Internship on Information System Audit

Submitted By:

Rashidul Islam

ID: 183-35-383

(27th Batch)

Department of Software Engineering

Daffodil International University

Supervised By:

Mr. Md. Maruf Hassan

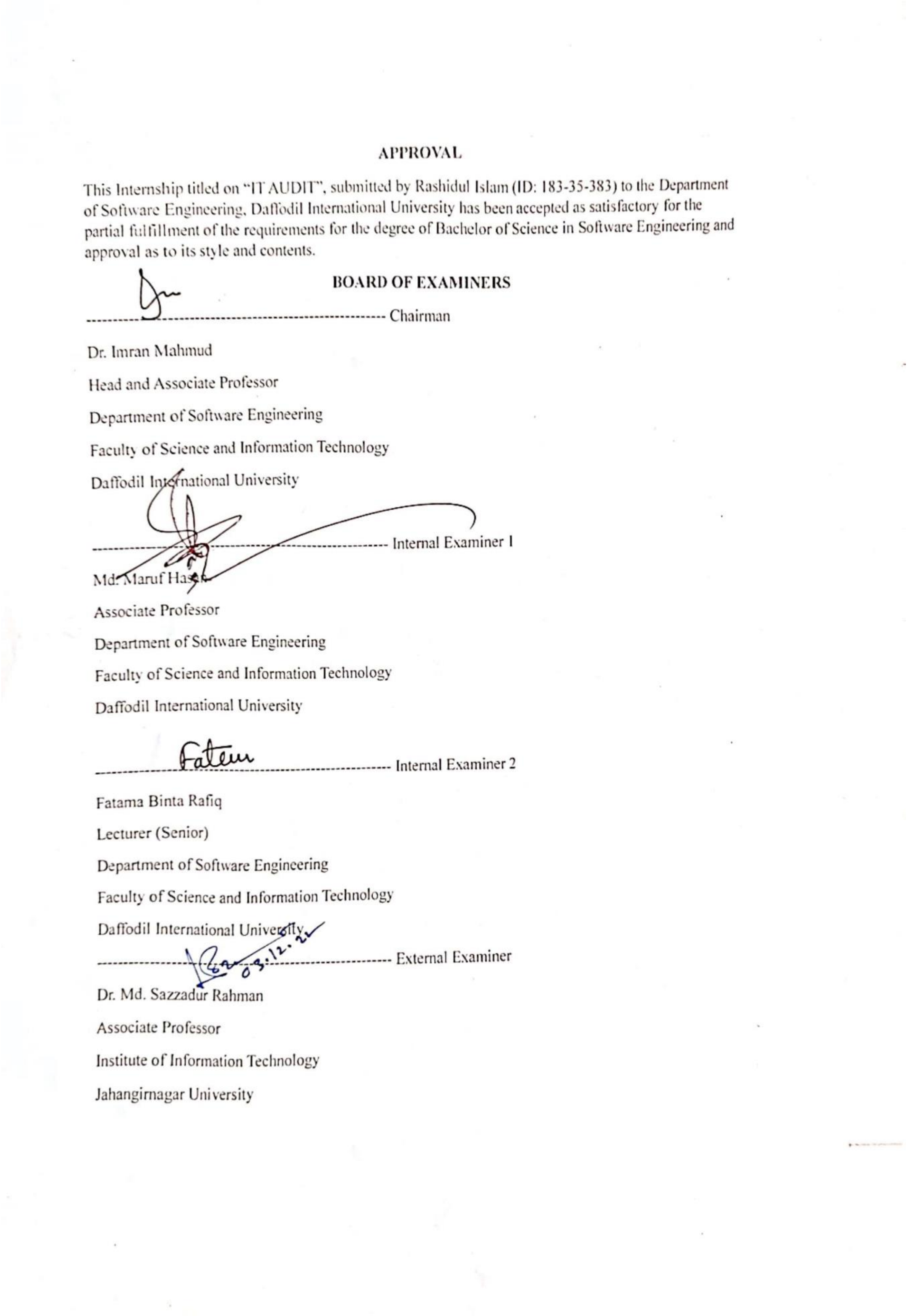
Associate Professor, Department of software Engineering

Daffodil International University

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

Department of Software Engineering
DAFFODIL INTERNATIONAL UNIVERSITY

Fall – 2022



APPROVAL

This Internship titled on "IT AUDIT", submitted by Rashidul Islam (ID: 183-35-383) 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. Maruf Hasan

Associate Professor

Department of Software Engineering

Faculty of Science and Information Technology

Daffodil International University

Fatem

-- Internal Examiner 2

Fatama Binta Rafiq

Lecturer (Senior)

Department of Software Engineering

Faculty of Science and Information Technology

Daffodil International University

03.12.22

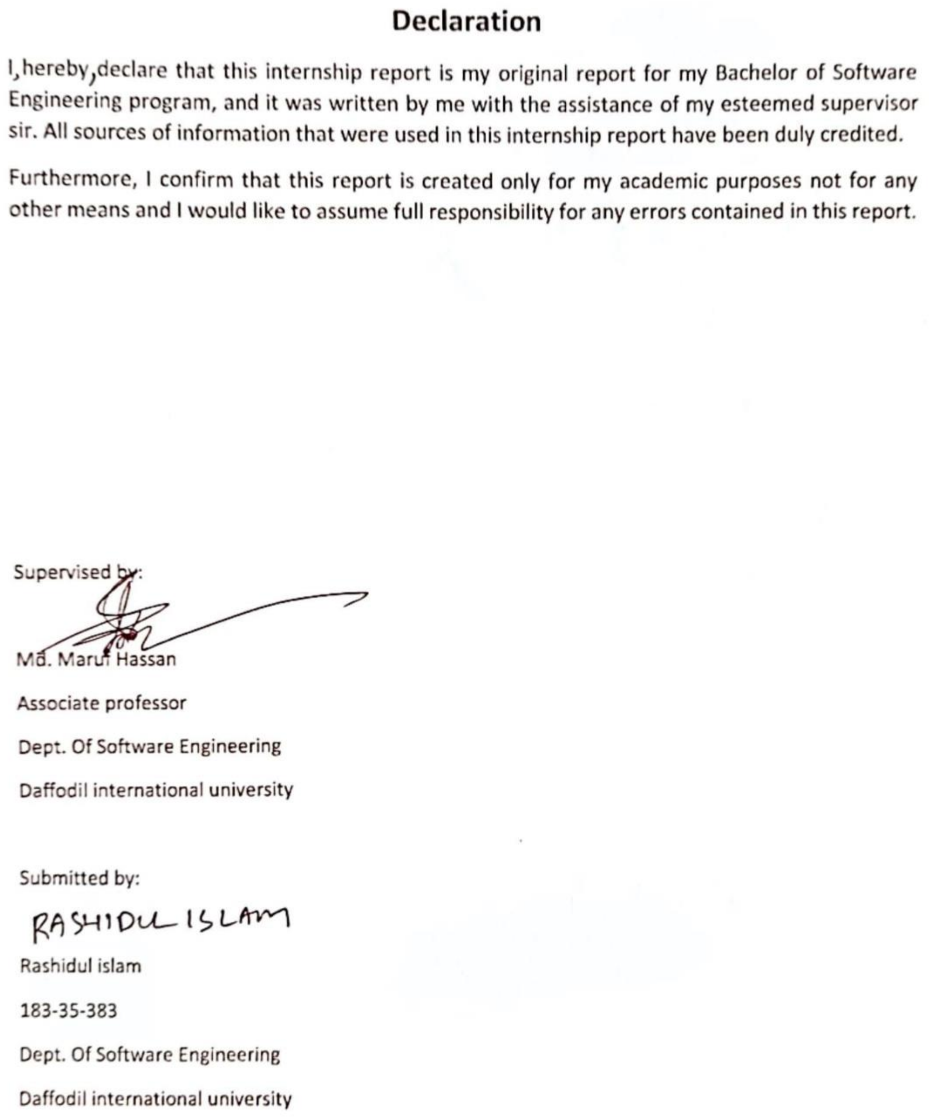
-- External Examiner

Dr. Md. Sazzadur Rahman

Associate Professor

Institute of Information Technology

Jahangirnagar University



Declaration

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

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

Supervised by:

Md. Maruf Hassan

Associate professor

Dept. Of Software Engineering

Daffodil international university

Submitted by:

RASHIDUL ISLAM

Rashidul islam

183-35-383

Dept. Of Software Engineering

Daffodil international university

ACKNOWLEDGEMENT

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

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

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

ABSTRACT

Information System (IS) audit and consultancy has become a popular approach among fresh graduates and students. This report consists of a description of my work as an IS auditor in ACNABIN Chartered Accountants. This firm has 10 partners in total. I am completing my internship under our honorable partner sir Muhammad Aminul Haque, FCA and I was supervised by our honorable director Mr. A.N.M. Shakawath Hossain CISA, I have completed my internship program in this firm from 15th of May, 2022 to 15th of November, 2022. In this report I will describe each and every work that I have learnt and implemented during my internship program.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Objective:

