INTERNSHIP REPORT

ON

INFORMATION SYSTEM AUDIT

Submitted By
Md. Habibullah
Student Id: 173-35-2279

Supervised By
Mr. Md. Maruf Hassan
Associate Professor

APPROVAL

This Internship titled on "**Information System Audit**", submitted by **Md Habibullah (ID: 173-35-2279)** 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

Professor Dr. Engr. AKM Masum
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

Dr. Marzia Ahmed
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

External Examiner

Dr. Md. Monowarul Islam
Associate Professor
Department of Computer Science & Engineering
Jagannath University

STUDENT'S DECLARATION

I certify that, under the direction of my esteemed supervisor, I created this internship report entirely on my own as part of my Bachelor of Software Engineering degree. Every reference and information source used in this paper has been duly acknowledged.

Furthermore, I certify that this paper was written exclusively for academic reasons and for no other purpose. I accept full responsibility for any mistakes or inconsistencies in this paper.

Md. Habibullah

ID: 173-35-2279

Batch: 24

ACKNOWLEDGEMENT

DEDICATION

I dedicate my report to my parents, who have not only encouraged me to pursue my ambitions but also helped me along the way.

ABSTRACT

There is a growing interest in information system (IS) auditing among students and recent graduates. My work as an IS auditor at ACNABIN Chartered Accountants, a firm with eight esteemed partners, is summarized in this report. With a detailed description of the tasks, skills, and information I acquired and applied throughout my internship, this report offers a comprehensive summary of the job I accomplished.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Goal:

Internship programs offer invaluable practical experience. They bridge the gap between academia and the professional world, allowing students to apply their knowledge, identify their strengths and weaknesses, and develop essential skills. These skills include teamwork, communication, presentation, and adaptability to new technologies. Working alongside experienced professionals provides unique learning opportunities.

1.2 Encouragement:

As a Cybersecurity student at Daffodil International University, I sought an internship to gain practical experience beyond my academic learning. My primary motivation was to delve deeper into cybersecurity by facing real-world challenges, such as conducting internal and external audits and providing consultancy services. Having completed the "Information System Audit & Assurance" course, I chose ACNABIN Chartered Accountants, where I could apply my knowledge and skills as both an internal and external IT Auditor.

1.3 Goal for the Intern:

- utilizing several cybersecurity frameworks .
- Providing consultancy services.
- To ensure that the framework's requirements are being fulfilled, validation is carried out.
- Preparing and delivering comprehensive final assessment reports.
- Learning about sensitive information pertaining to security.
- Acquiring proficiency in industry-standard and applications.
- Improving abilities.

2. COMPANY INFORMATION

2.1 Overview:

ACNABIN, a distinct institutional subsidiary of Baker Tilly International, is one of the largest accounting firms in Bangladesh. The organization offers services in the following areas: information systems audit, tax, business advice management, and security, all while maintaining the highest standards of quality. Since its establishment in 1985, ACNABIN has grown into a dependable and competent partner for business networks and associated clients.

Value delivered to partners and customers is the basis for evaluating performance at ACNABIN. The organization, which has more than 500 highly skilled workers, provides expertise in a variety of business fields to meet the diverse needs of its premium clients.

Sponsored member of Baker Tilly International, strives to fully comprehend customer problems rather than merely offering quick fixes. In addition to meeting present needs, the company creates long-term plans to upcoming difficulties.
and is still dedicated to improving its standing by helping its clients succeed. It has developed well-known and respected businesses throughout the years. The fundamental principles of Baker Tilly International, which direct its operations and vision, form the foundation of the company's culture.

Our dedication is in assisting our customers and optimizing the abilities of our employees.

2.2 Perception:

We surpass the standard auditor-client connection .

2.3 Delegation:

Respect guidelines for customer since we understand how vital it is to safeguard private and proprietary data. Trust is the foundation of our success, and we are dedicated to maintaining it through unwavering commitment to these principles. Our efforts are focused on earning and preserving the trust of our clients at all times.

2.4 Fundamental Services:

- IS Audit
- Compliance & Assurance
- ISO 27001.

