Daffodil International University

Submitted by

Sadrin Rahman Bhuiyan Piya
192-15-13269
Department of CSE
Daffodil International University

Supervised by

Professor Dr. Touhid Bhuiyan
Professor & Head
Department of CSE
Daffodil International University

This Project report has been submitted in fulfillment of the requirements for the

Degree of

Bachelor of Science in Computer Science Engineering

INTERNSHIP REPORT

ON

STANDARD IMPLEMENTATION (ISO 27001, SWIFT & PCI DSS)

By

Sadrin Rahman Bhuiyan Piya
ID: 192-15-13269

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised by

Professor Dr. Touhid Bhuiyan
Professor & Head
Department of CSE
Daffodil International University

Co-Supervised by

Ms. Most. Hasna Hena
Assistant Professor
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

18 APRIL 2023

APPROVAL

This Project titled “Standard Implementation (ISO 27001, SWIFT & PCI DSS)”, submitted by Ms. Sadrin Rahman Bhuiyan Piya and to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 18 April 2023

BOARD OF EXAMINERS

2/5/23

Chairman

Dr. Touhid Bhuiyan
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Ms. Subhenur Latif
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Mr. Abbas Ali Khan
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

External Examiner

Dr. Shamim H Ripon
Professor
Department of Computer Science and Engineering
East West University

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Professor Dr. Touhid Bhuiyan, Professor & Head, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

2/5/23

Professor Dr. Touhid Bhuiyan
Professor & Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Submitted by:

Piya

Sadrin Rahman Bhuiyan Piya
ID: 192-15-13269
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, I express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project successfully.

I really grateful and wish our profound our indebtedness to **Professor Dr. Touhid Bhuiyan**, **Professor & Head**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of “STANDARD IMPLEMENTATION (ISO 27001, SWIFT & PCI DSS)” to carry out this project. Her endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete this project.

I would like to express our heartiest gratitude to Mr. Dr. Touhid Bhuiyan, Head of CSE Head, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

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

Finally, I must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

The implementation of standard frameworks is essential to ensure the security and compliance of an organization's information technology infrastructure. Three widely recognized frameworks are ISO 27001, SWIFT, and PCI DSS.

ISO 27001 is a globally recognized standard that outlines the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It provides a systematic approach to managing sensitive company information, protecting it from unauthorized access, and ensuring the confidentiality, integrity, and availability of the data.

SWIFT, or the Society for Worldwide Interorganizational Financial Telecommunication, is a network that facilitates secure financial transactions between organizations worldwide. It is crucial that SWIFT users implement the necessary controls to protect against fraudulent transactions, and SWIFT has developed a security framework that outlines these controls.

PCI DSS, or the Payment Card Industry Data Security Standard, is a set of security standards established by major credit card companies to protect against payment card fraud. It requires organizations that handle payment card information to implement specific controls to ensure the security of the data.

Implementing these standards can help organizations to protect their sensitive data, mitigate risks, and demonstrate compliance with regulatory requirements. However, implementation can be complex and time-consuming, requiring a dedicated team with appropriate skills and resources.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Introduction

As a portion of the Internship of Undergraduate program of BSc in Computer Science & Engineering (CSE) at Daffodil International University (DIU), I interned in the Security Department of “Right Time Limited” (RightTime, short form). Internships are often very closely related to the student's academic and career goals which help me to gain knowledge about the job field. I continuously had an interest in Cyber Security and thus my internship in a Cyber Security specialist company Right Time Limited was a magnificent opening for me, this report is based on cyber security standard implementation.

1.2 Rational

Undoubtedly, an internship can provide invaluable experience and exposure to different industries, enabling interns to build their workplace confidence, etiquette, and habits. The knowledge gained through an internship can also count towards undergraduate applied or technical elective credits. By participating in an internship, students can enhance their theoretical knowledge and develop practical problem-solving skills. As I reflect on my own internship experience, I recognize the significance of bridging the gap between theoretical knowledge and practical involvement. This has challenged me to think differently and has provided a deeper understanding of the lessons learned in my academic coursework.