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

1.2 Motivation:

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

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

1.3 Internship Goals:

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

2. COMPANY INFORMATION

2.1 Introduction about the Firm:

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

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

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

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

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

2.2 Vision:

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

2.3 Mission:

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

2.4 Core Services:

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

2.5 Organizational Structure:

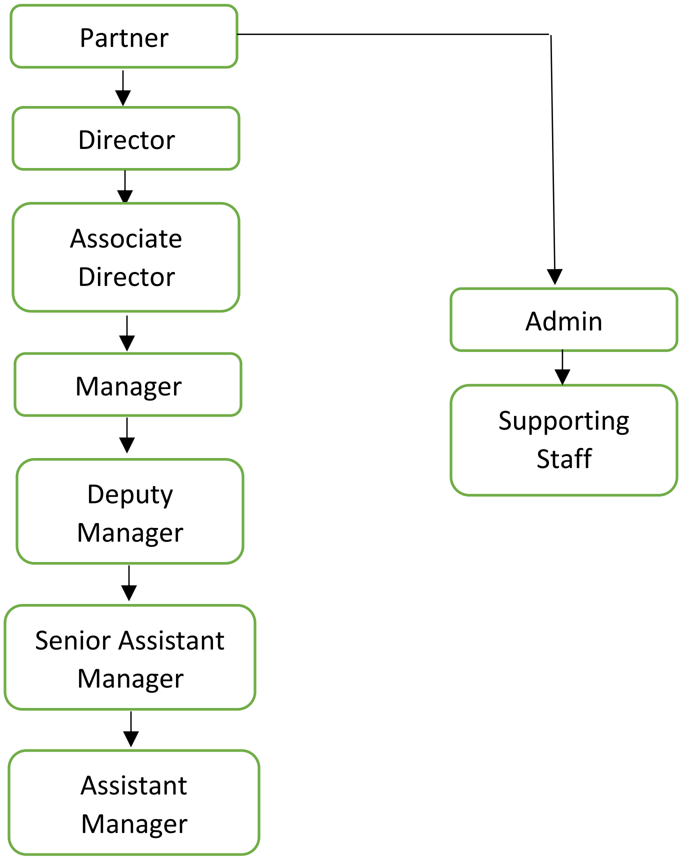


Fig – 1: Organogram Chart of ACNABIN CA

3. WORKING PROCEDURE

3.1 Introduction:

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

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

3.2 Overview:

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

3.2.1 Types of IT Audit

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

1. Internal Audit.
2. External Audit.

3.2.1.1 Internal IT Audit:

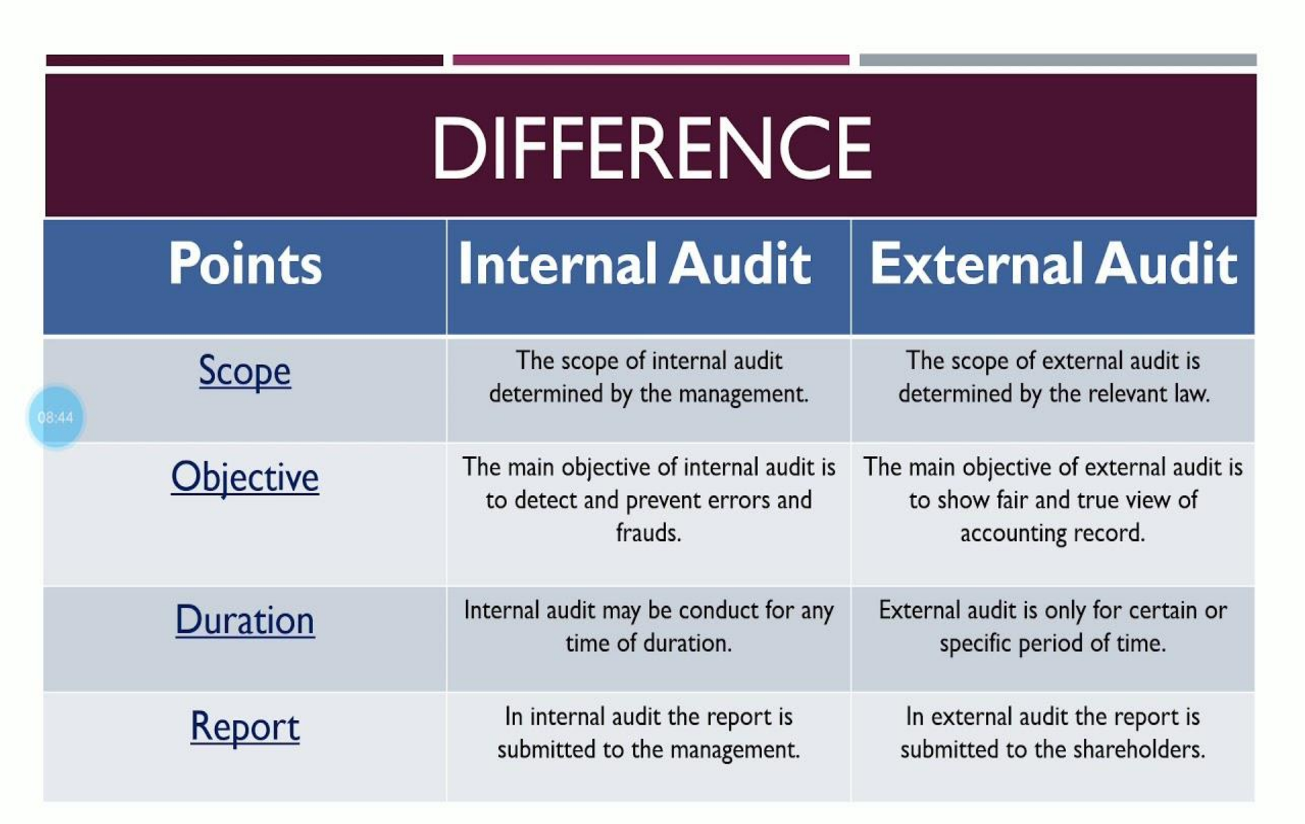
Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management,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

3.2.1.2 External IT Audit:

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

The objectives of an external audit are to determine:

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



DIFFERENCE

Points	Internal Audit	External Audit
Scope	The scope of internal audit determined by the management.	The scope of external audit is determined by the relevant law.
Objective	The main objective of internal audit is to detect and prevent errors and frauds.	The main objective of external audit is to show fair and true view of accounting record.
Duration	Internal audit may be conduct for any time of duration.	External audit is only for certain or specific period of time.
Report	In internal audit the report is submitted to the management.	In external audit the report is submitted to the shareholders.

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 –
2.
    - Walton
    - Grameenphone (GP)

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

3.4 Audit Procedure

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

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

Here are my working steps:

1. Arrangements

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

2. Warning

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

3. Commencement of meeting

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

4. Hands-on

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

5. Write a report

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

6. Board Response

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

7. Closing Session

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

8. Distribution of Final Audit Report

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

9. Follow-up

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

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

3.4.1 Documents requisition:

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

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

3.4.2 Requisition List:

We ask for these documents for an IT Audit:

SL#	**Document Required for IT Audit**
1	"ICT Security Policy".
2	Organogram chart of ICT department including job description, segregation of duties and fallback plan.
3	Organogram for ICT support unit.
4	Scheduled roster for ICT personnel
5	Internal and/or external IS audit report (Last Three (03)).
6	Information Security Training documents for last period, copy of yearly training plan, List of participants.
7	Incident/Problem management log
8	Assessment of the risk
9	Identification of mitigation control
10	Remedial plan to reduce the risk
11	Approval of the risk acknowledgement from the owner of the risk
12	IT based/enabled product list [marked recently launched (if any) product], list of upcoming products.
13	List of software (in house and purchased).
14	Document of change procedure for IS (Documentation about –Necessary change details in production environment, Audit log of changes)
15	User Acceptance Test (UAT) for changes
16	Inventory list of all ICT assets
17	Software licenses (OS, DB, Anti-Virus, MS Office, etc.)
18	Operating procedure (Operating procedure for the users, Scheduling process, system start-up, close down, restart, recovery process.)
19	Handling of exception condition.
20	Secure disposal policy
21	Active Directory and password control policy
22	Audit trail report including user ID, authorizer ID and date-time stamp for System for a particular period of time
23	Network design document (should contain protocols and security features)
24	Email and internet usage policy
25	Outsourced software documentation
26	Business Continuity Plan
27	Backup and restore log
28	Disaster Recovery test report, list of available software in DR site.
29	SLA with software vendor, connectivity provider and with other vendors
30	Documentation about—Total Bandwidth used, No of Fiber communication link with vendor name, Network security devices
31	Annual fire testing report

32	User Creation Policy and procedures (Domain, Email, Software etc.)
33	User deletion/deactivation Policy and procedures (Domain, Email, Software etc.)
34	Software Design & Development related documents
35	List of security solution (Firewall, Anti-virus, SIEM, PAM etc.)
36	Firewall and any other security solutions Report
37	Antivirus Dashboard Report
38	Software testing related documents
39	Role base access control list
40	List of computer/software users and their privilege
41	Server and Network utilization report in regular interval

3.4.3 Audit Format:

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

General Information:

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

Details Information*:*

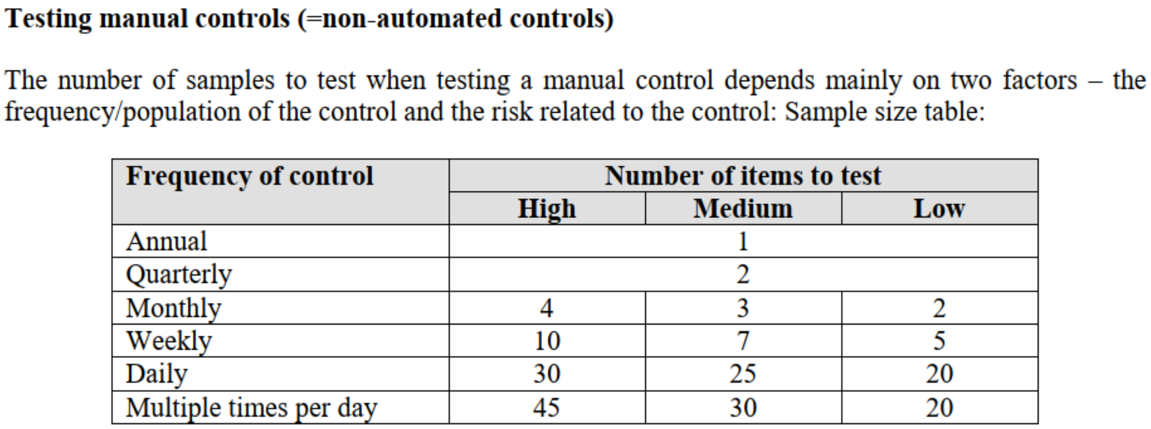
Area	**Status**	**Comments**
Logical Access Path		
Physical Access Path		
Remote Access		
Risk & Controls		
Risk Assessment		
List of IT Controls		
User Management		
User Management Policy		
User Creation Process		

List of All Active Users with Access Privilege		

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

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

Sample Size:



Testing manual controls (=non-automated controls)

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

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

3.4.4 Documents Analysis:

ICT Security Policy:

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

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

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

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

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

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

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

Risks should be identified and rated in three categories:

1. High
2. Medium
3. Low.

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

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

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

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

IT based/enabled product list:
This list contains all information of all the ICT assets that are being used by the employees of the company.