2.5 Departmentalization:

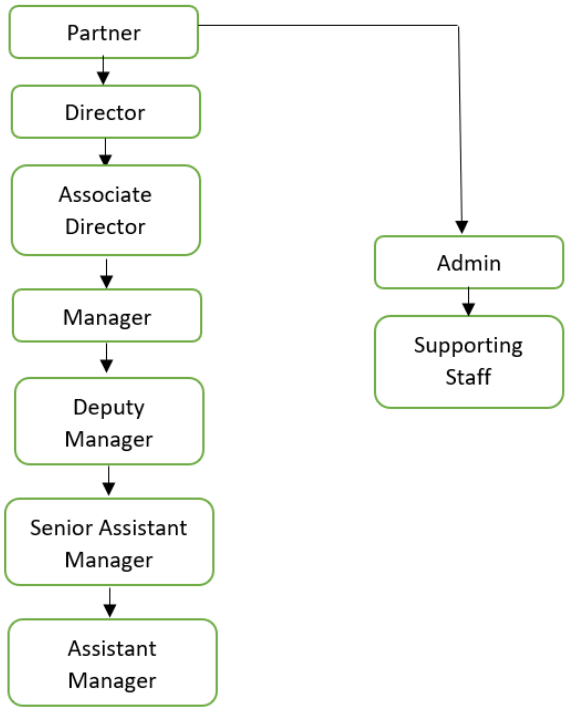


Fig 1: Structer of ACNABIN Chartered Accountants

3. OPERATIONAL PROCESS

3.1 Introduction:

The work and experiences I acquired as an IT auditor and cybersecurity consultant while working as an internship at ACNABIN Chartered Accountants are highlighted in this part. The IT Director of oversaw .

Synopsis:

I have performed three IT audits for three distinct customers during my internship, including manufacturing enterprises, architecture firms, and groups of organizations.

3.3 Kinds

Our company does two different kinds of audits. The following are some of the projects I've finished.

3. 4 Internal Audit

Aiming to enhance an organization's operations provide value, internal auditing is an objective, independent using systematic and disciplined evaluate enhance he governance, control, and management systems, it helps a business accomplish its goals.

3.3.2 External Audit:

An independent accountant conducting an audit . Usually, thean audit is to the finance accounts of an organization. All publicly traded corporations must have this certification, which is frequently demanded by lenders and investors. evaluate a accounting records, guarantee adherence to relevant accounting standards, and guarantee that financial statements fairly depict the client's status and performance.

