Final Internship report

on

‘Information Systems Auditor’

Supervised By
Fatama Binta Rafiq
Senior Lecturer
Department of Software Engineering
Daffodil International University

Submitted By
Md. Naziur Rahaman Monzu
ID: 181-35-2384
Department of Software Engineering
Daffodil International University

This intern report has been submitted to fulfill the requirement for the degree of Bachelor of Science in Software Engineering Major in Cyber Security

APPROVAL

This Internship titled on "**Information Systems Auditor**", submitted by **Md. Naziur Rahaman Monzu (ID: 181-35-2384)** 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

Md. Shohel Arman
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 am Md. Naziur Rahaman Monzu hereby declares that the internship report entitled as ‘Information Systems Auditor Internship’ is prepared by me after completion of about six months work at ACNABIN Chartered Accountants. Under the supervision of Fatama Binta Rafiq, Senior Lecturer, Department of Software Engineering, Daffodil International University I have done my internship.

This is a unique report that isn't submitted anywhere for academic purposes. The inputs & information mentioned here are also collected & organized by me. I am solely responsible for any misrepresentation of information in this report.

Finally, this report is submitted to the Faculty of Science and Information Technology, Department of Software Engineering, Daffodil International University, as a part to meet the requirements of Bachelor of Science in Software Engineering Major in Cyber Security degree.

Submitted By

……
Md. Naziur Rahaman Monzu
ID: 181-35-2384
Department of Software Engineering
Daffodil International University

Certified By

……...
Fatama Binta Rafiq
Senior Lecturer
Department of Software Engineering
Daffodil International University

Acknowledgement

I am very much grateful to Almighty Allah (SWT) for allowing me to complete my Bachelor study. I'm thankful to my parents for being there whenever I need. They always try to make me believe that I can achieve something.

I'm very much thankful & indebted to my supervisor, **Fatama Binta Rafiq** for his enormous support throughout my internship period. My respect & gratitude for him & always will be

I convey my sincere gratitude to Director (IT) **A.N.M. Shakawath Hossain** for his guidance, knowledge sharing & more importantly his motivation to work hard to learn.

Finally, I would like to thank **Dr. Imran Mahmud**, Associate Professor & Head of the Department of Software Engineering, Daffodil International University for his motivation to become a skilled person. I also want to thank all my teachers who supporting us throughout the Bachelor Program

Table Of Contents

Table of Figure

Chapter 1: Introduction

1.1 About Myself

My name is Md. Naziur Rahaman Monzu, bearing Student ID is 181-35-2384. Currently, I am working as an Analyst, Information Security Research & Development at Right Time Limited from 01/09/2022. As a part of my Bachelor of Science in Software Engineering Major in Cyber Security from Daffodil International University, I have done my internship as an Information Systems Auditor from ACNABIN Chartered Accountants under IT Audit Division which was started from 20/04/2022. I have always had a dream to work in the Cyber Security field and this internship has offered me the chance to work in this vast field of Cyber Security. This report is based on my internship experience at ACNABIN.

1.2 Background

Daffodil International University opens the opportunity to work in the Cyber Security field by offering a Major in Cyber Security degree. As a student of Cyber Security this internship was a part of my bachelor Program. I passed my Certified Ethical Hacker certification during my final year of studies. I have learnt penetration testing, vulnerability assessment, digital forensics and information system audit during my bachelor program. This internship helps me to enrich my theoretical knowledge with practical experience and also can learn new things.

1.3 Motivation

My main motivation to do this internship is to gain industry experience from the experts of this field. It is impossible to cover everything within the scope of an academic curriculum and gain industry experience. Another reason I decided to do an internship is that it helps me face real-world challenges throughout every project.

1.4 Objectives

The main objective of my internship was to enrich my theoretical knowledge with industry experience. My goal is to understand the fundamental concepts and components of an IT audit. From my internship tasks, I came to know many technical knowledge and the opportunities for technical ability. For improving communication ability, Leadership skill, Teamwork internship is a way to learn. Besides some other objectives are:

- To know more about ISO/IEC 27001 standards.
- To know about gap analysis process
- To know how to validate this Gaps
- To know about different type of Audit framework on Information Security
- To know about Remediation process according to Framework
- To know about proper report writing way

1.5 Scope

Day by day security becomes the most important thing for any organization. To protect data, they need to check their system flaws. During my internship period I worked with the Bank, Non-Banking Financial Organization, Telecommunication, Stock Exchange, Multinational & limited company.

Chapter 2: Organization Overview

2.1 About Company

2.1.1 About ACNABIN Chartered Accountants

ACNABIN is one of the popular accounting firms, representing Baker Tilly International as an independent network member firm in Bangladesh providing IT assurance, tax, business consulting, IT Audit, Information System Audit, Information Security Audit, ISO/IEC 27001 certification consultancy services ensuring high quality. From starting its journey way back in 1985, the firm has been one of the most efficient and trusted firms to the business communities and related stakeholders.

At ACNABIN, we measure success by reference to value created as desired by our clients and stakeholders. To serve our valued clients, about 500 professionals of varied experience and expertise have been relentlessly working every day across the markets. To understand not just what our customers want, but what their business needs; to meet not just immediate requirements but provide long-term solutions; to being not just reactive to client needs but being proactive to solve their future challenges and Risk issues. Our firm culture is conducted by the Baker Tilly Internal core values:

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

2.1.2 Vision and Mission:

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

We provide the CIA based service. We maintain the strictest principles of client confidentiality. The sensitive and competitive nature of proprietary information and its maintenance of it. We have constructed our success on such principles. We do our utmost to earn and keep clients trust and provide Services.