This part should contain the following contents:

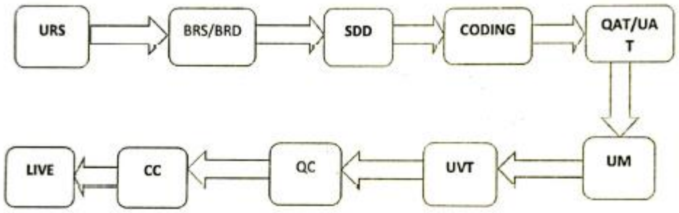
- Office
- Cost Centre

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

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

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

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



URS: User Requirement Specification
BRS: Business Requirement Specification
SDD: Software Design Document
QAT: Quality Assurance & Testing
UM: User Manual
UVT: User Verification Test
QC: Quality Control
CC: Configuration Controller

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

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

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

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

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

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

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

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

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

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

A business continuity plan includes:

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

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

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

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

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

SLA with software vendor, connectivity provider and with other vendors:
SLA stands for Service Level Agreement. SLA must be documented for the both parties in case of any purchase or service. SLA is the mutual agreement for the purchased service with all conditions.

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

Typical SLA content -

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

1. Contract overview -

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

2. Goals and targets -

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

3. Stakeholder -

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

4. Periodic review -

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

5. Service contract -

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

- Scope of services. Deal with the specific services provided by the contract. B. Phone Support.
- Customer requirements, including payment details at agreed intervals.

- Service provider requirements are also part of the service agreement and cover areas including defining response times for service-related incidents.
- Service premise. Here we discuss logging changes to the service and how they are communicated to stakeholders.

6. Service management -

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

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

User Creation & Deletion Policy and procedures:

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

Following contents should be considered for an access control policy:

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

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

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

3.4.5 Audit Report

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

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

Here I have attached a sample IT audit report:

4. CONCLUSION

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

REFERENCES

[1] *Advancing IT, audit, governance, risk, privacy & cybersecurity*. (n.d.). ISACA. Retrieved November 3, 2022, from https://www.isaca.org/

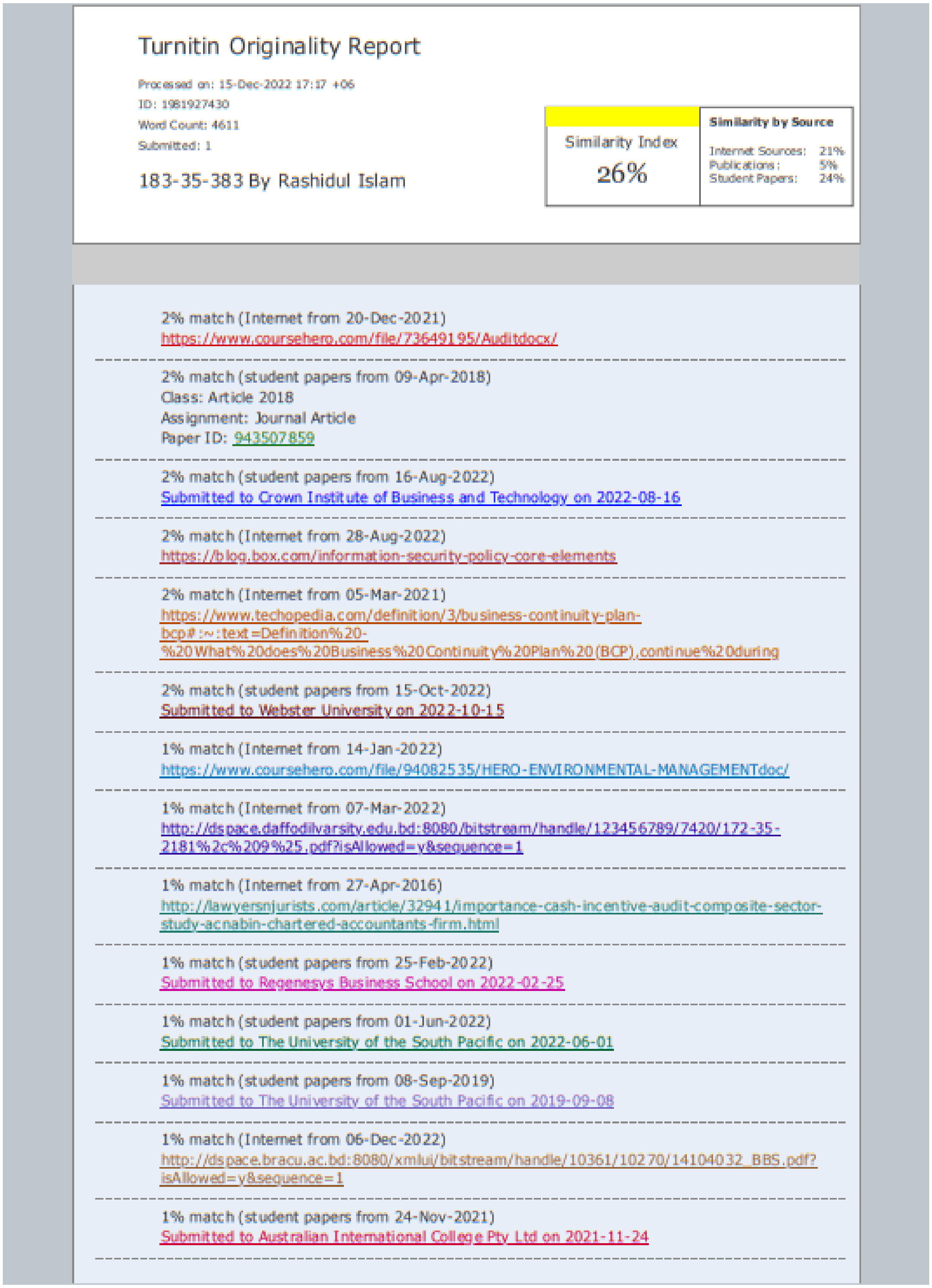
[2] *COBIT*. (n.d.). ISACA. Retrieved November 3, 2022, from https://www.isaca.org/resources/cobit

[3] *IS audit basics: The Core of IT Auditing*. (n.d.). ISACA. Retrieved November 3, 2022, from https://www.isaca.org/resources/isaca-journal/past-issues/2014/is-audit-basicsthe-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: 15-Dec-2022 17:17 +06
ID: 1981927430
Word Count: 4611
Submitted: 1

183-35-383 By Rashidul Islam

Similarity Index	Similarity by Source	
26%	Internet Sources:	21%
	Publications:	5%
	Student Papers:	24%

2% match (Internet from 20-Dec-2021)
https://www.coursehero.com/file/73649195/Auditdocx/

2% match (student papers from 09-Apr-2018)
Class: Article 2018
Assignment: Journal Article
Paper ID: 943507859

2% match (student papers from 16-Aug-2022)
Submitted to Crown Institute of Business and Technology on 2022-08-16

2% match (Internet from 28-Aug-2022)
https://blog.box.com/information-security-policy-core-elements

---

2% match (Internet from 05-Mar-2021)
https://www.techopedia.com/definition/3/business-continuity-plan-bcp#:~:text=Definition%20-%20What%20does%20Business%20Continuity%20Plan%20(BCP),continue%20during

---

2% match (student papers from 15-Oct-2022)
Submitted to Webster University on 2022-10-15

1% match (Internet from 14-Jan-2022)
https://www.coursehero.com/file/94082535/HERO-ENVIRONMENTAL-MANAGEMENTdoc/

1% match (Internet from 07-Mar-2022)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/7420/172-35-2181%2c%209%25.pdf?isAllowed=y&sequence=1

1% match (Internet from 27-Apr-2016)
http://lawyersnjurists.com/article/32941/importance-cash-incentive-audit-composite-sector-study-acnabin-chartered-accountants-firm.html