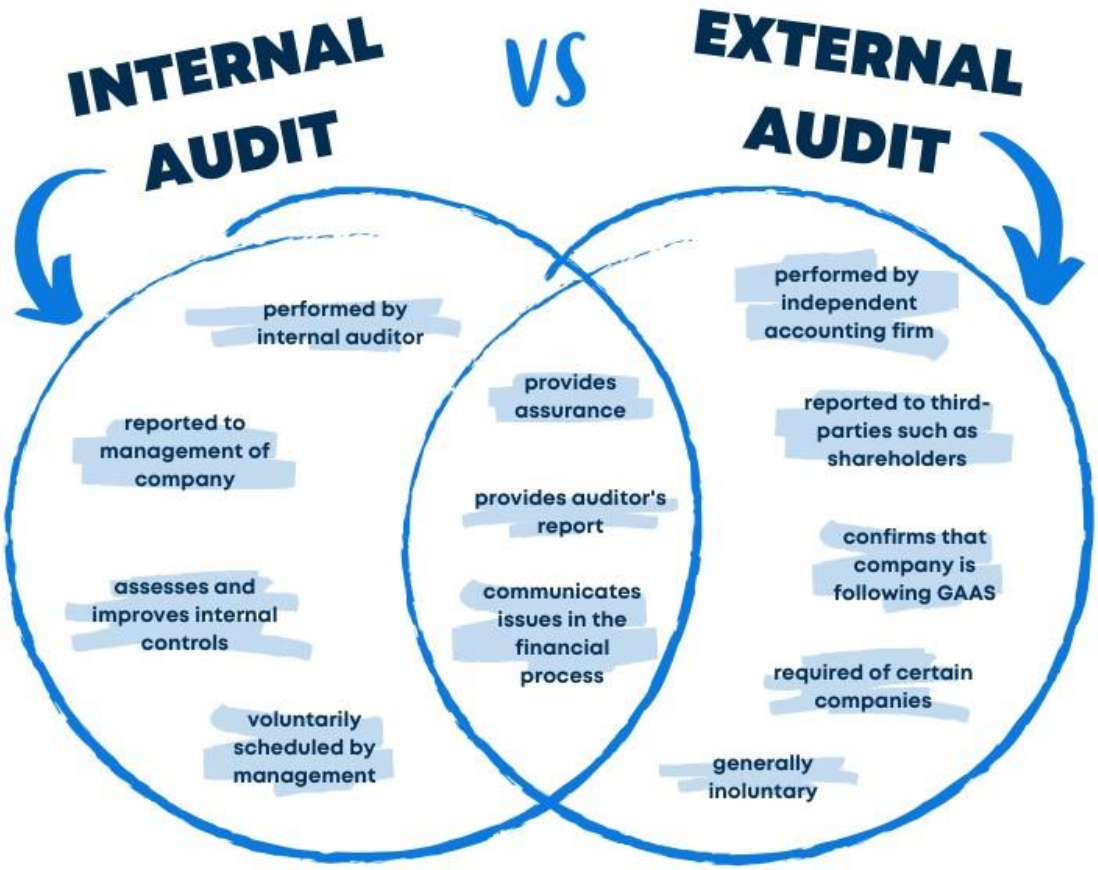


Fig 2: Structure

3.4 Major Clients:

My main customers, for whom I have performed internal and external IT audits, are:

- VOLUMEZERO Limited
- Walton Plaza

3.5 Audit Procedure

Today, every company depends on different IT infrastructures, which use technology to make corporate operations much simpler and more effective. We ask for particular papers pertaining to ICT security compliance in every IT audit, whether it is internal or external. We evaluate and confirm the conformity of these papers when they are received. After that, we find any non-compliance problems and bring them to management's attention so that appropriate action may be taken.

My steps of operation are as follows:

i. Ordering

Previous audits and expert reports pertinent to the subject under evaluation are reviewed by auditors. In order to obtain insights, they also look at pertinent rules and choices. After that, they create important audit plans that will direct the audit process.

ii. Alert

The appropriate will be informed impending rationale by Internal Audit Manager's workplace at the time of the first meeting.

iii. Start of

All employees involved in the audit, including supervisory and administrative officials, attend this meeting. The audit's goals and reasons are thoroughly covered during the session. The audit program may be modified in light of the data acquired during this conference to guarantee its applicability and efficacy.

iv. Practical

This phase doing necessary tests.

v. Reporting

A thorough report should be written following the completion of the hands-on training. Important topics such as the audit's goals and scope, guiding principles, main conclusions, and suggestions for changes or enhancements should all be covered in this report.

vi. Feedback

The administrative agency will get a draft audit report of the audited area for review and feedback on the proposed recommendations. The agency's response should include a detailed action plan outlining the steps for implementing the suggested changes.

vii. Last Session

Board responses and audit results will be reviewed and discussed at this meeting, which will be held in the Office of Officers. It is the ideal platform for posing queries and receiving responses. This meeting will also discuss any consequences of auditing methods that were not included in the previous report.

ix. Observation

About three months following the submission of the audit report, a follow-up investigation will be conducted by the audit management department. This check's objective is to determine whether corrective action has been carried out. I will provide complete style gained program.

5.For Documents:

The following criteria determine where the documents request is put in an IT audit:

- ICT Policy;
- Database Management log;
- Identification Mitigation Plan;

- Training awareness;
- Change Management Log
- Incident Report
- Technical controls
- Organizational Controls
- Audit Trial Report

3.5.2 Requisition List:

In an IT audit, the sample requisition list of General IT Audit Check list:

SL. No.	Initial Required Documents	Status	Feedback
1	'ICT Security Policy".	N/A	
2	Business Continuity Plan (BCP)		
3	An organizational chart for the ICT department		
4	Internal and external IS audit report.		
5	Documents for Information Security Training		
6	Incident management log		
7	Risk Assessment		
8	Mitigation control		
9	List of software		
10	Inventory list of all ICT assets		
11	Disposal policy		
12	Active Directory control policy		
13	Audit trail report		
14	Backup and restore log		
16	Change Management log		
20	Role-based access control list		
21	Password Management Policy		
23	Business Requirement Documents and Data Flow Diagram of ERP		
24	Router Configuration.		