The name ACNABIN mainly came from 7 partners of the firm:

A	ABM Azizuddin
C	Anwaruddin Chowdhury
N	ASM Nayeem
A	HM Abul Kalam Azad
B	ATMA Bari
I	Iftekhar Hossain
N	Mohammad Nurun Nabi

2.1.3 Location

Corporate Office:
BDBL Bhaban (Level-13 & 15)
12 Kawran Bazar Commercial Area
Dhaka-1215, Bangladesh

Branch Office:
Jahan Building No. 7 (1st Floor, North Side)
59 Agrabad Commercial Area
Chattogram-4100, Bangladesh

2.2 Company Organogram

Figure 1: Organogram

2.3 Operation Process

Like any other major chartered firm in the industry, ACNABIN chartered accountants practice good information systems. Information systems are utilized by the business and firm for data collection, storage, analysis, and dissemination to clients and stakeholders. For the time being, ACNABIN uses ERP-based information systems to store, gather, and process data for their clients, employees, and stakeholders. ACNABIN tracks the daily work activities of their employees using ERP software. Each employee at ACNABIN has a login for the ERP system via which they can apply to enter a job ticket for their upcoming audit customer. The ACNABIN workers can enter timesheet entries for their daily attendance with the aid of this program. Firms use ERP software to maintain employee activity and give the conveyance properly.

ACNABIN also has a database where they keep their client information and store it appropriately. Only the firm's partners have access to the database. Because client financial information is highly confidential, that's why data from ACNABIN's database is accessible only to partners. Normally, every accounting firm is required to keep audited information in its database for at least 5 years (ICAB, 2022). ACNABIN is also required to follow the ICAB's rules.

2.4 SWOT Analysis

Figure 2: SWOT Analysis

2.5 Recommendation

During my internship period I worked from the client office. Besides I can recommend something where ACNABIN can develop to grow their operation.

- ACNABIN can develop a job assigned software so that it levels the pressure among the employees.
- ACNABIN can develop a good salary policy.
- Organize more training to develop employee's skills

Chapter 3: Internship Period

3.1 Introduction

Audit & Assurance service is one of the key services of every Chartered Accountant firm in Bangladesh. Like every other country in the world Bangladeshi companies need to do audits every year. In Bangladesh, many CA firms such as ACNABIN play a key role in providing audit services in business sectors.

As a junior auditor who has worked for ACNABIN for the last five months, I have witnessed some significant observations regarding audit and assurance quality, which is a key service provided by ACNABIN chartered accountants. One of the key findings from those observations is Bangladesh's lack of quality audit assurance services. The problem arises as a result of a scarcity of accounting professionals in Bangladesh.

3.2 Overview

During my internship period I worked with the Bank, Non-Banking Financial Organization, Telecommunication, Stock Exchange, Multinational & limited company.

3.2.1 Types of IT Audit

3.2.1.1 Internal Audit

Internal audit refers to a self-supported service that evaluates an organization's internal controls, corporate practices, processes, and styles. An internal audit assists in icing compliance with the colorful laws that apply to a company. An organization can prepare its accounts and records in agreement with the applicable legal conditions and reporting.

An organization's operational standards and effectiveness are examined during an internal audit. Operations like paying bills, accepting deliveries, and placing orders may be governed by rules within an organization. Additionally, an internal audit aids in determining whether employees adhere to internal operational standards.

An internal audit aids in the identification of issues or inefficiencies and the implementation of necessary corrections. Any employee fraud, including embezzlement of funds, can be discovered by internal audits. The audit can also determine whether a particular vendor is given preference over other low-cost suppliers or whether there are intentional cost overruns.

3.2.1.2 External Audit:

An external audit is a process where any organization hires an authorized firm for their in-depth audit. During the process of an external audit, an auditor will review a company's information systems. Purpose of the audit to find the accuracy and completeness of their information related systems. To get the best result, auditors follow some security standards or framework.

A company typically conducts not more than one external audit per year. External IT security audits are a great way to totally review where your business presently stands with its data, network and device security to find out if there are any implicit security issues and how to resolve them before any dangerous security breaches occur.

Risks to your IT security include hand practices, natural disasters and vicious attacks similar to malware, viruses and phishing attacks. Ensuring you have flexible monitoring

and defensive measures in place across your emails, data lines, network monitoring, data backups and software updates should ensure your business stays secure and online.

3.3 Major Clients

Throughout my internship period I worked with numerous companies for external & internal audit purposes.