---

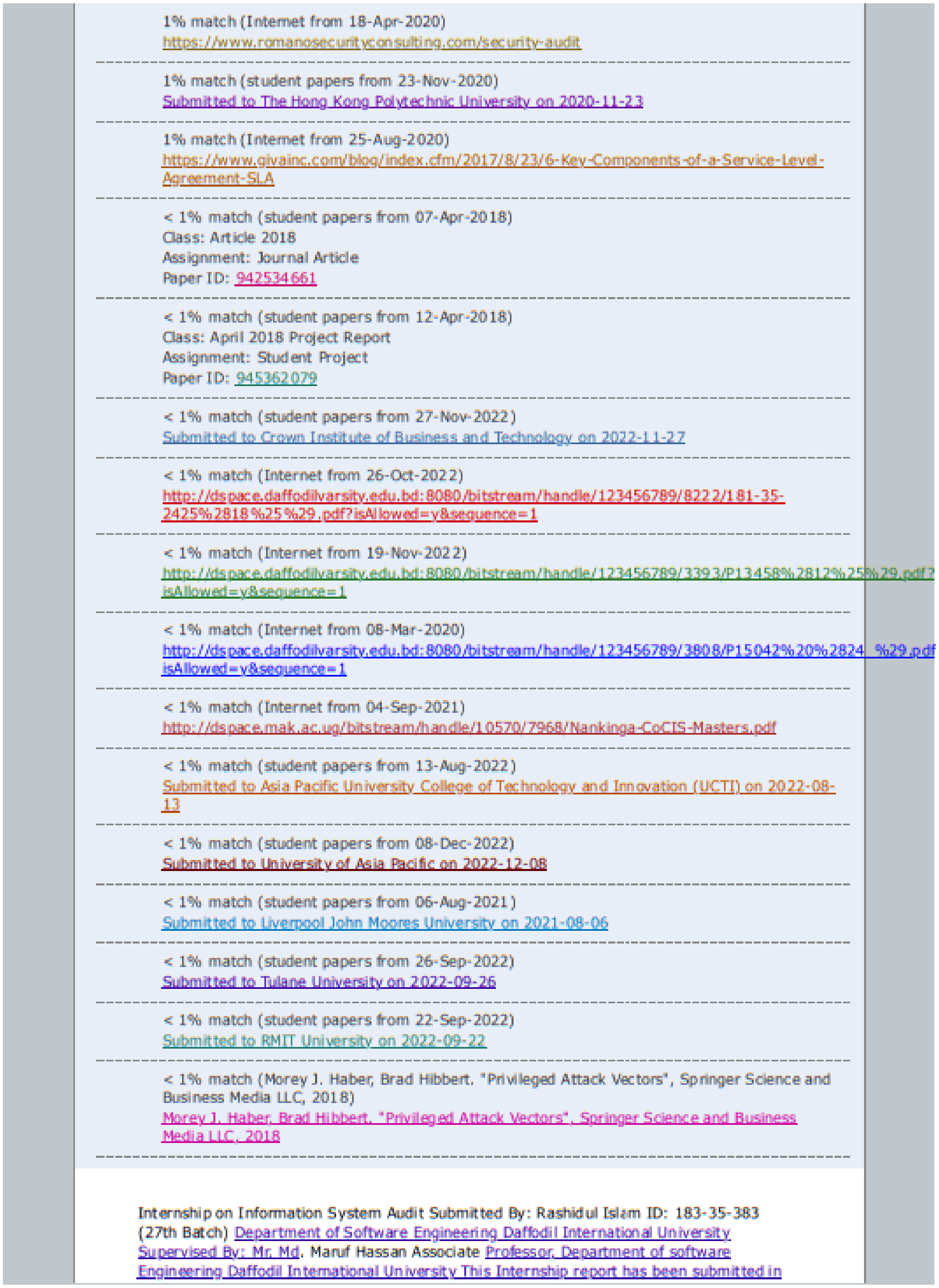
1% match (student papers from 25-Feb-2022)
Submitted to Regenesys Business School on 2022-02-25

1% match (student papers from 01-Jun-2022)
Submitted to The University of the South Pacific on 2022-06-01

1% match (student papers from 08-Sep-2019)
Submitted to The University of the South Pacific on 2019-09-08

1% match (Internet from 06-Dec-2022)
http://dspace.bracu.ac.bd:8080/xmlui/bitstream/handle/10361/10270/14104032_BBS.pdf?isAllowed=y&sequence=1

1% match (student papers from 24-Nov-2021)
Submitted to Australian International College Pty Ltd on 2021-11-24



1% match (Internet from 18-Apr-2020)
https://www.romanosecurityconsulting.com/security-audit

1% match (student papers from 23-Nov-2020)
Submitted to The Hong Kong Polytechnic University on 2020-11-23

1% match (Internet from 25-Aug-2020)
https://www.givainc.com/blog/index.cfm/2017/8/23/6-Key-Components-of-a-Service-Level-Agreement-SLA

< 1% match (student papers from 07-Apr-2018)
Class: Article 2018
Assignment: Journal Article
Paper ID: 942534661

< 1% match (student papers from 12-Apr-2018)
Class: April 2018 Project Report
Assignment: Student Project
Paper ID: 945362079

< 1% match (student papers from 27-Nov-2022)
Submitted to Crown Institute of Business and Technology on 2022-11-27

< 1% match (Internet from 26-Oct-2022)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/8222/181-35-2425%2818%25%29.pdf?isAllowed=y&sequence=1

< 1% match (Internet from 19-Nov-2022)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/3393/P13458%2812%25%29.pdf?
isAllowed=y&sequence=1

< 1% match (Internet from 08-Mar-2020)
http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/3808/P15042%20%2824_%29.pdf
isAllowed=y&sequence=1

< 1% match (Internet from 04-Sep-2021)
http://dspace.mak.ac.ug/bitstream/handle/10570/7968/Nankinga-CoCIS-Masters.pdf

< 1% match (student papers from 13-Aug-2022)
Submitted to Asia Pacific University College of Technology and Innovation (UCTI) on 2022-08-13

< 1% match (student papers from 08-Dec-2022)
Submitted to University of Asia Pacific on 2022-12-08

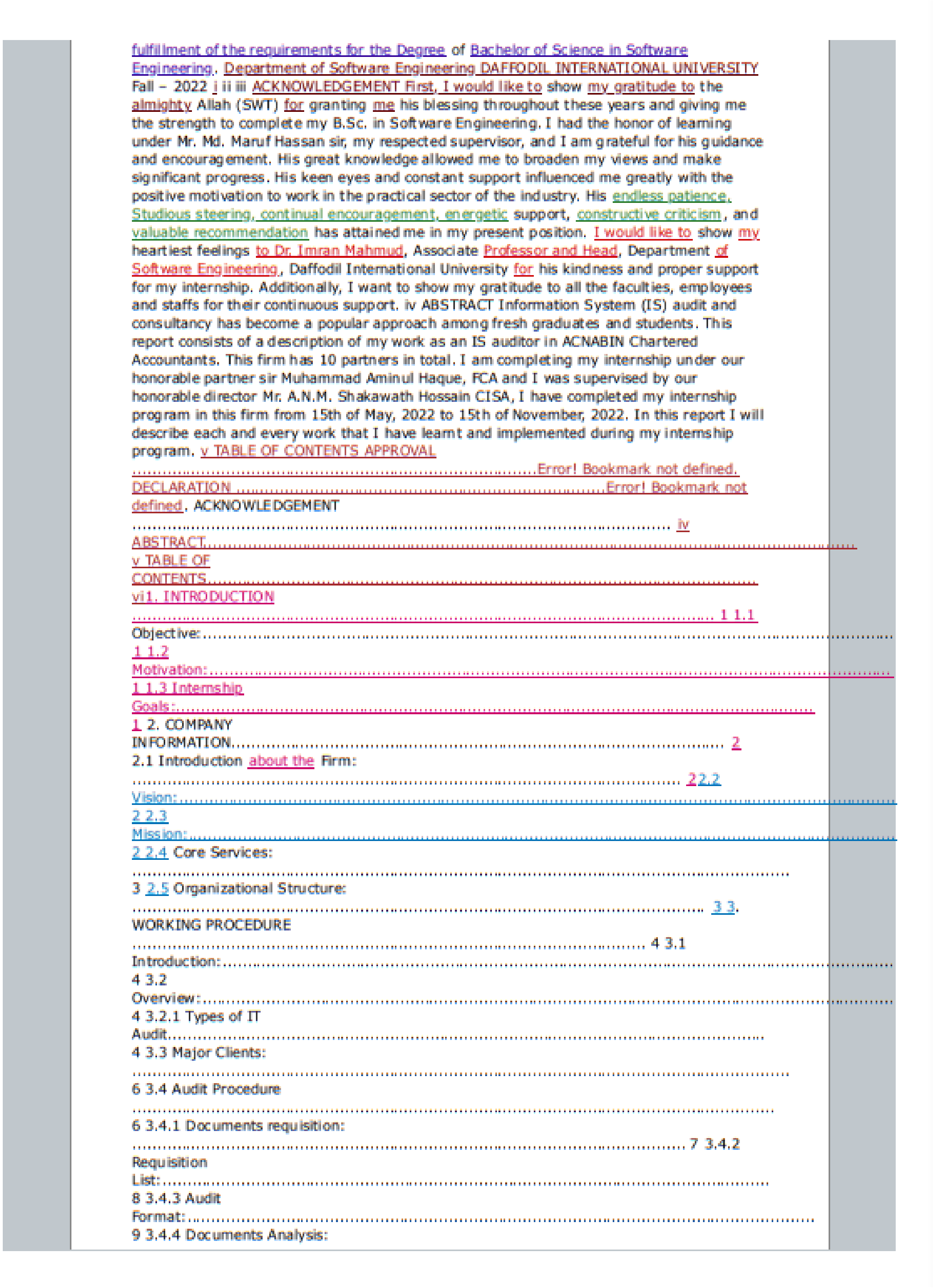
< 1% match (student papers from 06-Aug-2021)
Submitted to Liverpool John Moores University on 2021-08-06

< 1% match (student papers from 26-Sep-2022)
Submitted to Tulane University on 2022-09-26