3.5.3 Audit Format

Sample Of Audit format

General Information:

Date	
Name of the System	
Description	
Classification	
Owner	
Custodian	
Location	
IP Address	

Details Information:

Area	Status	Comments
Path of Logical Access		
Path of Physical Access		
Risk & Controls		
User Management		
User Management Policy		
User Create Process		
List of Active Users		
Password Management		
Password Policy		
Minimum Length of Password		
Password Complexity		
Password Expiry Period		
Backup & Restore		
Backup Policy		
Recovery Point Objective		
Recovery Time Objective		
Backup Log		
Change Management		
Change Management Policy		
User Acceptance Testing (UAT)		
Hardening		
Configuration Management Policy		
Patch Management Policy		

Path of Logical Access:

Path of Physical Access:

User Creation Process:

Patch Deployment Process:

Change Process:

Incident Management Process:

3.5.4 Documents Review:

Policy:

An authorized and documented ICT Security policy is required for every organization, manufacturing company, bank, non-bank financial institution, or multinational corporation that has implemented IT infrastructure for business reasons.

Generally,

- putting in place a thorough organizational security management plan.
- Identifying affected .
- Minimizing the harm.
- preserving the company's standing as a strong information security provider.
- Ensuring compliance with relevant legal standards and regulatory requirements.
- Securing sensitive client information against unauthorized access or breaches.
- limiting access to data for those who need it for valid reasons.

Organizational chart

A diagram that shows an organization's hierarchy and reporting lines is called an organogram chart, often referred to as an organizational chart. It is most frequently used to show how a business, government agency.

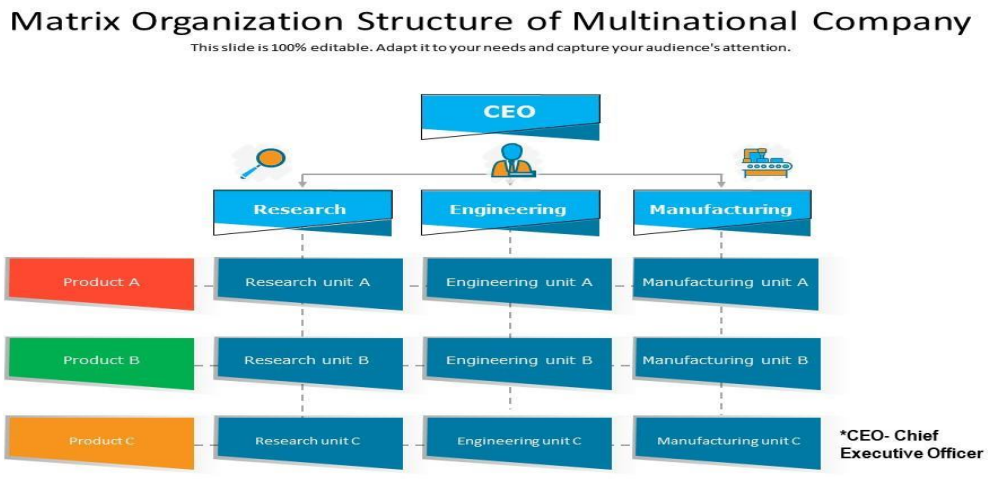


Fig – 3: Organogram of a multinational Company

Risk:

Any event involving ICT security that occurs within the company has to be recorded in order to determine the incident's risk.

Impact:

Several risk can compromise an organization's CIA standard.

And Rating of that risk which are found.The risk rating matrix should be established by the relevant firm or organization according to its business criticality.

Mitigation control:

One cannot completely remove risk. However, company choose weighing risks.

Approval :

Various risks associated with different departments, and the respective heads of these departments are designated as the risk owners. These risk owners are responsible for managing and addressing the risks within their areas. After the risks have been assessed, it is essential to obtain approval from the risk owners, acknowledging their awareness and acceptance of identified risks.

IT Asset list:

The following information :

- CPU
- Router
- Monitor
- Switch
- Device Brand
- Device Model
- User Name
-

- Location
- Vendor
- Author
- Specification ID

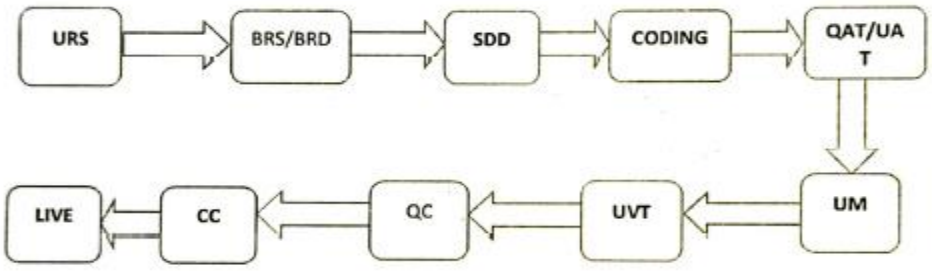
Product :

The business should keep track of the software that needs management approval. This covers both purchased and in-house software.