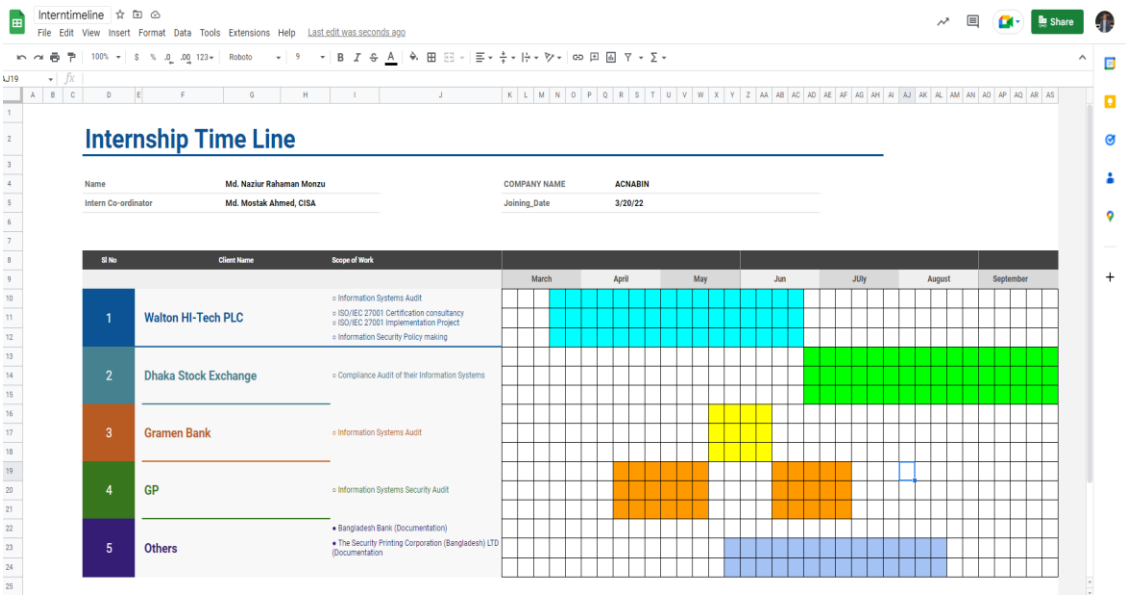


Figure 3: Gantt Chart of timeline

3.3.1 Internal Audit Clients

- Walton Hi -Tech Industries PLC

  I worked with Walton Hi -Tech Industries PLC on Four projects. This are:

  - Information Systems Audit
  - ISO/IEC 27001 Certification consultancy
  - Information Security Policy making
  - ISO/IEC 27001 Implementation Project

3.3.2 External Audit Clients

- Grameen Bank
    - Information Systems Audit
- Grameen Phone
    - Information Systems Security Audit
- Dhaka Stock Exchange
    - Compliance Audit of their Information Systems
- Bangladesh Bank
- The Security Printing Corporation (Bangladesh) LTD

Chapter 4: Information Systems Audit

4.1 Information Systems Audit (ISO/IEC 27001)

ISO/IEC 27001 is a widely known and acknowledged standard for the management of information security systems (ISMS). ISO/IEC 27001 is one the most widely used standards for information security. ACNABIN provides ISO/IEC 27001 consultancy to achieve ISO/IEC 27001 certification.

4.2 Audit Process

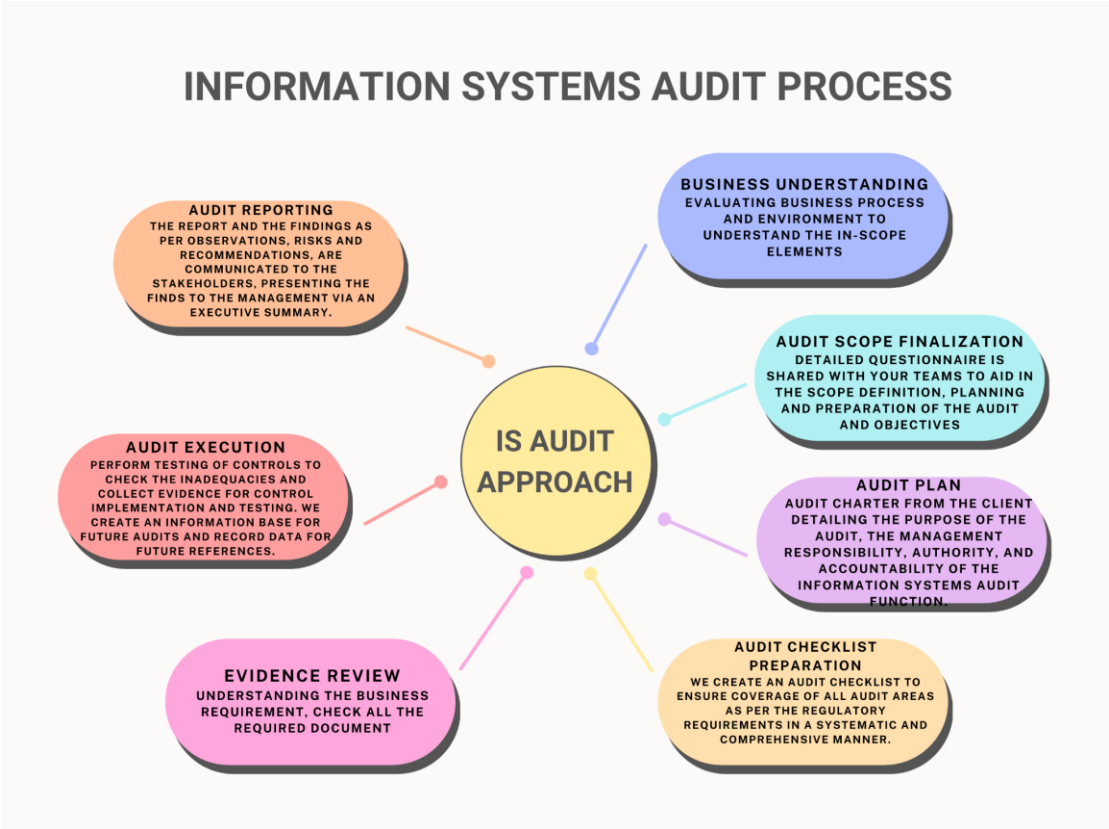


Figure 4: Audit Process

4.2 Audit Checklist

Every Audit firm follows their own audit checklist. During my internship I followed a checklist which was developed by ACNABIN's IT Audit Head A N M Shakhawath Hossain. The checklist as follows:

4.2.1 General Information

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

4.2.2 Details Information

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

Area	Status	Comments
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		

Area	Status	Comments
Backup Medium		
Backup Labeling		
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		

Area	Status	Comments
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		

Area	Status	Comments
Audit Trail Log Review		
Medium of Log preserve		
Location of the Log		
Security		
Data Retention Policy		
Data Retention Period		
Secure Disposal Policy		
Antivirus / 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		

4.2.2.1 Logical Access Path

It involves using a digital procedure to access an application or system. akin to how we sign into computers. Clients offer SS but with constraints and secrecy.