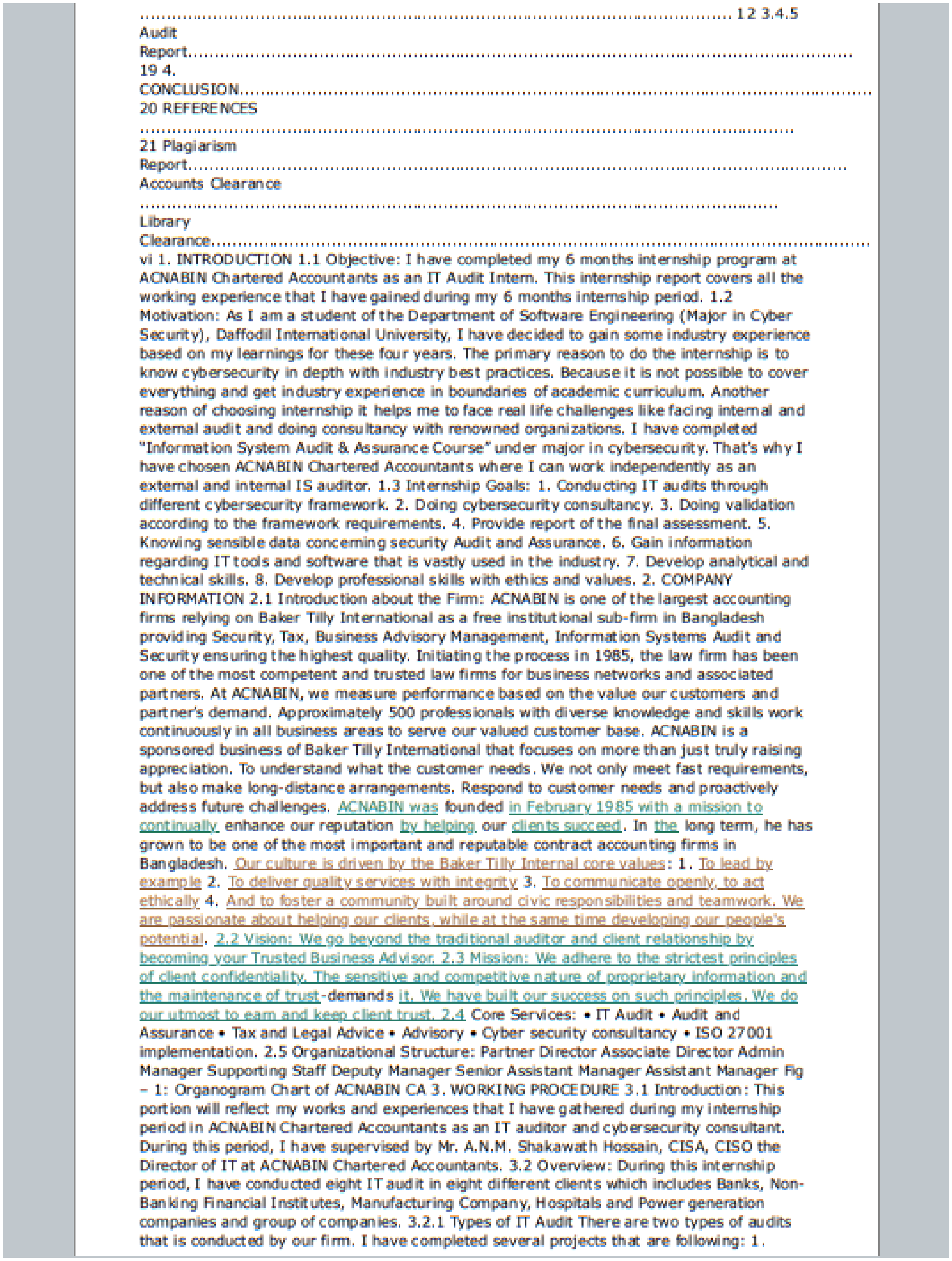
< 1% match (student papers from 22-Sep-2022)
Submitted to RMIT University on 2022-09-22

< 1% match (Morey J. Haber, Brad Hibbert. "Privileged Attack Vectors", Springer Science and Business Media LLC, 2018)
Morey J. Haber, Brad Hibbert. "Privileged Attack Vectors", Springer Science and Business Media LLC, 2018

Internship on Information System Audit Submitted By: Rashidul Islam ID: 183-35-383 (27th Batch) Department of Software Engineering Daffodil International University Supervised By: Mr. Md. Maruf Hassan Associate Professor, Department of software Engineering Daffodil International University This Internship report has been submitted in



fulfillment of the requirements for the Degree of Bachelor of Science in Software Engineering. Department of Software Engineering DAFFODIL INTERNATIONAL UNIVERSITY Fall – 2022 i ii iii ACKNOWLEDGEMENT First, I would like to show my gratitude to the almighty Allah (SWT) for granting me his blessing throughout these years and giving me the strength to complete my B.Sc. in Software Engineering. I had the honor of learning under Mr. Md. Maruf Hassan sir, my respected supervisor, and I am grateful for his guidance and encouragement. His great knowledge allowed me to broaden my views and make significant progress. His keen eyes and constant support influenced me greatly with the positive motivation to work in the practical sector of the industry. His endless patience, Studious steering, continual encouragement, energetic support, constructive criticism, and valuable recommendation has attained me in my present position. I would like to show my heartiest feelings to Dr. Imran Mahmud, Associate Professor and Head, Department of Software Engineering, Daffodil International University for his kindness and proper support for my internship. Additionally, I want to show my gratitude to all the faculties, employees and staffs for their continuous support. iv ABSTRACT Information System (IS) audit and consultancy has become a popular approach among fresh graduates and students. This report consists of a description of my work as an IS auditor in ACNABIN Chartered Accountants. This firm has 10 partners in total. I am completing my internship under our honorable partner sir Muhammad Aminul Haque, FCA and I was supervised by our honorable director Mr. A.N.M. Shakawath Hossain CISA, I have completed my internship program in this firm from 15th of May, 2022 to 15th of November, 2022. In this report I will describe each and every work that I have learnt and implemented during my internship program. v TABLE OF CONTENTS APPROVAL