Ordering :

Important modifications to the production environment should be documented. To prevent going against CIA guidelines, all modifications to the system must be authorized. An audit log of the modifications must also be kept.

One of our clients maintains the following change procedure:



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: Change procedure

Testing :

The end user must perform a User Acceptance Test (UAT) following the required system modifications.

Applications Authorizations:

Original Application system, database, antivirus, Microsoft preserved. Any company or group using an unlicensed system would be breaking the law.

Operation:

Destry Asset:

All ICT assets must be disposed of securely by any company. A of prevents it from being utilized again for any reason.

Password control policy:

To prevent data breaches, every business or organization should adhere to the following password guidelines:

- Enforce password history: 4 passwords remembered
- Maximum password age: 60 days
- Minimum password age: 2 days
- Minimum password length: 8 characters
- Minimum password length audit: Not Defined
- Password must meet complexity requirements: Enabled
- Store passwords using reversible encryption: Disabled

Network Architecture:

Incorporate the and protocols connectedness of the complete network through servers, routers, firewalls, databases, cloud computing, and end-user PCs.

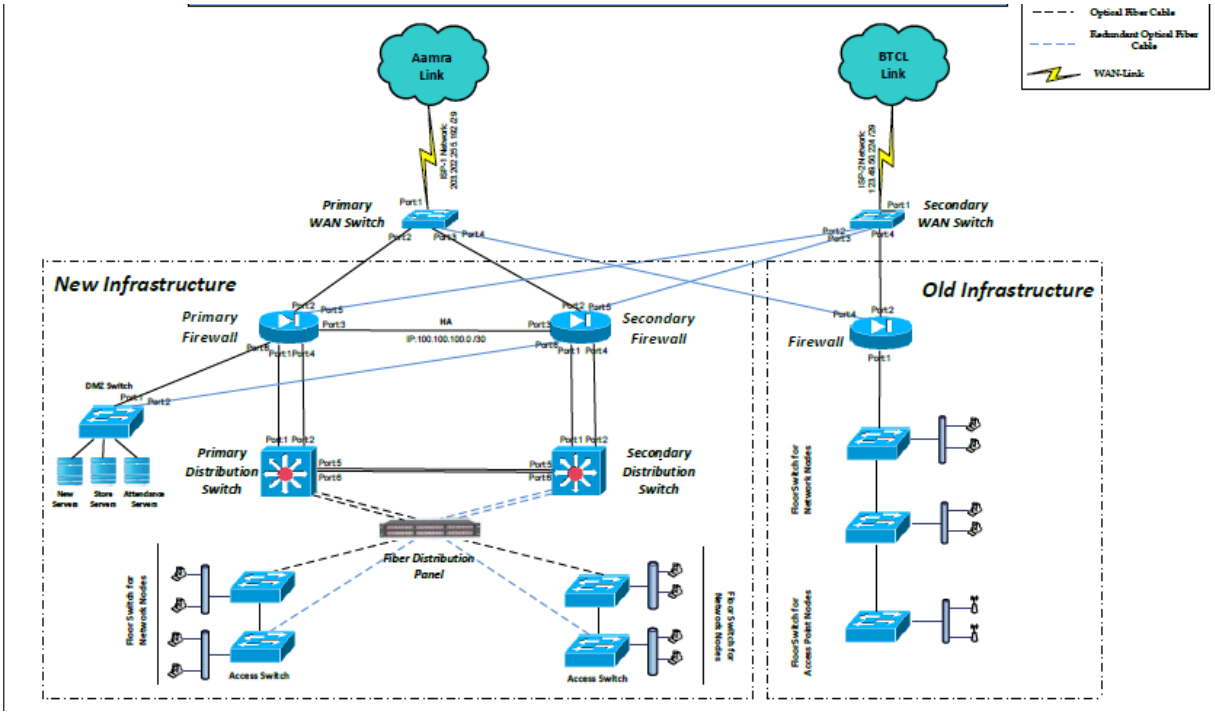


Fig 6: Network Design Document

User policy:

An enterprise must establish addresses topics in order to guarantee safe email communication and guard against penetrated

- Don't send private or proprietary information by email.
- It is forbidden to use business email for personal purposes.
- Instructions on how to use attachments.
- A mandate that workers only utilize authorized email providers.
- Mail archiving policy. An instruction manual for auto responders.