4.2.2.2 User Management

This will comprise a list of active and revoked users, together with information about their jobs, duties, and access privileges. Like:

- 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)

4.2.2.3 Password Management

It covers setups and password complexity. Included in this are all the criteria, such as the minimum number of characters required for a valid password, the character types, the duration of passwords, password lock out. Like

- Password Policy
- Minimum Length of Password
- Password Complexity
- Password Expiry Period

- Remember Password
- Minimum Days
- No of wrong password input
- Password Lock Period

4.2.2.4 Backup & Restore

In backup & restore part we collect data about system data backup & restore. There are many checkpoints to check. Like:

- Backup Policy
- Recovery Point Objective (RPO)
- Recovery Time Objective (RTO)
- Backup Frequency
- Backup Log
- Backup Medium
- Backup Labeling
- Backup Store
- Frequency of Backup Restoring
- Backup Restore Log

4.2.2.5 BIA / BCP / DRP

Table of Content of BIA / DRP document

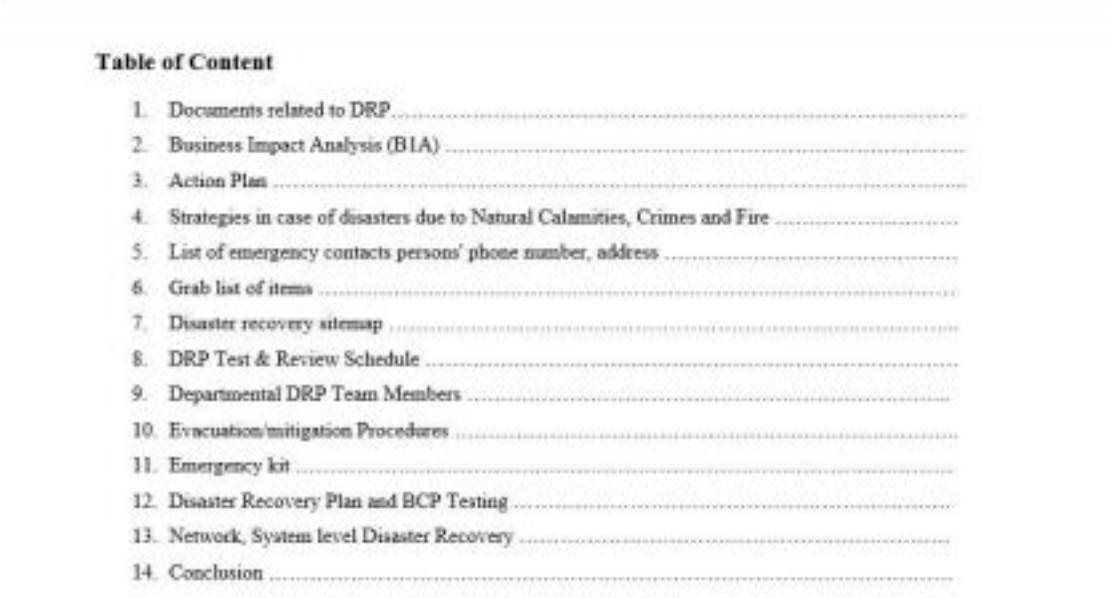


Table of Content

Figure 5: Table of contents of DRP & BIA

4.2.3 Risk Register

In Risk Related topics we maintained some criteria such as

- Risk ID
- Risk Category
- Risk Score
- Type of Risk

4.3 Controls for ISO 27001

There are 114 controls in ISO/IEC 27001 Information Security Management Systems (ISMS). These 114 controls are grouped into 14 control categories. This are:

