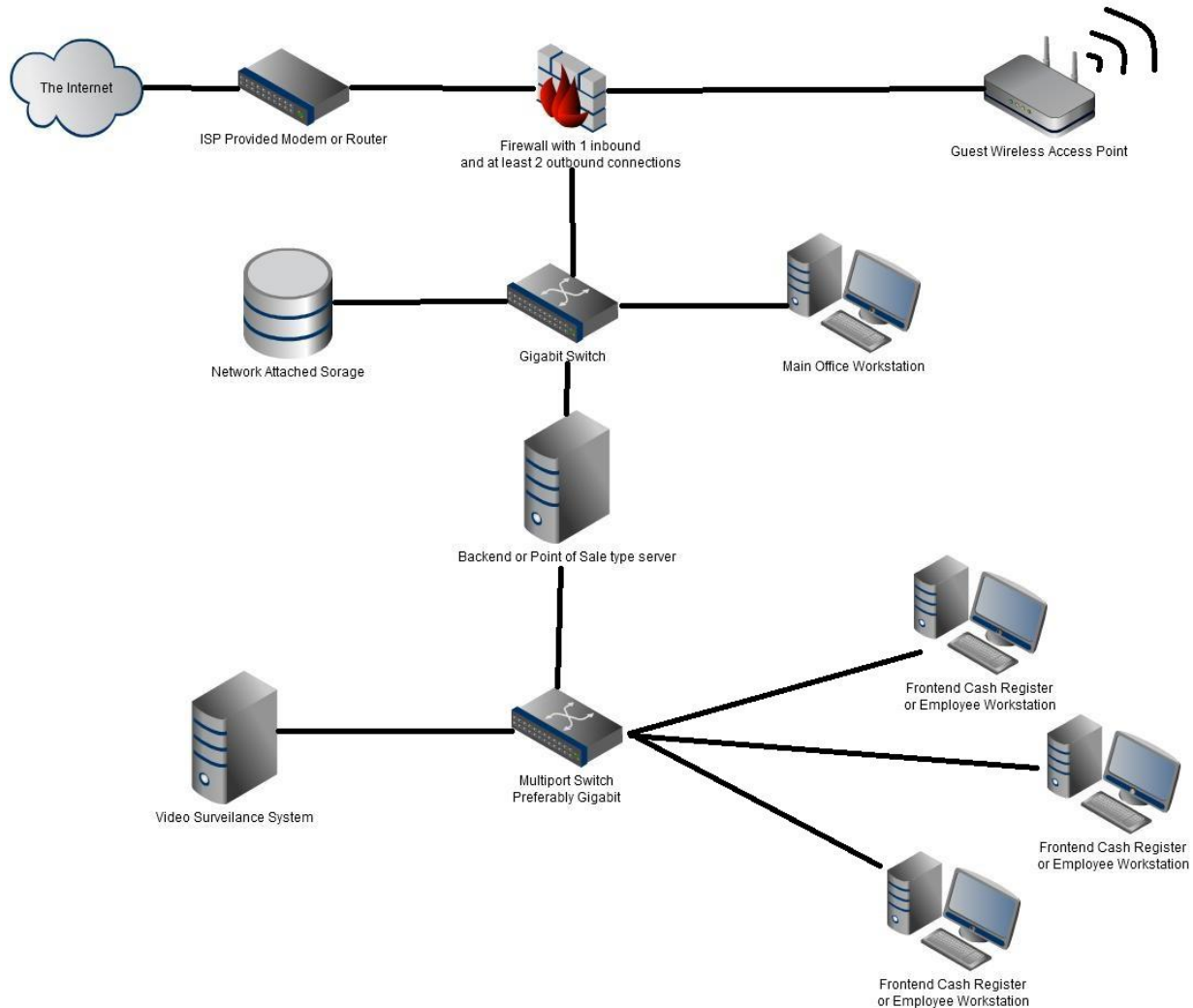
**Password control policy:**

The following password recommendations should be followed by every business or organization to safeguard their infrastructure from security breaches:

- Minimum length is 8 characters, and maximum length, if specified by the user, is 64 characters.
- Permit the use of Unicode and ASCII characters, including spaces.
- Verify potential credentials against a list of values that are known to be widely used, anticipated, or compromised.
- Don't make more than 100 continuous incorrect ensure the rights on a single account.
- Enable the "paste" feature when inputting a password.
- There are no complexity demands.
- There is no password expiration date.
- Make multi-factor authentication mandatory (MFA).