1.3 Background

As a student at Daffodil International University (DIU), I have been fortunate enough to have the opportunity to complete an internship as part of my Bachelor's program. Studying Computer Science & Engineering (CSE) has given me a strong foundation in this field over the past three years. Cybersecurity is the practice of protecting computer systems, networks, and data from cyber-attacks through the use of technology, processes, and controls. This includes cyber laws, penetration testing, programming, cryptography, and more, all of which are crucial to preventing cyber-attacks.

During my internship at RightTime, I had the opportunity to expand my knowledge and skills in different areas of cybersecurity, such as Security Operations Center (SOC) analysis, Vulnerability Assessment and Penetration Testing (VAPT), Digital Forensics, and Firewall Installation. Although the journey was challenging, I discovered a new potential within myself as I faced new technologies and barriers.

As part of my role, I was primarily focused on implementing and preparing organizations for certification under various industry standards, such as ISO 27001 - Information Security Management System (ISMS), SWIFT - The Society for Worldwide InterOrganization Financial Telecommunication, and Payment Card Industry Data Security Standard (PCI DSS). It was a rewarding experience to contribute towards achieving these certifications for our clients.

1.4 Motivation

One of the main purposes of pursuing an internship is to gain practical experience and further enhance my knowledge beyond what can be taught in the academic curriculum. As the Executive for Information Security, I have already covered a lot of ground that was previously challenging for me. However, I recognize that there is always more to learn, and an internship provides the perfect opportunity to gain additional insights and experience in the field.

In addition to increasing my knowledge, another key motivation for pursuing an internship is to build the necessary skills to tackle real-world challenges. Throughout my internship, I have been fortunate to work under the guidance of an experienced supervisor who has provided me with opportunities to work on complex projects and exposed me to real-life situations. This hands-on experience has been invaluable in building my confidence and equipping me with the practical skills required to succeed in the industry.

I am grateful for the opportunity to apply the theoretical knowledge gained through my academic coursework to real-world scenarios. This has allowed me to see the practical applications of the concepts I have learned and provided me with a deeper understanding of the industry. Overall, my internship experience has been a truly enriching and rewarding experience that has further solidified my passion for information security and cybersecurity

1.5 Objectives

Overall, the objectives of implementing these standards are to improve information security, protect sensitive data, and mitigate the risk of cyber threats, data breaches, and other security incidents that could harm the organization's reputation, financial stability, and overall success.
The objectives of implementing the ISO 27001, SWIFT, and PCI DSS standards are as follows:

ISO 27001: The objective of implementing ISO 27001 is to establish a systematic and risk-based approach to managing sensitive information and protecting it from unauthorized access, disclosure, or misuse. It aims to ensure the confidentiality, integrity, and availability of information by implementing a comprehensive set of controls and best practices.

SWIFT: The objective of implementing SWIFT is to ensure secure and reliable financial messaging between financial institutions worldwide. It aims to protect against fraudulent activity, such as unauthorized access to financial messaging systems, data breaches, and other cyber threats.

PCI DSS: The objective of implementing PCI DSS is to ensure that all organizations that accept, process, store, or transmit credit card information maintain a secure environment that protects cardholder data. It aims to reduce the risk of data breaches, fraud, and theft by implementing a set of controls and best practices for securing cardholder data.

The other important purposes are as follows –

- Collaborating with the development manager to perform SOC analysis and digital forensic investigations.
- Participating in company development meetings and providing valuable insights on security-related matters.
- Adhering to ethical principles when working with confidential data and promoting a culture of confidentiality within the team.
- Conducting in-depth analysis of phishing emails to identify potential threats and vulnerabilities.
- Conducting Vulnerability Assessment and Penetration Testing (VAPT) to identify and address potential security weaknesses.
- Using password cracking techniques to test the strength of passwords and improve security measures.
- Responsively addressing requests and inquiries from the security assessment team to ensure timely and effective threat response.