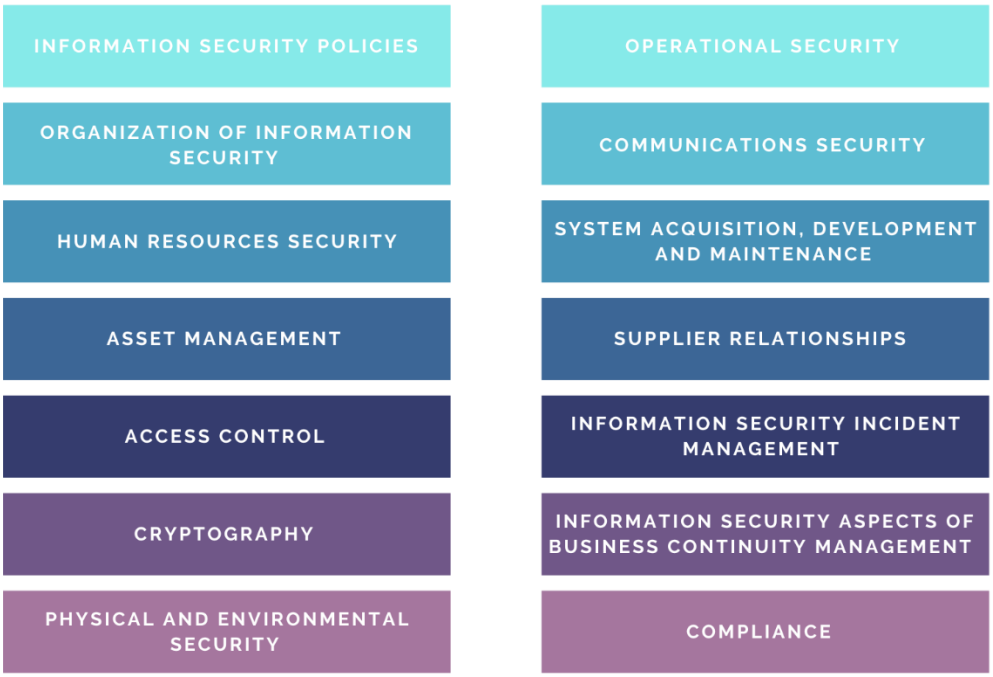


Figure 6: Control Groups of ISO 27001

4.4 Audit Report

4.4.1 Observation Sample

4.4.1 Observation Sample 1

User Review Report Not Found

Observation

During our audit we observed that XXX does not perform user review for its EBS users.

Risk

- XXX may not ensure that users those are not active/not using their account are inactivated/removed from EBS system.
- Unwanted user account may have been used by potential threat factor which may lead to business loss, financial loss and reputation loss.
- Accountability may not be established.

Recommendation

Management should ensure that review of user account is performed in regular basis.

IT Dept. Response

We have an automatic schedule for review user list and inactive those users which are not system login minimum 30 days. If you have any standard user review structure, please share with us. We will check.

Management Response

4.4.1 Observation Sample 2

Non-compliance of user creation policy

Observation

As per step-3, XXX ’s EBS User Access guideline, user accounts will be made inactivated/closed for those who have not accessed the system in last 30 days.

It has been observed that some user not accessed the system/left the organization, however, their accounts have not been made inactivated/closed yet.

Risk

- Non-compliance with XXX ’s EBS User Access guideline.
- Accountability may not be established.
- XXX may face business loss, financial loss and reputation loss.

Recommendation

Management should ensure that ‘XXX ’s EBS User Access guideline’ is compiled and followed accordingly.

IT Dept. Response

User inactive process is fully automated. So, there are no possibility to missing any specific user except manual access. Please share with us you’re finding we will give u feedback.

Management Response

4.4.1 Observation Sample 3

Service Level Agreement (SLA) with Lexicon

Observation

We observed that XXX had a Service Level Agreement with Lexicon. Which has expired in 31st December 2020. XXX informed us they have continued with Lexicon until 31st December 2021; however, they could not provide us any relevant document. From January 2022, XXX is taking service from Millennium I.T. E.S.P (PVT) LTD. on the basis of purchase order. Final agreement has not taken place yet.

Risk

XXX should ensure that up to date service level agreement is maintained

Recommendation

XXX should ensure that up to date service level agreement is maintained

IT Dept. Response

False observation. Our SLA with Lexicon has expired in 31st December 2020. We have taken management approval to continue until new one. And provide you several time.

Purchase order with Millennium I.T. E.S.P (PVT) LTD has approved and complete SLA is in progress, hope it will do very soon.

Management Response

4.4.2 Final Audit Report Sample 1

Fact: 01

Information System Audit

Fact

As per section 2.4.5 of Bangladesh Bank Guideline on ICT Security for Banks and Non-Bank Financial Institutions, May 2015, Version 3.0 states that, “Internal Information System audit shall be done periodically at least once a year. The report must be preserved for regulators as and when required. Bank or NBFI shall also ensure that audit issues are properly tracked and, in particular, completely recorded, adequately followed up and satisfactorily rectified.”

As per section 2.4.6 of Bangladesh Bank Guideline on ICT Security for Banks and Non-Bank Financial Institutions, May 2015, Version 3.0 states that, “The bank/branch or NBFI shall take appropriate measures to address the recommendations made in the last Audit Report (external/internal). This must be documented and kept along with the Audit Report mentioned in 2.4.5.”

As per section 2.5.2 of Bangladesh Bank Guideline on ICT Security for Banks and Non-Bank Financial Institutions, May 2015, Version 3.0 states that, “The audit report shall be preserved for regulators as and when required.”

As per section 2.4.1.1 of XXX Bank Limited Guideline on ICT Security Policy, 2021, Version 2.0 states that, “Internal Information System Audit shall be carried out only by Internal Audit or relevant division (other than Information Technology Division)”

As per section 2.4.2.1 of XXX Bank Limited Guideline on ICT Security Policy, 2021, Version 2.0 states that, “External Auditor(s) shall be engaged for information system auditing in line with the regular financial audit.”

As per section 2.4.2.2 of XXX Bank Limited Guideline on ICT Security Policy, 2021, Version 2.0 states that, “The Audit report shall be preserved for regulators as and when required.”

During our audit period we found:

- XXX Bank Limited didn’t perform Internal Information System (IS) Audit by Internal Audit.
- XXX Bank Limited didn’t any third party or External Auditor to perform IS Audit.
- From Bangladesh Bank’s audit report, November 30, 2021, we came to know there is a lot of findings related to the IT operation which are not solved yet and we also did not get any satisfactory update on those issues.