Business Plan:

Business Continuity Plans (BCPs) are strategic plans created to keep businesses running in the event of catastrophes or natural disasters. These occurrences might include fires or other disturbances that stop regular company operations. Organizations must identify possible risks and

create a thorough business continuity plan (BCP) in order to be ready for such circumstances and guarantee that critical activities will continue in the event that the threats become real.

A business continuity plan includes:

- Threat analysis for organizations.

- Easy access to administrative contact information.

- A map indicating the designated areas for employees.

- A page outlining support for the organization.

- Collaboration across all departments or sections of the organization.

- Collection of feedback from all members to improve organizational processes and decisions.

You should identify possible threats to your regular operations while creating your business continuity plan. Main taks requid to keep everything running. How many employees are necessary to run your business, and what equipment and data are needed managers and their contact details have to be part of the business continuity strategy. These people ought to keep each other's contact details private. remotely and in order to plan our return to work if we are unable to come to the office. This involves putting disaster recovery plans and data backups into action.

Restoring:

A company has to maintain a data backup at a display location. Necessary, the so recover the date.

Commitment:

The acronym SLA represents Service Level Agreement. Any purchase or service agreement must have a SLA that is signed by both parties. The terms and conditions of the acquired service are outlined in this mutual agreement.

For organizations and customers alike, setting precise SLAs is essential to ensuring seamless operations and support. In her work on developing SLAs, Naomi Karten emphasizes how crucial they are as a document for managing expectations, a communication tool, and a dispute resolution process.

Here have sample;

Finding 1: Absence of ICT security policy.

Observation

An ICT security policy is a document outlining guidelines and procedures to protect an organization's information and technology assets from unauthorized access, use, disclosure, disruption, modification, or destruction. It covers a range of topics, including access controls, data encryption, incident response, and disaster recovery.

During our audit period, we observed that [redacted] does not have ICT security policy.

Risk Rating:

Risk:

- Without a clear security framework, sensitive data may be exposed to unauthorized individuals.
- Lack of proper security practices can lead to system failures and disruptions.
- Without clear security protocols, incident response and risk management processes may be delayed or ineffective.

Recommendations:

Develop a Comprehensive ICT Security Policy.

Management Response:

Finding 2: Absence of Business Continuity Plan (BCP).

Observation

A Business Continuity Plan (BCP) is a strategic framework outlining how an organization will sustain essential operations during unforeseen disruptions, such as natural disasters, cyberattacks, or other emergencies. It includes minimizing downtime, ensuring employee safety, and safeguarding critical business functions.

In our audit period we observed that [redacted] does not have Business Continuity Plan (BCP).

Risk Rating:

Risk:

- Without a BCP, the organization may struggle to respond effectively to unexpected events, leading to prolonged downtime, loss of productivity, and potential financial losses.
- Failure to have a BCP in place may result in non-compliance with industry regulations, exposing the organization to legal and regulatory consequences.
- Without a plan to mitigate disruptions, the organization may face increased recovery costs, insurance premiums, and potential legal liabilities, impacting overall financial stability.

Recommendation:

[redacted] should develop Business Continuity plan (BCP)

Management Response:

Finding 3: User Acceptance Test (UAT) is not performed properly

Observation

The ICT policy lacks a formal requirement for conducting and documenting User Acceptance Testing (UAT) for new systems or updates. UAT is critical for ensuring that systems meet business requirements and user expectations before deployment.

During our audit period, we observed that "XXX" does not perform User Acceptance Test (UAT).

Risk Rating:

Risk:

- Without UAT, systems may go live with functionality issues or fail to meet user requirements.
- May lead to operational inefficiencies and increased support costs.
- It may reduce productivity, potentially impacting customer experience and business performance.

Recommendation:

Implement a formal UAT process, requiring UAT reports to be completed, reviewed, and signed off before any system moves to production.

Management Response:

Finding 4: Weaknesses in Privileged Access Management Control.

Observation

During our audit period, we observed that [redacted] person has individuals an admin role, and one person has both admin and super admin roles in the application system. Furthermore, they all possess the
same access privileges and all the accounts are active.