1.6 Report Layout

- In chapter one, I talked about the introduction, why I wanted to do this internship, types of technologies that I want to learn and my objective.
- In chapter two, I gave a description of the company where I did my internship, described their market situation, products and made a SWOT analysis.
- In chapter three, I talked about my roles, daily tasks, tools, and technologies that I used, as well as a project that I started.
- In chapter four, I discuss my current competencies, challenges, and solutions. In chapter five, I concluded this report and discussed the future scope.

CHAPTER 2

INTERNSHIP ORGANIZATION

2.1 About

RightTime is a leading cyber security and managed IT firm that offers consultation and services to businesses of all sizes. They recognize that every organization, regardless of its size, requires a comprehensive cyber security program. Their team of experienced security experts is committed to delivering cutting-edge business cyber security solutions and services. RightTime's solutions safeguard businesses by protecting their employees, customers, facilities, and operations from both internal and external threats. Their approach enables businesses to work smarter through advanced security and information management solutions.

2.2 Company Profile

Right Time Limited ("RightTime", short form) has started its journey in the year 2009 (It is serving for 13^{+} years) with the motto "together we make the world happier". It's purely an Information Security Consultation (Information Security Management Standard – ISMS), Auditing (IS Security Graded Audit, Forensic Audit, Vulnerability Assessment & Penetration Testing, Data Center & Disaster recovery Site Audit), RightTime provide Custom Skill Development Training/ Workshop (Specially Information Security & Cyber security), Project Management (mainly ITES, e.g. End to End Solutions for building Security Operation Center - SOC and Centralized Forensic Solutions etc.), Technical Documentation (end to end) and Providing Service in the area of Information System Governance, Risk Management, Compliance etc. Provider and assist for Various ISO Consultation & Accreditation/Certification (e.g. ISO 27001, ISO 20000, ISO 9001, ISO 22301, ISO 27005, ISO 1400 etc.). RightTime support for CMMI Certification. It directly providing Information Security Related Services e.g. PCI DSS (Payment Card Industry Data Security Standard) Compliance Consultation (e.g. Preparatory Consultation, Gap Analysis, Remediation Support, Technical Documentation etc.) & Audit Services (Compliance Audit). Further to this, it do SWIFT Assessment and Consultation Services.

RightTime is the first formally enlisted Information System Auditing Firm (specialized in Information security) of the Controller of Certifying Authority under the Ministry of Information & Communication Technology (ICT), Govt. of Bangladesh. It is Internationally Registered Vendor of World Organization Group (VIN: 140663) for Information System Solutions, Consultation and Assurance (auditing) services etc. It is the member of “Bangladesh

Association of Software and Information Services” (BASIS). It has partnership with EC-Council (Security Training) and Pearson Vue (online approved computer testing center).

And for ISO Consultation & Accreditation/Certification- It is the partner of Canadian, UK and US based ISO Certification Company. Besides, It is permitted to perform SWIFT consultation and Audit Services. It is worth mentioning that Right Time is the first Bangladesh based Internationally Recognized/Registered Security Service Provider i.e. PCI QSA (Payment Card Industry Qualified Security Assessor) since 2013 by PCI SSC (Payment Card Industry Security Standard Council, USA).

RightTime are sound in Information System Documentation (Policy, process, standard creation /improvement), Information Security Consultation, Skill Developing (various IS/ IT related training etc.), Preparatory Consultation for various ISO/ BS certification (i.e. ISO 27001, 9001, 14000, 20000, etc.), Software Audits and Software Development Life Cycle and comprehensive Information System Audit (i.e. Network Vulnerability Assessment, Security Threat Evolution Penetration Testing, Forensic Audit etc.).