Implication/Risk

Non-compliance with section 2.4.5 of Bangladesh Bank Guideline on ICT Security Policy for Banks and Non-Bank Financial Institutions, May 2015, Version 3.0

Non-compliance with section 2.4.6 of Bangladesh Bank Guideline on ICT Security Policy for Banks and Non-Bank Financial Institutions, May 2015, Version 3.0

Non-compliance with section 2.5.2 of Bangladesh Bank Guideline on ICT Security Policy for Banks and Non-Bank Financial Institutions, May 2015, Version 3.0

Non-compliance with section 2.4.1.1 of XXX Bank Limited Guideline on ICT Security Policy, 2021, Version 2.0

Non-compliance with section 2.4.2.1 of XXX Bank Limited Guideline on ICT Security Policy, 2021, Version 2.0

Non-compliance with section 2.4.2.2 of XXX Bank Limited Guideline on ICT Security Policy, 2021, Version 2.0

Recommendation

- XXX Bank Limited should perform Internal Information System (IS) audit at least once a year.
- XXX Bank Limited should preserve Internal Information System (IS) audit Report for regulators as and when required.
- XXX Bank Limited should ensure that audit issues are properly tracked and, in particular, completely recorded, adequately followed up, and satisfactorily rectified.
- XXX Bank Limited should carried out only by Internal Audit or relevant division.
- XXX Bank Limited should take necessary steps to resolve audit findings as soon as possible.

Management Response

Fact: 02

Risk Assessment

Fact

As per section 3.2.5 of Bangladesh Bank Guideline on ICT Security for Banks and Non-Bank Financial Institutions, May 2015, Version 3.0 states that, “ICT security department/unit/cell shall conduct periodic ICT risk assessment of ICT related assets (process and system) and provide recommendation to risk owners for mitigation.”

As per section 3.1.6 of Bangladesh Bank Guideline on ICT Security for Banks and Non-Bank Financial Institutions, May 2015, Version 3.0 states that, “The Bank or NBFI shall define the risk accountability applies to those who owned the required resources and have the authority to approve the execution and/or accept the outcome of an activity within specific ICT Risk processes. Ownership of risk stays with owner or custodian whoever is in better position to mitigate the identified risk for that specific ICT asset.”

As per section 8.1.1 of Bangladesh Bank Guideline on ICT Security for Banks and Non-Bank Financial Institutions, May 2015, Version 3.0 states that, “In drawing up a project management framework, the Bank or NBFI shall ensure that tasks and processes for developing or acquiring new systems include project risk assessment and classification, critical success factors for each project phase, definition of project milestones and deliverables. The Bank or NBFI shall clearly define in the project management framework, the roles and responsibilities of staff involved in the project.”

As per section 3.2.2 of XXX Bank Limited Guideline on ICT Security Policy, 2021, Version 2.0 states that, “The Bank shall define and identify and Risk Factors those influence the frequency and / or business impact of risk Scenarios.”

As per section 3.2.3 of XXX Bank Limited Guideline on ICT Security Policy, 2021, Version 2.0 states that, “ICT Security Cell shall conduct an ICT risk assessment of ICT related assets (process, and system) every quarter and provide a recommendation to risk owners for migration.”

During our audit period we found that:

- XXX Bank Limited didn’t conduct the ICT risk assessment properly.
- The Risk Register provided by XXX Bank Limited does not contain all the information required by the standards like threat, likelihood, owner etc.
- There is no methodology to identify Risk Level.

Implication/Risk

Non-compliance with Bangladesh Bank Guideline on ICT Security for Banks and Non-Bank Financial Institutions, May 2015, Version 3.0, Section 3.2.5

Non-compliance with Bangladesh Bank Guideline on ICT Security for Banks and Non-Bank Financial Institutions, May 2015, Version 3.0, Section 8.1.1

Non-compliance with XXX Bank Limited Guideline on ICT Security Policy, 2021, Version 2.0, Section 3.2.2

Non-compliance with XXX Bank Limited Guideline on ICT Security Policy, 2021, Version 2.0, Section 3.2.3

Without assessing the risk bank may not allow to identify the risk of the IS operation and may not be able to implement efficient and effective controls to mitigate those risks which may lead to financial loss, business loss as well as reputational loss.

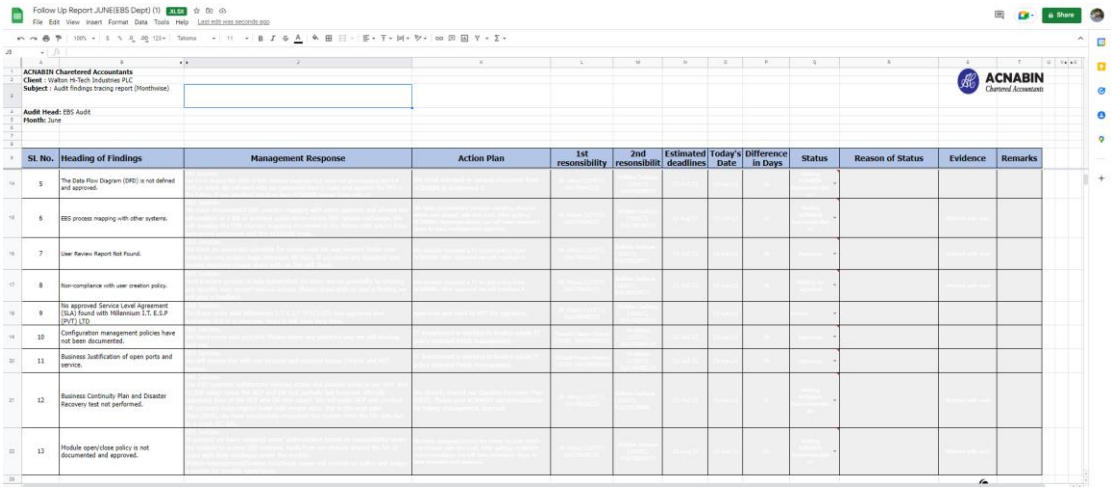
Recommendation

- XXX Bank Limited should conduct periodic ICT risk assessment of ICT related assets.
- XXX Bank Limited should define risk owners and mitigate controls.
- XXX Bank Limited should define and identify the Risk Factors, the frequency and / or business impact of risk Scenarios.