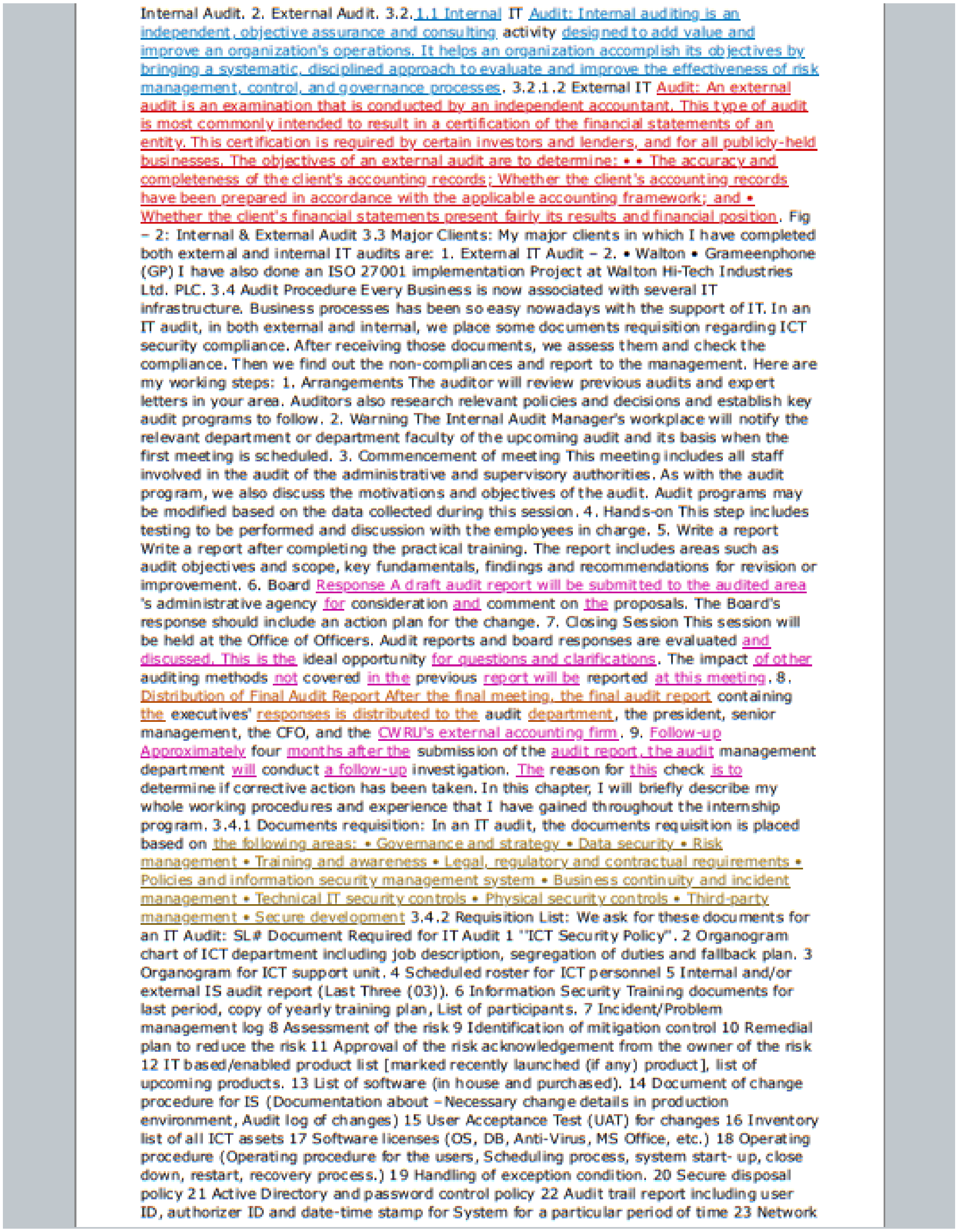


……… 12 3.4.5
Audit
Report……
19 4.
CONCLUSION……
20 REFERENCES

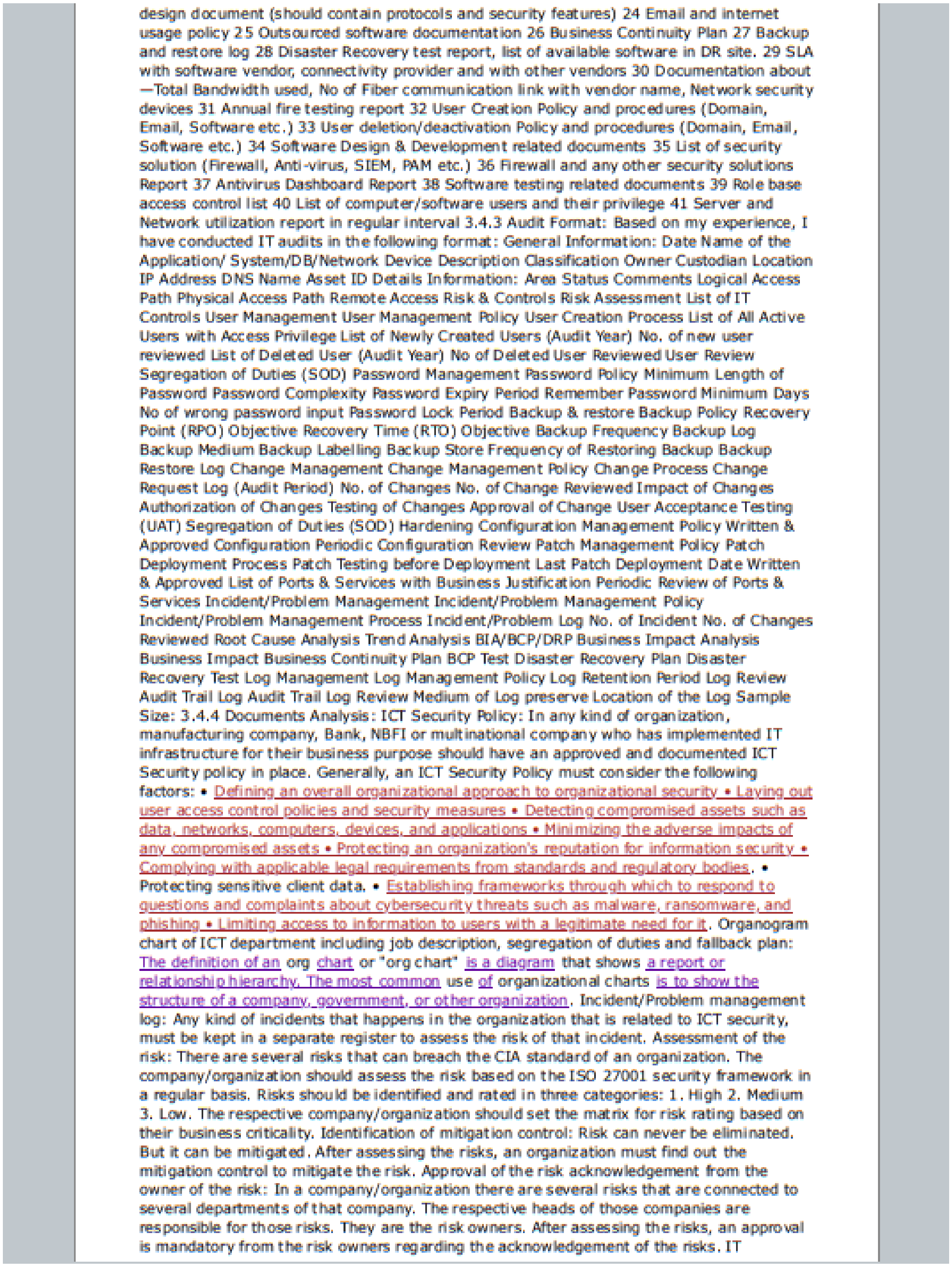
………
21 Plagiarism
Report……
Accounts Clearance

……
Library
Clearance……

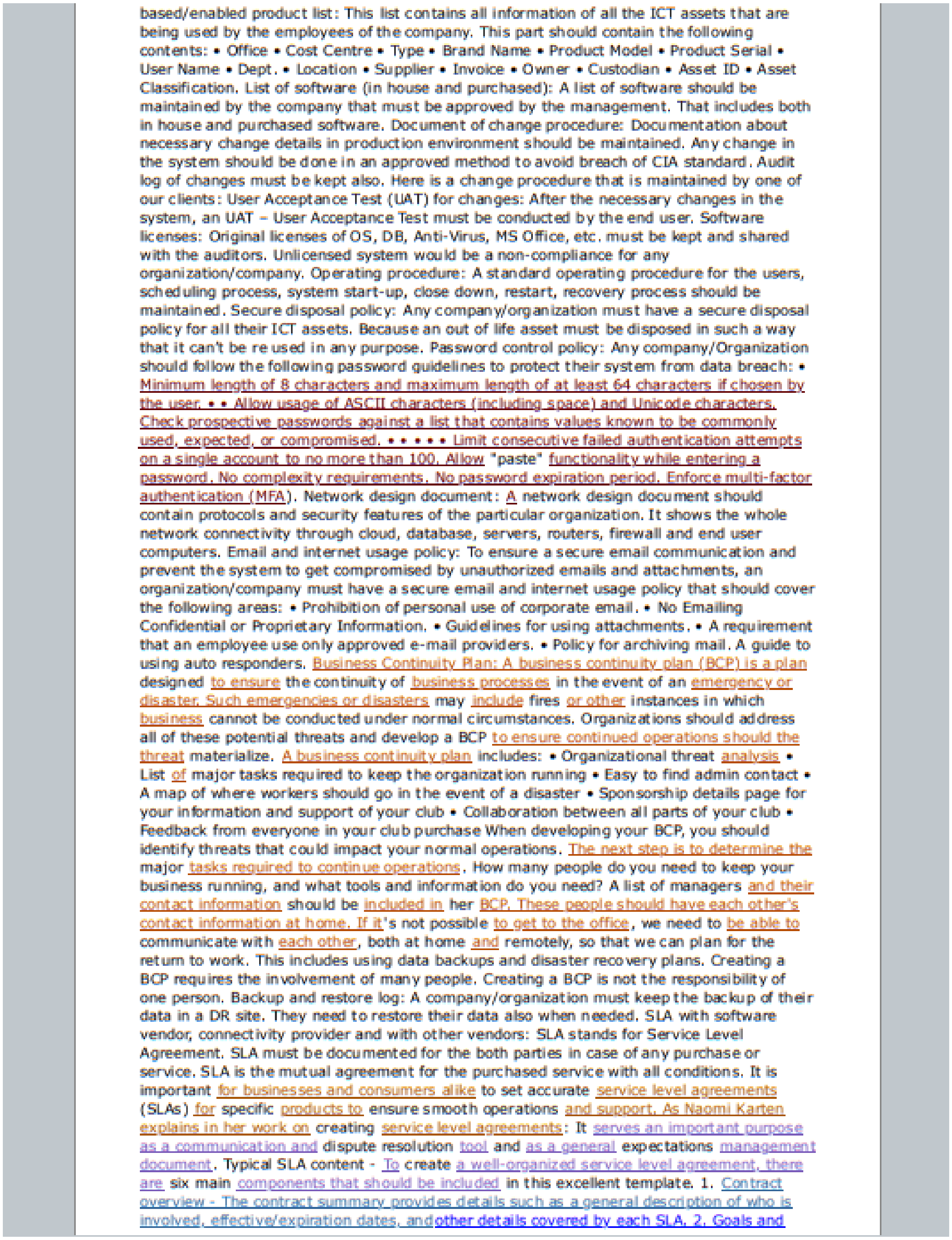
vi 1. INTRODUCTION 1.1 Objective: I have completed my 6 months internship program at ACNABIN Chartered Accountants as an IT Audit Intern. This internship report covers all the working experience that I have gained during my 6 months internship period. 1.2 Motivation: As I am a student of the Department of Software Engineering (Major in Cyber Security), Daffodil International University, I have decided to gain some industry experience based on my learnings for these four years. The primary reason to do the internship is to know cybersecurity in depth with industry best practices. Because it is not possible to cover everything and get industry experience in boundaries of academic curriculum. Another reason of choosing internship it helps me to face real life challenges like facing internal and external audit and doing consultancy with renowned organizations. I have completed "Information System Audit & Assurance Course" under major in cybersecurity. That's why I have chosen ACNABIN Chartered Accountants where I can work independently as an external and internal IS auditor. 1.3 Internship Goals: 1. Conducting IT audits through different cybersecurity framework. 2. Doing cybersecurity consultancy. 3. Doing validation according to the framework requirements. 4. Provide report of the final assessment. 5. Knowing sensible data concerning security Audit and Assurance. 6. Gain information regarding IT tools and software that is vastly used in the industry. 7. Develop analytical and technical skills. 8. Develop professional skills with ethics and values. 2. COMPANY INFORMATION 2.1 Introduction about the Firm: ACNABIN is one of the largest accounting firms relying on Baker Tilly International as a free institutional sub-firm in Bangladesh providing Security, Tax, Business Advisory Management, Information Systems Audit and Security ensuring the highest quality. Initiating the process in 1985, the law firm has been one of the most competent and trusted law firms for business networks and associated partners. At ACNABIN, we measure performance based on the value our customers and partner's demand. Approximately 500 professionals with diverse knowledge and skills work continuously in all business areas to serve our valued customer base. ACNABIN is a sponsored business of Baker Tilly International that focuses on more than just truly raising appreciation. To understand what the customer needs. We not only meet fast requirements, but also make long-distance arrangements. Respond to customer needs and proactively address future challenges. ACNABIN was founded in February 1985 with a mission to continually enhance our reputation by helping our clients succeed. In the long term, he has grown to be one of the most important and reputable contract accounting firms in Bangladesh. Our culture is driven by the Baker Tilly Internal core values: 1. To lead by example 2. To deliver quality services with integrity 3. To communicate openly, to act ethically 4. And to foster a community built around civic responsibilities and teamwork. We are passionate about helping our clients, while at the same time developing our people's potential. 2.2 Vision: We go beyond the traditional auditor and client relationship by becoming your Trusted Business Advisor. 2.3 Mission: We adhere to the strictest principles of client confidentiality. The sensitive and competitive nature of proprietary information and the maintenance of trust-demands it. We have built our success on such principles. We do our utmost to earn and keep client trust. 2.4 Core Services: • IT Audit • Audit and Assurance • Tax and Legal Advice • Advisory • Cyber security consultancy • ISO 27001 implementation. 2.5 Organizational Structure: Partner Director Associate Director Admin Manager Supporting Staff Deputy Manager Senior Assistant Manager Assistant Manager Fig – 1: Organogram Chart of ACNABIN CA 3. WORKING PROCEDURE 3.1 Introduction: This portion will reflect my works and experiences that I have gathered during my internship period in ACNABIN Chartered Accountants as an IT auditor and cybersecurity consultant. During this period, I have supervised by Mr. A.N.M. Shakawath Hossain, CISA, CISO the Director of IT at ACNABIN Chartered Accountants. 3.2 Overview: During this internship period, I have conducted eight IT audit in eight different clients which includes Banks, Non-Banking Financial Institutes, Manufacturing Company, Hospitals and Power generation companies and group of companies. 3.2.1 Types of IT Audit There are two types of audits that is conducted by our firm. I have completed several projects that are following: 1.