IT give emphasis in regard to mapping of ICT Act 2006 (Amendment in 2009), requirement of regulatory body i.e. Central Organization e.g. ICT Security Guideline Version 3.0 published May 2015 by Central Organization (Bangladesh Organization)etc. and use ISO/ BS, International Register of Certificated Auditors (IRCA), Control Objectives for Information Technology (COBIT), Infrastructure Library for Information Technology (ITIL), Institute of Internal Audit (IIA) Information System Audit and Control Association (ISACA) etc. framework and follow our ISecGrade methodology for designing and directing the mentioned service(s). You may check the following link for an easy understanding http://www.righttime.biz.

Our Value Proposition:

Information is the lifeblood of organizations, a vital business asset in today's IT-enabled world. Information Systems and networks link every internal department and connect us with a myriad of suppliers, partners and markets. Access to high-quality, complete, accurate and up-to-date information makes managerial decision-making relatively easy by reducing the margin for error. RightTime do give guarantee to access your high-quality information by designing and building information systems that are effective at gathering, analyzing and outputting the information you need; and RightTime also secure your information systems against risks to their confidentiality, integrity, availability (CIA) and reliability of information.

Collaborate communication approach:

Our team is committed to a collaborative relationship based on transparent, timely and proactive communication. Pour Unsurpassed Organizationing and IT Experience allows us to identify the most important issues you will be facing earlier than anyone else. This knowledge, combined with our collaborative culture, means your organization and we (RightTime) can identify and resolve issue together, before they become problems, and in fact we expect that frequently we can offer solutions that help prevent issues from arising.

Transparent consultation process:

There will be no walls between your organization and us (RightTime) during the technical consultation Process, Including with our Main Office. We respect to be involved early in the Process as complex technical Issues and transaction arise. organization will always
have a seat at the table, form issue identification through resolution.

Commitment to continuous improvement:

We will contribute to the organization`s continuous improvement efforts by providing relevant industry examples and bench mark, and by helping you achieve the maximum benefits. We will also focus in continuously improving our own service. We expect honesty and transparency form you about our performance, both in our national daily communication and in our formal Assessment of service Quality process

Right Time Limited has a vendor neutral approach in the market. We do not have any tie-ups or understanding with any vendors or implementation partner. This provides our clients with the assurance that the advice we provide is unbiased and in their interests.

Tools and Methodology:

Right Time Limited has some of the most comprehensive Licensed & Custom Tools and Database that our professionals use in their engagements. The content is reviewed on a regular basis by a Research and Development (R&D) team and is of significant value to our clients.

We will deliver on your requirements:

Based on the information and clarification provided by you, we have customized our proposal in a way as to ensure significant efficiency, effective gains, and also help you into maintain a control framework over time while maintaining flexibility as your business changes.

You have highlighted your expectation in RFP. We know that we can help you achieve all that you envision- a business partnership, improved risk coverage, flexibility, cost-efficiency and the resources you need (and when and where you need them).

Our Strength/ Declaration of Competence:

We are competent and capable of piloting any organization both for ISO/ PCI SSC compliance and Information Systems Audits (Including Penetration Testing), sound in IT related skill development and also have hands on experience on project management for financial institutions, multinational companies and Government sector as well.

The technical team comprises qualified security consultants full and part time with experience ranging from 3 to 25 years in the field of networking and security. The range of security/software quality certification of our team is at par with world standards.

We are sound in Information System Documentation (Policy, process, standard creation

/improvement), Information Security Consultation, Skill Developing (various IS/ IT related training etc.), Preparatory Consultation for various ISO/ BS certification (i.e. ISO 27001, 9001, 14000, 20000, etc.), Software Audits and Software Development Life Cycle and comprehensive Information System Audit (i.e. Network Vulnerability Assessment, Security Threat Evolution Penetration Testing, Forensic Audit etc.).