Management Response

4.4.2 Final Audit Report Sample

It contains all of the final observations and recommendations for what companies are doing and how they are eligible to do business in foreign countries.



ACNABIN Charetered Accountants
Client : Walton Hi-Tech Industries PLC
Subject : Audit findings tracing report (Monthwise)
Audit Head: EBS Audit
Month: June

Sl. No.	Heading of Findings	Management Response	Action Plan	1st resonsibility	2nd resonsibilit	Estimated deadlines	Today's Date	Difference in Days	Status	Reason of Status	Evidence	Remarks
5	The Data Flow Diagram (DFD) is not defined and approved.											
6	EBS process mapping with other systems.											
7	User Review Report Not Found.											
8	Non-compliance with user creation policy.											
9	No approved Service Level Agreement (SLA) found with Millennium I.T. E.S.P (PVT) LTD											
10	Configuration management policies have not been documented.											
11	Business Justification of open ports and service.											
12	Business Continuity Plan and Disaster Recovery test not performed.											
13	Module open/close policy is not documented and approved.											

Figure 7: Audit Report Demo

4.5 Prove of Work

Here are some sample of email communication between Me (ACNABIN) & clients

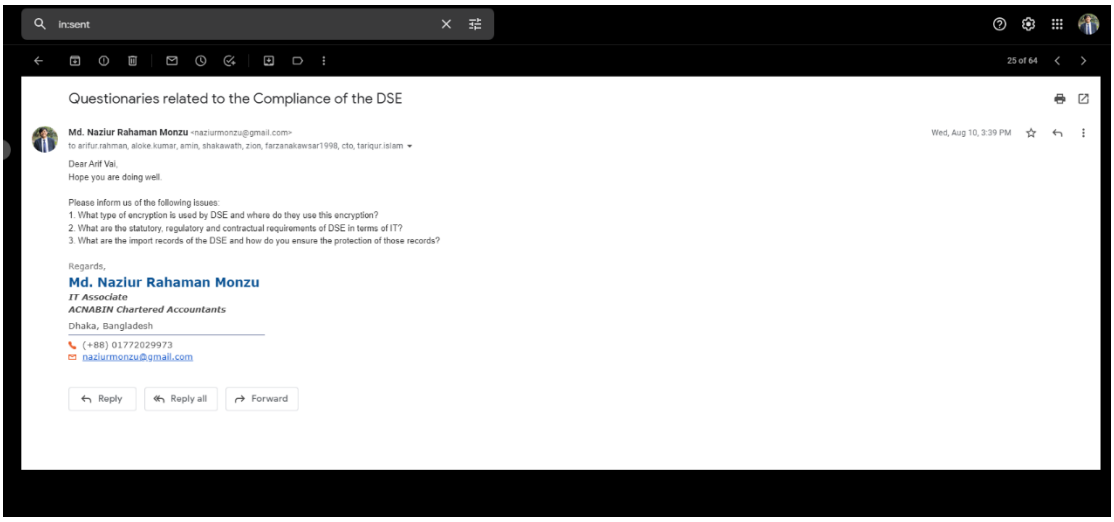


Figure 8: Prove of work

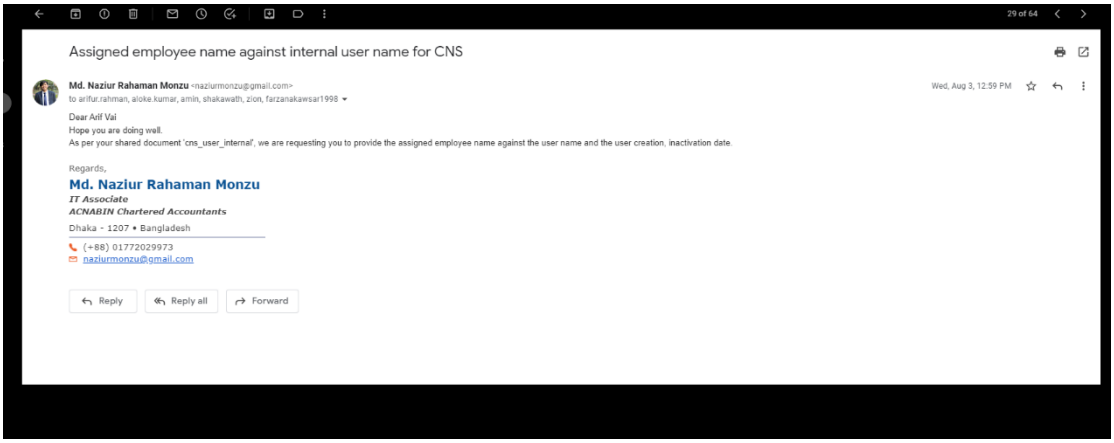


Figure 9: Prove of work

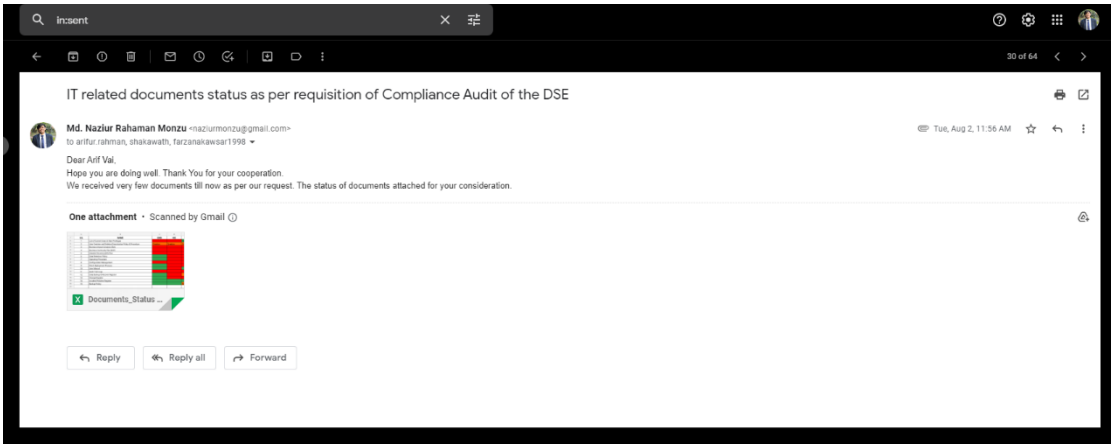


Figure 10: Prove of work

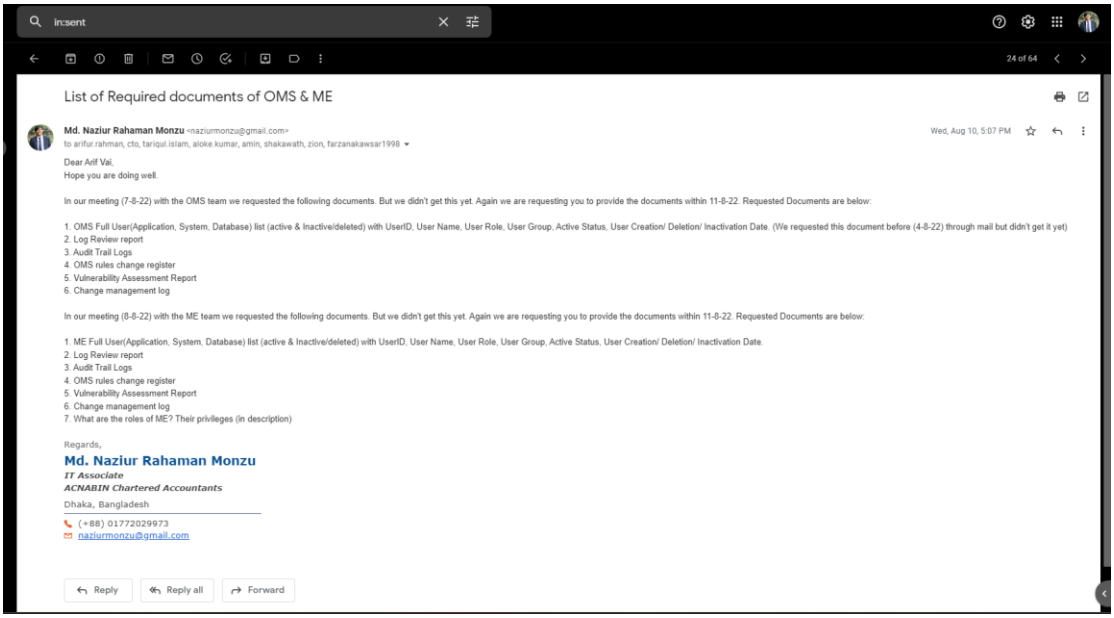


Figure 11: Prove of work

4.6 Benefits of Information Systems Audit (ISO/IEC 27001)

ISO/IEC 27001 is an international standard & most followed for Information Security Management. Here are some benefits of ISO/IEC 27001

- Increasing reliability on certified organization's systems
- Increasing reliability on certified organization's information
- Increasing stakeholders' confidence on organization
- Increase confidentiality, integrity, availability of data
- Management processes have really been improved
- Decreasing risk & threat for data
- Overall improvement of business

Chapter 5: Compliance Audit

5.1 Introduction