**Network design document:**

The standards and security features specific to the organization should be included in the network design paper. Via cloud, database, servers, routers, firewalls, and end user devices, it displays the connection of the entire network.



**Fig 6:** Network Design Document

**Email and internet usage policy:**

An organization or company must have a protected email and internet utilizing the resources that should cover the following topics in order to maintain secure e - mail and prevent the system from being hacked by unauthorized emails and attachments:

- Use of business email for personal purposes is forbidden.
- No Emailing of Private or Confidential Information.
- Useful guidelines for attachments
- A mandate that an employee utilize only registered e-mail providers.
- Mail archiving standards. An instruction booklet for autoresponders.

**Business Continuity Plan:**

A business continuity plan (BCP) is a strategy created to ensure that operational procedures will continue in the case of an emergency or natural disaster. Fires as well as other circumstances where business cannot be handled normally are examples of such emergencies or disasters. In order to ensure that business operations continue in the event that a danger situation occurs, organizations should address every one of these potential hazards and develop a BCP.

A business continuity plan includes:

- A map showing where employees should move in the event of a crisis.
- An analysis of the threats to the organization.
- A list of the major tasks needed to keep the organization operating.
- Collaboration between all club members.
- Feedback from all club members.
- Endorsement details page for your assistance and knowledge of your group.

You should consider dangers that could affect your everyday operations while creating your BCP. The next stage is to decide which major chores are necessary to keep everything running. How many employees, what equipment, and what knowledge are required to maintain your business on track?

Her BCP should have a list of administrators and their contact details. They ought to have each other's phone numbers at home. We must be able to contact with one another both at residence and virtually if going to the office is not an option so that together we can prepare for returning to work. Employing backup process and planning for disaster recovery is part of this.

A large number of people must be involved in developing a BCP. A BCP is not the sole responsibility of one individual.

**Backup and restore log:**

Data backups for a firm or organization must be kept at a disaster recovery site. When required, they must also restore their data.

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

service level agreement, or SLA. In the event of any transaction or service, SLA must always be established for the benefit of both parties. SLA is the international convention for the service that was acquired, containing all of the terms.

Setting precise service level agreements (SLAs) for certain goods is crucial for both businesses and customers to guarantee efficient operations and support. Creating terms and conditions serves a crucial function as a communicative and conflict resolution tool as well as a general preconceptions management document, as Naomi Karten notes in her work on the subject.

## **Typical SLA content -**

There are six key elements that need to be included in this great template in order to establish a well-structured service level agreement.

### 1. Contract overview -

A comprehensive overview of those engaged, the start and end dates of each SLA, and other information are all provided in the contract summary.

### 2. Goals and targets -

Goals and objectives must be included in the next section. Herein is set forth the aim of the Agreement, including the possibilities of mutual agreement.

### 3. Stakeholder -

The parties to the contract are described in this section. An IT services and his IT client, for instance.

### 4. Periodic review -

Performance evaluations should be noted, and they should specify the characteristics of the testing period for her specific SLA as well as the effective and expiration dates.

### 5. Service contract -

The service contract, which comes next, is most often the largest component of the terms and conditions. There are numerous significant components in it for which network operators are accountable. This section's subjects include:

- The services' scope. Discuss the particular services covered by the contract. Support by phone (B).
- Customer needs, such as payment information sent at predetermined times.
- The service agreement also includes standards for service providers that include specifying reaction timeframes for service-related events.
- Service location. Here, we talk about notifying stakeholders of service modifications that are made to the logging system.

### 6. Service management -

The service level agreement's final section addresses service management. Both service requests and service availability are covered in this section. The availability of phone assistance, the turnaround times for service requests, and the possibilities for remote support are all detailed in a clear SLA.