We give emphasis in regard to mapping of ICT Act 2006 (Amendment in 2009), requirement of regulatory body i.e. Central Organization e.g. ICT Security Guideline Version 3.0 published May 2015 by Central Organization (Bangladesh Organization)etc. and use ISO/ BS, International Register of Certificated Auditors (IRCA), Control Objectives for Information Technology (COBIT), Infrastructure Library for Information Technology (ITIL), Institute of Internal Audit (IIA) Information System Audit and Control Association (ISACA) etc. framework and follow our ISecGrade methodology for designing and directing the mentioned service(s). You may check the following link for an easy understanding http://www.righttime.biz.

2.3 RightTime Private Limited Dept. Hierarchy

RightTime Private Limited is a multi-departmental organization that comprises the following departments:

1) **Customer Service Department**: This department is responsible for interacting with clients to provide them with information and resolve any inquiries or complaints they may have. Customer service representatives usually gather information over the phone.

2) **Accounting Department**: The accounting department provides financial support and accounting services to the organization. It maintains records of accounts payable and receivable, inventory, payroll, fixed assets, and other financial components. The department's accountants also audit the records of each department to determine the company's financial position and recommend cost-effective changes to run the organization efficiently.

3) **Management Department**: The management department oversees all operations and manages each department within the organization.

4) **Marketing Department**: The marketing department handles RightTime's promotional activities and provides after-sale services to clients.

5) **Cybersecurity Consulting and Assessment Department**: This department handles all cybersecurity-related technical work at RightTime. It comprises cybersecurity specialists who assess and advise on cybersecurity measures to protect the organization from cyber threats.

6) **Human Resources Department:** The HR department provides employee services, such as appointment letters, salary increments, rewards, and other requirements. It also manages job circulars, checks candidate CVs, and issues appointment letters to new hires.

2.4 Services of RightTime Private Ltd.

The Service delivery of RightTime is given as bullet form:

Industry we cover:

1. FIs - Organization & NBFI
2. Mobile &Telecommunications
3. Payment Gateways and Payment Processor
4. Educational Institutions
5. E-Commence & Retail Merchants
6. Insurance
7. IT and BPO Services
8. Health Care
9. Power Sector

Services/Domain Expertise:

1. Services

1) Consultation

- Information Security & Cyber Security Consulting
- Project Management

- Consultation on Shaping up DC & DRS
- Swift Cyber Security Consulting
- Technical Documentation On ITES

2) Auditing

- Information System Audit
- Information Technology Audit
- Information Security Graded Audit
- DC & DRS Auditing

3) Security Testing

- Vulnerability Assessment & Presentation Testing Services
- Digital Forensics
- Code Review
- Software Quality Assurance & Testing
- Swift CSP Independent Assessment

4) Certification

- PCI DSS Certification
- ISO 27001, ISO 9001, ISO 20000-1, ISO 22301, ISO 13485, ISO 5001, ISO 14001 etc.
- CMMI (Capability Maturity Model Integration)
- Tia 942 For Data Center
- GDPR Assessment
- HIPAA Assessment

5) Managed Service

- SOC as A Service
- Cloud App Monitoring as A Service
- MDR as A Service (Managed End Point Detection and Response)
- Managed Nextgen Firewall as A Service
- Vulnerability Assessment (VA) As A Service Penetration Testing (PT) As A Service DAM (Database Auditing & Management) as A Service

2. Solutions

1) Security assessment (VA & PT) Tools

- Burp Suite
- Net Sparker
- Tenable
- Acunetix
- Core Impact

2) Cyber Security Management & Visibility solutions

- SIEM
- Firewall (Especially Next Gen)
- Log Management
- Patch management
- Privilege Access Management (PAM)

3. Training

1) Assessment

- Certified Penetration Testing Professional (CPENT)
- Offensive Security Certified Professional (OSCP)
- Certified Information system Auditor (CISA)
- Computer Hacking Forensic Investigator (CHFI)
- GIAC Penetration Testing (GPEN)
- GIAC Web Application Penetration Testing (GWAPT)