Risk Rating:

Risk:

- Integrity may not be ensured.
- A larger pool of users with Super Admin-level access expands the potential attack vectors for malicious actors.
- Mistakes or accidental actions by authorized Admins could have severe consequences due to their elevated privileges.
- Accountability may not be ensured.

Recommendation:

Implement least privilege access control.

Management Response:

Finding 5: Change Management log is not Maintain

Observation

The Change Management Log is a comprehensive record of all changes made to a project or system. It tracks changes from initiation to closure, including their impact, approval status, and implementation details.

During our audit period we observed that [redacted] doesn't maintain Change management log.

Risk Rating:

Risk:

- May lead to system vulnerabilities, data corruption, or operational disruptions.
- Lack of transparency and accountability regarding system changes.

Recommendation:

Maintain and keep the record of change management log.

Management Response:

Finding 6: Incident management log is not documented for our audit period

Observation

The Incident Management Log is a detailed record of all incidents that disrupt IT services. It tracks each incident's timeline, resolution steps, and impact, aiding in problem resolution and future incident prevention.

During our audit period, we observed that [redacted] does not maintain a centralized log for system to record and track security incidents, breaches, or operational disruptions.

Risk Rating:

Risk:

- Lack of managing log makes it difficult to track, analyze, or learn from past incidents.
- Incidents may not be resolved in a timely or effective manner due to insufficient information about previous occurrences or response efforts.
- Ineffective audits and loss of organizational trust.

Recommendation:

Implement a centralized Incident Management Log to document every security event, including incident type, severity, date/time, root cause, response actions, and resolution status.

Management Response:

Finding 7: Business Impact Analysis (BIA) is not performed

Observation

A Business Impact Analysis (BIA) is a systematic process to identify potential threats to business operations and assess their potential impact.

During our audit period, we observed that [redacted] does not have Business Impact Analysis (BIA) documents to evaluate the potential effects of disruptions to business operations, critical systems, and processes.

Risk Rating:

Risk:

- Lack of understanding of the criticality of business processes, dependencies, and acceptable recovery times.
- Ineffective allocation of resources for business continuity and disaster recovery planning.
- Potential non-compliance with regulatory or industry standards requiring BIA.

Recommendation:

Implement and maintain a formal Business Impact Analysis (BIA) document.

Management Response:

4. CONCLUSION

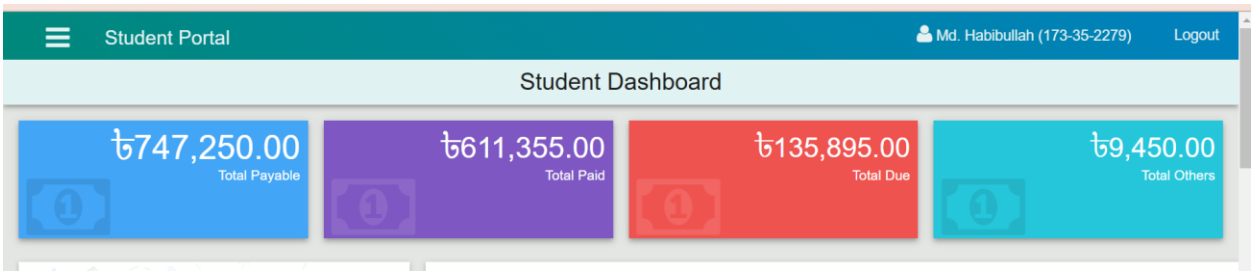
In Auditing we examine the IT Structure and its security. Which based on business model. We follow up their policy and industry standard . We also clarify is it internationally recognized or not. We used the framework of NIST, Covit , ISO. And we also categorized by depertment like health for HIPPA, For Europe GDPR. The all are has to authorized that auditing lookup.

So for Industry's quality it is important and also a good initiate for us.

REFERENCES

1. *ISACA (Information Systems Audit and Control Association)*
2. *COBIT*. ISACA. https://www.isaca.org/resources/cobit
3. *Information Technology Control and Audit (4th ed.) by Sandra Senft,Frederick Gallegos, and Aleksandra Davis*
4. https://econpapers.repec.org/article/tafuipsxx/v_3a10_3ay_3a2014_3ai_3a1_3ap_3a53-55.htm
5. CISA Official Review Manual, 28th Edition

Accounts Clearance



Library Clearance