Maintaining a positive connection among service providers and customers consumers entails numerous, if not all, of the aforementioned sections and subsections, whether one chooses to create a service - level agreements or simply ignore it.

### **User Creation & Deletion Policy and procedures:**

Every business or organization has to have appropriate user creation policies and practices in place for its domain, email, software, etc.

An policy governing access control should take the following elements into account:

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:**

Software requirement specifications diagrams, use cases, UI/UX design documents, class diagrams, er diagrams, data flow diagrams, and others must all be in place before beginning software development.

We must gather them and evaluate them in accordance with the company's requirements and operational demands.

### **3.6.5 Audit Report**

I must produce an audit report after studying all the documents, and it must include the following sections:

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

## **3.7 Consultancy Audit (ISO 27001 implementation)**

### **3.7.1 Induction**

ISO (Information organization for standardization) 27001 is a framework for IT security implementation and can also assist in determining the status of information security and the degree of compliance with security policies, directives, and standards. (ISACA) The information security management system preserves the confidentiality, integrity, and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed. It is important that the information security management system is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. It is expected that an information security management system implementation will be scaled by the needs of the organization. This International Standard can be used by internal and external parties to assess the organization's ability to meet the organization's information security requirements. The order in which requirements are presented in this International Standard does not reflect their importance or imply the order in which they are to be implemented. The list items are enumerated for reference purposes only. ISO/IEC 27000 describes the overview and the vocabulary of information security management systems, referencing the information security management system family of standards (including ISO/IEC 27003[2], ISO/IEC 27004[3], and ISO/IEC 27005[4]), with related terms and definitions.

### **3.7.2 Scope**

The parameters for establishing, putting into practice, maintaining, and continuously enhancing a security management system isms within the context of organizations are laid out in this International Standard. In accordance with the demands of the company, this Iso Standard also specifies requirements for the evaluation and management of information security threats. This International Standard's standards are general in nature and are meant to be important for all organizations, despite of their form, size, or nature.

### **3.7.3 Control objectives and controls**

- 1.Policies for information security.
2. Information security management.
3. Protection of human resources.
4. Asset administration.
5. Access management.
6. Cryptography.

7. Environmental and physical safety.
8. Security in operations.
9. Protection of communications.
10. System development, acquisition, and upkeep.
11. Relationships with suppliers.
12. Management of information security incidents.
13. Business continuity management information security considerations.
14. compliance.

Any organization that wishes to apply ISO 27001 must meet the requirements of these 14 controls. The establishment, implementation, maintenance, and ongoing improvement of a security management system isms within the framework of the organization can all be covered by these 14 controls.

#### **3.7.4 Benefits**

A company can be certified to the international standard ISO 27001. Companies can develop their-

- Improvements in customer and supplier partner confidence.
- Rise in company resilience.
- Alignment with customer requirements.
- Better management practices and
- Alignment with corporate risk policies are just a few of the benefits that can be attained.

### **3.8 Compliance Audit**

#### **3.8.1 Introduction**

The way IT has changed over the years has had a perfect impact on the company's overall compliance-related problems.

Because they aid firms in setting a certain protocol regarding compliance-related concerns which are set by authorities and other connected bodies, it is apparent that IT Compliance linked difficulties can be recognized as remarkable and very significant.

As a result, it is clear why IT Compliance Auditors are in high demand. They cover a wide range of compliance-related topics as well as other important elements that might protect the organization from potential financial losses.

As can be observed, IT Compliance Auditors are tasked with making sure that any IT-related concerns within the firm are legal as well as any other pertinent issues that may aid organizations in abiding by the established laws and company policies.



### **3.8.2 Major IT Compliance Regulatory frameworks**

#### **PCI-DSS (Payment Card Industry Data Security Standard)**

PCI compliance is a set of regulations that ensure that all companies that accept, process, store, or transmit credit card data maintain a secure environment to protect it.

#### **SOC 2 (Systems and Organizational Controls)**

SOC 2 is a compliance audit defined by the and is an accepted standard of current technology companies. Its main focus is being able to store customer data, and it applies to service providers who use the cloud. These companies are required to be SOC 2 compliant due to their strict policies and procedures.