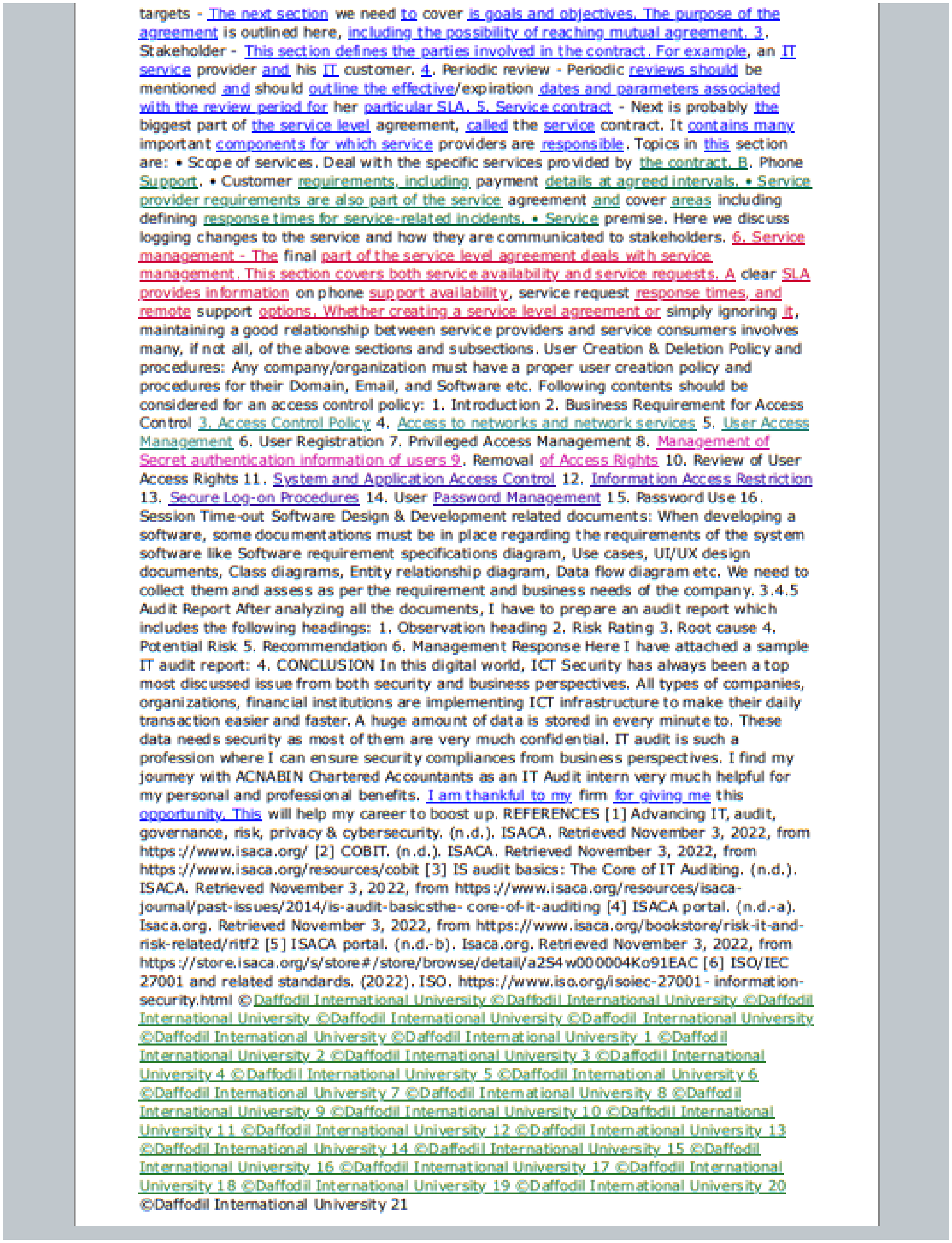
Internal Audit. 2. External Audit. 3.2.1.1 Internal IT Audit: Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. 3.2.1.2 External IT Audit: An external audit is an examination that is conducted by an independent accountant. This type of audit is most commonly intended to result in a certification of the financial statements of an entity. This certification is required by certain investors and lenders, and for all publicly-held businesses. The objectives of an external audit are to determine: • • The accuracy and completeness of the client's accounting records; Whether the client's accounting records have been prepared in accordance with the applicable accounting framework; and • Whether the client's financial statements present fairly its results and financial position. Fig – 2: Internal & External Audit 3.3 Major Clients: My major clients in which I have completed both external and internal IT audits are: 1. External IT Audit – 2. • Walton • Grameenphone (GP) I have also done an ISO 27001 implementation Project at Walton Hi-Tech Industries Ltd. PLC. 3.4 Audit Procedure Every Business is now associated with several IT infrastructure. Business processes has been so easy nowadays with the support of IT. In an IT audit, in both external and internal, we place some documents requisition regarding ICT security compliance. After receiving those documents, we assess them and check the compliance. Then we find out the non-compliances and report to the management. Here are my working steps: 1. Arrangements The auditor will review previous audits and expert letters in your area. Auditors also research relevant policies and decisions and establish key audit programs to follow. 2. Warning The Internal Audit Manager's workplace will notify the relevant department or department faculty of the upcoming audit and its basis when the first meeting is scheduled. 3. Commencement of meeting This meeting includes all staff involved in the audit of the administrative and supervisory authorities. As with the audit program, we also discuss the motivations and objectives of the audit. Audit programs may be modified based on the data collected during this session. 4. Hands-on This step includes testing to be performed and discussion with the employees in charge. 5. Write a report Write a report after completing the practical training. The report includes areas such as audit objectives and scope, key fundamentals, findings and recommendations for revision or improvement. 6. Board Response A draft audit report will be submitted to the audited area 's administrative agency for consideration and comment on the proposals. The Board's response should include an action plan for the change. 7. Closing Session This session will be held at the Office of Officers. Audit reports and board responses are evaluated and discussed. This is the ideal opportunity for questions and clarifications. The impact of other auditing methods not covered in the previous report will be reported at this meeting. 8. Distribution of Final Audit Report After the final meeting, the final audit report containing the executives' responses is distributed to the audit department, the president, senior management, the CFO, and the CWRU's external accounting firm. 9. Follow-up Approximately four months after the submission of the audit report, the audit management department will conduct a follow-up investigation. The reason for this check is to determine if corrective action has been taken. In this chapter, I will briefly describe my whole working procedures and experience that I have gained throughout the internship program. 3.4.1 Documents requisition: In an IT audit, the documents requisition is placed based on the following areas: • Governance and strategy • Data security • Risk management • Training and awareness • Legal, regulatory and contractual requirements • Policies and information security management system • Business continuity and incident management • Technical IT security controls • Physical security controls • Third-party management • Secure development 3.4.2 Requisition List: We ask for these documents for an IT Audit: SL# Document Required for IT Audit 1 "ICT Security Policy". 2 Organogram chart of ICT department including job description, segregation of duties and fallback plan. 3 Organogram for ICT support unit. 4 Scheduled roster for ICT personnel 5 Internal and/or external IS audit report (Last Three (03)). 6 Information Security Training documents for last period, copy of yearly training plan, List of participants. 7 Incident/Problem management log 8 Assessment of the risk 9 Identification of mitigation control 10 Remedial plan to reduce the risk 11 Approval of the risk acknowledgement from the owner of the risk 12 IT based/enabled product list [marked recently launched (if any) product], list of upcoming products. 13 List of software (in house and purchased). 14 Document of change procedure for IS (Documentation about – Necessary change details in production environment, Audit log of changes) 15 User Acceptance Test (UAT) for changes 16 Inventory list of all ICT assets 17 Software licenses (OS, DB, Anti-Virus, MS Office, etc.) 18 Operating procedure (Operating procedure for the users, Scheduling process, system start- up, close down, restart, recovery process.) 19 Handling of exception condition. 20 Secure disposal policy 21 Active Directory and password control policy 22 Audit trail report including user ID, authorizer ID and date-time stamp for System for a particular period of time 23 Network



design document (should contain protocols and security features) 24 Email and internet usage policy 25 Outsourced software documentation 26 Business Continuity Plan 27 Backup and restore log 28 Disaster Recovery test report, list of available software in DR site. 29 SLA with software vendor, connectivity provider and with other vendors 30 Documentation about —Total Bandwidth used, No of Fiber communication link with vendor name, Network security devices 31 Annual fire testing report 32 User Creation Policy and procedures (Domain, Email, Software etc.) 33 User deletion/deactivation Policy and procedures (Domain, Email, Software etc.) 34 Software Design & Development related documents 35 List of security solution (Firewall, Anti-virus, SIEM, PAM etc.) 36 Firewall and any other security solutions Report 37 Antivirus Dashboard Report 38 Software testing related documents 39 Role base access control list 40 List of computer/software users and their privilege 41 Server and Network utilization report in regular interval 3.4.3 Audit Format: Based on my experience, I have conducted IT audits in the following format: General Information: Date Name of the Application/ System/DB/Network Device Description Classification Owner Custodian Location IP Address DNS Name Asset ID Details Information: Area Status Comments Logical Access Path Physical Access Path Remote Access Risk & Controls Risk Assessment List of IT Controls User Management User Management Policy User Creation Process List of All Active Users with Access Privilege List of Newly Created Users (Audit Year) No. of new user reviewed List of Deleted User (Audit Year) No of Deleted User Reviewed User Review Segregation of Duties (SOD) Password Management Password Policy Minimum Length of Password Password Complexity Password Expiry Period Remember Password Minimum Days No of wrong password input Password Lock Period Backup & restore Backup Policy Recovery Point (RPO) Objective Recovery Time (RTO) Objective Backup Frequency Backup Log Backup Medium Backup Labelling Backup Store Frequency of Restoring Backup Backup Restore Log Change Management Change Management Policy Change Process Change Request Log (Audit Period) No. of Changes No. of Change Reviewed Impact of Changes Authorization of Changes Testing of Changes Approval of Change User Acceptance Testing (UAT) Segregation of Duties (SOD) Hardening Configuration Management Policy Written & Approved Configuration Periodic Configuration Review Patch Management Policy Patch Deployment Process Patch Testing before Deployment Last Patch Deployment Date Written & Approved List of Ports & Services with Business Justification Periodic Review of Ports & Services Incident/Problem Management Incident/Problem Management Policy Incident/Problem Management Process Incident/Problem Log No. of Incident No. of Changes Reviewed Root Cause Analysis Trend Analysis BIA/BCP/DRP Business Impact Analysis Business Impact Business Continuity Plan BCP Test Disaster Recovery Plan Disaster Recovery Test Log Management Log Management Policy Log Retention Period Log Review Audit Trail Log Audit Trail Log Review Medium of Log preserve Location of the Log Sample Size: 3.4.4 Documents Analysis: ICT Security Policy: In any kind of organization, manufacturing company, Bank, NBFI or multinational company who has implemented IT infrastructure for their business purpose should have an approved and documented ICT Security policy in place. Generally, an ICT Security Policy must consider the following factors: • Defining an overall organizational approach to organizational security • Laying out user access control policies and security measures • Detecting compromised assets such as data, networks, computers, devices, and applications • Minimizing the adverse impacts of any compromised assets • Protecting an organization's reputation for information security • Complying with applicable legal requirements from standards and regulatory bodies. • Protecting sensitive client data. • Establishing frameworks through which to respond to questions and complaints about cybersecurity threats such as malware, ransomware, and phishing • Limiting access to information to users with a legitimate need for it. Organogram chart of ICT department including job description, segregation of duties and fallback plan: The definition of an org chart or "org chart" is a diagram that shows a report or relationship hierarchy. The most common use of organizational charts is to show the structure of a company, government, or other organization. Incident/Problem management log: Any kind of incidents that happens in the organization that is related to ICT security, must be kept in a separate register to assess the risk of that incident. Assessment of the risk: There are several risks that can breach the CIA standard of an organization. The company/organization should assess the risk based on the ISO 27001 security framework in a regular basis. Risks should be identified and rated in three categories: 1. High 2. Medium 3. Low. The respective company/organization should set the matrix for risk rating based on their business criticality. Identification of mitigation control: Risk can never be eliminated. But it can be mitigated. After assessing the risks, an organization must find out the mitigation control to mitigate the risk. Approval of the risk acknowledgement from the owner of the risk: In a company/organization there are several risks that are connected to several departments of that company. The respective heads of those companies are responsible for those risks. They are the risk owners. After assessing the risks, an approval is mandatory from the risk owners regarding the acknowledgement of the risks. IT