How IT has changed over the years has had a positive impact on the overall compliance-related issues of an enterprise. IT compliance-related issues are proving to be phenomenal and of great importance, as it has been established that they help organizations develop specific protocols on compliance-related issues set by governments and other relevant bodies. can be viewed. As a result, it can be seen that IT compliance auditors are in high demand as they include a substantial background in compliance and other related features that can act as a safeguard for the business. against possible financial losses. It can be seen that the IT compliance auditor must ensure that all IT related matters in the organization are in compliance with the law, along with other related matters that can help the organization meet the laws and regulations. conditions are set in the company.

5.2 Some Compliance Audit Framework

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

  PCI-DSS compliance is a must for those who use Mastercard, American Express, JCB, VISA, discover bank card & all companies that accept, process, store, or transmit credit card data

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

  SOC 2 is a compliance audit defined by and a standard accepted by technology companies today. Its main purpose is to be able to store customer data and apply it to service providers using the cloud. These companies are required to comply with SOC 2 due to their strict policies and procedures.

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

  The EU GDPR is one of the most comprehensive government mandated data privacy frameworks implemented to date. It came into effect in May 2018 and aims to protect the privacy of EU citizens' data. However, this regulation does not only apply to European companies; it is open to anyone who processes the data of European citizens

Chapter 6: IT Audit as a career

Today is the world of technology. Besides development of the technology the risk of compromission of an organization is getting higher also. So, every company needs to do an IT Audit at least once a year.

For the Bank & Non-Banking Financial Institution it is mandatory to do an Information Security Audit once a Year by Bangladesh Bank. Bangladesh Bank also makes PCI-DSS certification compulsory for all companies that accept, process, store, or transmit credit card data.

ISO/IEC 27001 certification is also a mandatory requirement for those who have worked with user data by the ICT Ministry.

So, we can see that there are so many job fields open for security professionals. In Bangladesh we have lack of skilled people in the Security domain.