#### **ISO (International Organization of Standardization)**

The ISO compliance audit is part of the ISO/IEC 27K Series and is an information security compliance standard. This standard helps companies manage and develop a high level of protection for their critical data such as employee or third-party data, financial information, and intellectual property.

Both the SOC 2 and the ISO 27001 certifications are risk management processes that involve people, processes, and technology. The certification requires an independent auditor to assess the company's security controls and to ensure that the risks are being appropriately mitigated.

ISO works to promote standards that align with the business practices of over 160 countries. This helps to resolve any disagreement between businesses in the same industry.

#### **GDPR (General Data Protection Regulation)**

The EU's GDPR is one of the most comprehensive government-imposed data privacy frameworks implemented to date. It went into effect in May 2018 and is meant to protect the data privacy of EU citizens. However, this regulation doesn't just apply to European companies; it's for anyone who processes the data of European citizens.

For compliance, we must flow company roles and regulations. comply with their policy and procedures. we ensure that all IT-related issues within the organization comply with the law, as

well as other relevant issues that can help organizations abide by the set laws and conditions within the company.

### **Assessment of the risk:**

The CIA standard of an organization can be violated by a number of dangers. The business or organization should routinely evaluate the risk based on the ISO 27001 security framework.

Three categories should be used to categorize risks:

1. High
2. Medium
3. Low.

Based on the criticality of their particular business, each company or organization should establish the framework for risk evaluation.

### **Identification of mitigation control:**

Risk cannot be totally eliminated. However, it can be lessened. An organization must identify the risk mitigation control after considering the hazards.

### **3.8.3 Audit Report**

I must create an audit report after studying every document that contains the following headings:

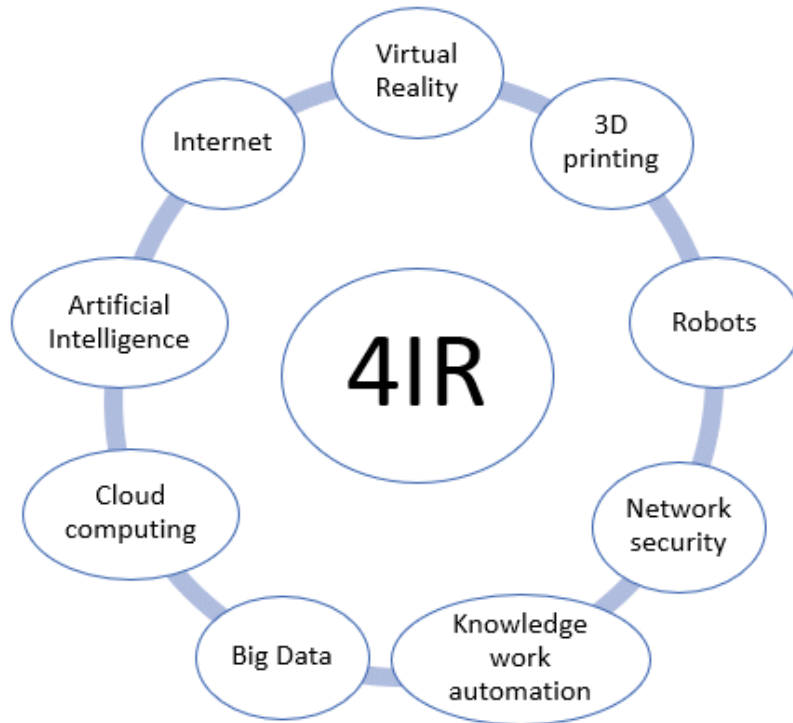
1. The first observation heading.
2. Risk Assessment and Potential Risk.
3. Recommendation.
4. The Management Reaction.

### 3.9 IT Audit Future

#### CHARACTERISTICS OF 4IR



#### COMPONENTS OF 4IR



**Figure No 03: 4IR**

We are advancing toward the fourth industrial revolution day by day. Internet of Things (IoT), robotics, virtual reality (VR), and ai are all part of the fourth industrial revolution (AI). Automation and IT are the fourth IR's pillars. Therefore, there is a significant chance for auditor to audit those systems to review those autonomous and IT infrastructures to determine whether they are properly working or not, or to uncover vulnerabilities as well as risk.