based/enabled product list: This list contains all information of all the ICT assets that are being used by the employees of the company. This part should contain the following contents: • Office • Cost Centre • Type • Brand Name • Product Model • Product Serial • User Name • Dept. • Location • Supplier • Invoice • Owner • Custodian • Asset ID • Asset Classification. List of software (in house and purchased): A list of software should be maintained by the company that must be approved by the management. That includes both in house and purchased software. Document of change procedure: Documentation about necessary change details in production environment should be maintained. Any change in the system should be done in an approved method to avoid breach of CIA standard. Audit log of changes must be kept also. Here is a change procedure that is maintained by one of our clients: User Acceptance Test (UAT) for changes: After the necessary changes in the system, an UAT – User Acceptance Test must be conducted by the end user. Software licenses: Original licenses of OS, DB, Anti-Virus, MS Office, etc. must be kept and shared with the auditors. Unlicensed system would be a non-compliance for any organization/company. Operating procedure: A standard operating procedure for the users, scheduling process, system start-up, close down, restart, recovery process should be maintained. Secure disposal policy: Any company/organization must have a secure disposal policy for all their ICT assets. Because an out of life asset must be disposed in such a way that it can't be re used in any purpose. Password control policy: Any company/Organization should follow the following password guidelines to protect their system from data breach: • Minimum length of 8 characters and maximum length of at least 64 characters if chosen by the user. • • Allow usage of ASCII characters (including space) and Unicode characters. Check prospective passwords against a list that contains values known to be commonly used, expected, or compromised. • • • • • Limit consecutive failed authentication attempts on a single account to no more than 100. Allow "paste" functionality while entering a password. No complexity requirements. No password expiration period. Enforce multi-factor authentication (MFA). Network design document: A network design document should contain protocols and security features of the particular organization. It shows the whole network connectivity through cloud, database, servers, routers, firewall and end user computers. Email and internet usage policy: To ensure a secure email communication and prevent the system to get compromised by unauthorized emails and attachments, an organization/company must have a secure email and internet usage policy that should cover the following areas: • Prohibition of personal use of corporate email. • No Emailing Confidential or Proprietary Information. • Guidelines for using attachments. • A requirement that an employee use only approved e-mail providers. • Policy for archiving mail. A guide to using auto responders. Business Continuity Plan: A business continuity plan (BCP) is a plan designed to ensure the continuity of business processes in the event of an emergency or disaster. Such emergencies or disasters may include fires or other instances in which business cannot be conducted under normal circumstances. Organizations should address all of these potential threats and develop a BCP to ensure continued operations should the threat materialize. A business continuity plan includes: • Organizational threat analysis • List of major tasks required to keep the organization running • Easy to find admin contact • A map of where workers should go in the event of a disaster • Sponsorship details page for your information and support of your club • Collaboration between all parts of your club • Feedback from everyone in your club purchase When developing your BCP, you should identify threats that could impact your normal operations. The next step is to determine the major tasks required to continue operations. How many people do you need to keep your business running, and what tools and information do you need? A list of managers and their contact information should be included in her BCP. These people should have each other's contact information at home. If it's not possible to get to the office, we need to be able to communicate with each other, both at home and remotely, so that we can plan for the return to work. This includes using data backups and disaster recovery plans. Creating a BCP requires the involvement of many people. Creating a BCP is not the responsibility of one person. Backup and restore log: A company/organization must keep the backup of their data in a DR site. They need to restore their data also when needed. SLA with software vendor, connectivity provider and with other vendors: SLA stands for Service Level Agreement. SLA must be documented for the both parties in case of any purchase or service. SLA is the mutual agreement for the purchased service with all conditions. It is important for businesses and consumers alike to set accurate service level agreements (SLAs) for specific products to ensure smooth operations and support. As Naomi Karten explains in her work on creating service level agreements: It serves an important purpose as a communication and dispute resolution tool and as a general expectations management document. Typical SLA content - To create a well-organized service level agreement, there are six main components that should be included in this excellent template. 1. Contract overview - The contract summary provides details such as a general description of who is involved, effective/expiration dates, andother details covered by each SLA. 2. Goals and



targets - The next section we need to cover is goals and objectives. The purpose of the agreement is outlined here, including the possibility of reaching mutual agreement. 3. Stakeholder - This section defines the parties involved in the contract. For example, an IT service provider and his IT customer. 4. Periodic review - Periodic reviews should be mentioned and should outline the effective/expiration dates and parameters associated with the review period for her particular SLA. 5. Service contract - Next is probably the biggest part of the service level agreement, called the service contract. It contains many important components for which service providers are responsible. Topics in this section are: • Scope of services. Deal with the specific services provided by the contract. B. Phone Support. • Customer requirements, including payment details at agreed intervals. • Service provider requirements are also part of the service agreement and cover areas including defining response times for service-related incidents. • Service premise. Here we discuss logging changes to the service and how they are communicated to stakeholders. 6. Service management - The final part of the service level agreement deals with service management. This section covers both service availability and service requests. A clear SLA provides information on phone support availability, service request response times, and remote support options. Whether creating a service level agreement or simply ignoring it, maintaining a good relationship between service providers and service consumers involves many, if not all, of the above sections and subsections. User Creation & Deletion Policy and procedures: Any company/organization must have a proper user creation policy and procedures for their Domain, Email, and Software etc. Following contents should be considered for an access control policy: 1. Introduction 2. Business Requirement for Access Control 3. Access Control Policy 4. Access to networks and network services 5. User Access Management 6. User Registration 7. Privileged Access Management 8. Management of Secret authentication information of users 9. Removal of Access Rights 10. Review of User Access Rights 11. System and Application Access Control 12. Information Access Restriction 13. Secure Log-on Procedures 14. User Password Management 15. Password Use 16. Session Time-out Software Design & Development related documents: When developing a software, some documentations must be in place regarding the requirements of the system software like Software requirement specifications diagram, Use cases, UI/UX design documents, Class diagrams, Entity relationship diagram, Data flow diagram etc. We need to collect them and assess as per the requirement and business needs of the company. 3.4.5 Audit Report After analyzing all the documents, I have to prepare an audit report which includes the following headings: 1. Observation heading 2. Risk Rating 3. Root cause 4. Potential Risk 5. Recommendation 6. Management Response Here I have attached a sample IT audit report: 4. CONCLUSION In this digital world, ICT Security has always been a top most discussed issue from both security and business perspectives. All types of companies, organizations, financial institutions are implementing ICT infrastructure to make their daily transaction easier and faster. A huge amount of data is stored in every minute to. These data needs security as most of them are very much confidential. IT audit is such a profession where I can ensure security compliances from business perspectives. I find my journey with ACNABIN Chartered Accountants as an IT Audit intern very much helpful for my personal and professional benefits. I am thankful to my firm for giving me this opportunity. This will help my career to boost up. REFERENCES [1] Advancing IT, audit, governance, risk, privacy & cybersecurity. (n.d.). ISACA. Retrieved November 3, 2022, from https://www.isaca.org/ [2] COBIT. (n.d.). ISACA. Retrieved November 3, 2022, from https://www.isaca.org/resources/cobit [3] IS audit basics: The Core of IT Auditing. (n.d.). ISACA. Retrieved November 3, 2022, from https://www.isaca.org/resources/isaca-journal/past-issues/2014/is-audit-basicsthe- 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 ©Daffodil International University ©Daffodil International University ©Daffodil International University ©Daffodil International University ©Daffodil International University ©Daffodil International University ©Daffodil International University 1 ©Daffodil International University 2 ©Daffodil International University 3 ©Daffodil International University 4 ©Daffodil International University 5 ©Daffodil International University 6 ©Daffodil International University 7 ©Daffodil International University 8 ©Daffodil International University 9 ©Daffodil International University 10 ©Daffodil International University 11 ©Daffodil International University 12 ©Daffodil International University 13 ©Daffodil International University 14 ©Daffodil International University 15 ©Daffodil International University 16 ©Daffodil International University 17 ©Daffodil International University 18 ©Daffodil International University 19 ©Daffodil International University 20 ©Daffodil International University 21