While some people (typically those in charge of monitoring, controlling, and providing assurance that it is utilized safely, professionally, and in a way that complies with regulations) find the prospects that technology presents to be endlessly thrilling, others see it as menacing and incomprehensible. Since it has been difficult for internal audit teams to locate IT audit specialists, there is now additional pressure on them to use technology more wisely in their audits. Their worries are increased by the quick development of new technologies, such as blockchain and artificial intelligence.

#### **4.Benefits of the Internship**

The ability to learn how to conduct an annual audit as an external auditor was the biggest benefit I gained during my internship. I may also observe the culture and policies of the CA firm and adjust myself accordingly. I was given the chance to write a policy about Walton. I have faced difficulties in my new position since I have had to mentor newcomers. However, I was able to properly address all of these issues and goals while completing the task at hand. I gain knowledge on how to interact with clients in a professional manner. How to communicate with senior staff members like a bank's CTO or depth ardent head and obtain relevant information in the form of documents. This new knowledge will be useful to me in the future because professionalism is a key component of IT audits. My communication and interpersonal skills in the workplace were also improved by the internship program because I frequently interacted with clients and senior colleagues. In addition to all of these things, I have about four months of IT audit experience, which has given me a thorough understanding of the current business and employment chances in the corporate and international industry.

## **5. 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>

## Turnitin Originality Report

Processed on: 14-Dec-2022 15:33 +06  
ID: 1980997047  
Word Count: 6974  
Submitted: 1

183-35-2588 By Maruf Hasan Rudro

Similarity Index	Similarity by Source
20%	Internet Sources: 17% Publications: 4% Student Papers: 16%

4% match (Internet from 08-Mar-2022)

<https://www.zluri.com/blog/how-to-do-it-compliance-audit/>

3% match (Internet from 14-Dec-2021)

[http://reg.upm.edu.my/eISO/portal/standard%20ISO/MS%20ISO%20IEC%2027001\\_2013.pdf](http://reg.upm.edu.my/eISO/portal/standard%20ISO/MS%20ISO%20IEC%2027001_2013.pdf)

2% match (Internet from 07-Apr-2021)

<http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/5414/192-25-763%20%286%25%29.pdf?isAllowed=y&sequence=1>

2% match (student papers from 09-Apr-2018)

Class: April 2018 Project Report

Assignment: Student Project

Paper ID: [943600277](#)

1% match (Internet from 21-Nov-2022)

<http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/7382/171-35-2075%20%2820%25%29.pdf?isAllowed=y&sequence=1>

1% match (Internet from 26-Oct-2021)

<https://www.slideshare.net/AdityaJain335/it-audit-internship-report-123370119>

1% match (student papers from 26-Nov-2022)

[Submitted to Westford School of Management on 2022-11-26](#)

1% match (student papers from 21-Sep-2022)

[Submitted to Republic of the Maldives on 2022-09-21](#)

1% match (Internet from 27-Jan-2015)

<http://www.mvaezi.ir/files/ISO-IEC%2027001-2013.pdf>

1% match (Internet from 18-Apr-2020)

<https://www.romanosecurityconsulting.com/security-audit>

< 1% match (Internet from 26-Oct-2022)

<http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/20.500.11948/1118/FINAL%20AV3839.pdf?isAllowed=y&sequence=1>

< 1% match (Internet from 20-Nov-2022)

[http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/4325/P14518%20%2824\\_%29.pdf?isAllowed=y&sequence=1](http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/4325/P14518%20%2824_%29.pdf?isAllowed=y&sequence=1)

< 1% match (Internet from 01-Oct-2021)

<http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/5275/172-15-9858%20%2826%25%29.pdf?isAllowed=y&sequence=1>

< 1% match (Internet from 20-Nov-2022)

[http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/5693/171-35-1870%20%2824\\_%29.pdf?isAllowed=y&sequence=1](http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/5693/171-35-1870%20%2824_%29.pdf?isAllowed=y&sequence=1)

<p>&lt; 1% match (Internet from 20-Nov-2022)  <a href="http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/4031/P14373%20%2827%29.pdf?isAllowed=y&amp;sequence=1">http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/4031/P14373%20%2827%29.pdf?isAllowed=y&amp;sequence=1</a></p>
<p>&lt; 1% match (student papers from 07-Apr-2018)  Class: Article 2018  Assignment: Journal Article  Paper ID: <a href="#">942534661</a></p>
<p>&lt; 1% match (Internet from 29-Aug-2020)  <a href="http://docplayer.net/50136436-No-iso-certified-companies-among-largest-data-breaches.html">http://docplayer.net/50136436-No-iso-certified-companies-among-largest-data-breaches.html</a></p>
<p>&lt; 1% match (student papers from 26-Sep-2022)  <a href="#">Submitted to Tulane University on 2022-09-26</a></p>
<p>&lt; 1% match (student papers from 07-Sep-2022)  <a href="#">Submitted to Study Group Australia on 2022-09-07</a></p>
<p>&lt; 1% match (Internet from 03-Jul-2021)  <a href="https://www.coursehero.com/file/76784883/P12129-19-pdf/">https://www.coursehero.com/file/76784883/P12129-19-pdf/</a></p>
<p>&lt; 1% match (student papers from 25-Nov-2022)  <a href="#">Submitted to University of Hertfordshire on 2022-11-25</a></p>
<p>&lt; 1% match (student papers from 03-Oct-2022)  <a href="#">Submitted to University of Salford on 2022-10-03</a></p>
<p>&lt; 1% match (student papers from 06-Aug-2021)  <a href="#">Submitted to Liverpool John Moores University on 2021-08-06</a></p>
<p>&lt; 1% match (student papers from 10-Mar-2022)  <a href="#">Submitted to University of Derby on 2022-03-10</a></p>
<p>&lt; 1% match (Internet from 17-Jan-2022)  <a href="http://lib.buet.ac.bd:8080/xmlui/bitstream/handle/123456789/3505/Full%20Thesis.pdf?isAllowed=y&amp;sequence=1">http://lib.buet.ac.bd:8080/xmlui/bitstream/handle/123456789/3505/Full%20Thesis.pdf?isAllowed=y&amp;sequence=1</a></p>
<p>&lt; 1% match (Internet from 24-Sep-2022)  <a href="https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/forums-showcase-common-challenges-facing-it-audit-directors">https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2017/forums-showcase-common-challenges-facing-it-audit-directors</a></p>
<p>&lt; 1% match (student papers from 20-Oct-2022)  <a href="#">Submitted to The University of the South Pacific on 2022-10-20</a></p>
<p>&lt; 1% match (Internet from 11-Nov-2020)  <a href="https://ndre.sreda.gov.bd/index.php?ag=&amp;di=&amp;fs=&amp;i=2&amp;id=01&amp;ob=1&amp;ps=1&amp;s=&amp;sg=">https://ndre.sreda.gov.bd/index.php?ag=&amp;di=&amp;fs=&amp;i=2&amp;id=01&amp;ob=1&amp;ps=1&amp;s=&amp;sg=</a></p>
<p>&lt; 1% match (Internet from 12-Dec-2022)  <a href="https://www.intosaicommunity.net/wgita/wp-content/uploads/2020/06/IT-Audit-Report-on-the-Efficiency-and-Effectiveness-in-Public-Service-Delivery-through-G2C-Platform.pdf">https://www.intosaicommunity.net/wgita/wp-content/uploads/2020/06/IT-Audit-Report-on-the-Efficiency-and-Effectiveness-in-Public-Service-Delivery-through-G2C-Platform.pdf</a></p>
<p>&lt; 1% match (student papers from 30-May-2021)  <a href="#">Submitted to University of Mauritius on 2021-05-30</a></p>
<p>&lt; 1% match (Internet from 10-Sep-2018)  <a href="http://smart.tdcc.com.tw/pdf/others/a260.pdf">http://smart.tdcc.com.tw/pdf/others/a260.pdf</a></p>