2) Management

- Certified Ethical Hacking (CEH)
- Certified Disaster recovery Professional
- Certified Incident Handler (ECIH)
- Certified SOC Analyst (CSA)
- Certified Threat Intelligent Analyst (CTIA)
- Certified Information security Manager (CISM)
- Certified Information System Security Professional (CISSP)
- GIAC Certified Project Manager (GCPM)
- Open Source Intelligence (OSINT)

3) RightTime Customized

- Foundation track (Corporate)
- Network Defense and Operations (Corporate)
- Software Security (Corporate)
- Vulnerability Assessment & Penetration Testing (VA & PT)- (Corporate)
- Cyber Forensic - (Corporate)
- Governance - (Corporate)
- Certified Disaster recovery Professional
- Certified Incident Handler (ECIH)
- Certified SOC Analyst (CSA)
- Certified Threat Intelligent Analyst (CTIA)
- Certified Information security Manager (CISM)
- Certified Information System Security Professional (CISSP)
- GIAC Certified Project Manager (GCPM)
- Open Source Intelligence (OSINT)
- Governance - (Corporate)

2.5 Company Attestation with Valued Entities

Associations

Table 2.5.1: Associations

Sl No	Name of the Organization (Association)	Domain/Area
1	CCA, Ministry of ICT, Bangladesh	First and running empaneled Security Assessor/Audit Firm
2	PCI SSC (payment Card Industry Security Standard Council), USA	PCI DSS Compliance Validation Service (Scoping, Gap Analysis, Remediation Consultation, Compliance Audit etc.)
3	WBGs (World Organization Group)	Enlisted Security Assessor Firm – Vendor Identification Number (VIN): 140663
4	SWIFT (Society for Worldwide Interorganizational Financial Telecommunications)	RightTime is authorized to perform SWIFT CSP Independent Assessment (as SWIFT Listed Assessor). And also provides Cyber Security Consultation Services as listed SWIFT Cyber Security service Provider CSSP).
5	Bangladesh Association of Software and Services (BASIS), Bangladesh	General Member, ID: G591, (Representing Co Chairman, Digital Security)
6	E-Commerce Association of Bangladesh (e-CAB), Bangladesh	General Member, ID: 787

Partners

Table 2.5.2: Partners

Sl No	Name of the Partnership	Domain/Area
1	EC-Council (International Council of E-Commerce Consultants), USA	Approved Training Center (ATC) [world's largest certification body for Information Security professionals]
2	Pearson Vue, UK	Approved Online Testing Center. [it is the global leader in computer-based testing for IT, academic, government and professional programs]
3	PECB - ISO Certification (and others) (Canadian Based)	Approved partner [Affiliation with: IAS-US, IAAR-US, IPC-Germany, Club Ebios-France, Credential Engine-US]
	ARS/SCK - ISO Certification (and others) (Indian Based)	Business Association [Affiliation with: ANAB-US, CNAS-China, RvA-Netherland, UKAS-England (UK)]
4	ACNABIN, Bangladesh	Partnership with Financial Assessment/ Audit firm for financial control validation (if any) [Member of ICAB – {Institute of Chartered Accountants of Bangladesh), Bangladesh]
5	Security Assessment & Management Tools Invicti (Acunetix & Net Sparker), Tenable Partner (Vulnerability Assessment & Management) HelpSystems: Core Impact (reseller), PortSwigger (Burp Suite)	Security Tools/Application Partnership

2.6 Certified Pool in various Domain of IS/IT:

Table 2.6.1: Certified Pool

Certifications	
CISSP, CISA, CISM, CGEIT, CRISC	PCI QSA, PCIP, C|EH, C|HFI, CSCF, ECSA, LPT, CEI
Swift Certified Professional	Core Professional, Buirp Suite Pro, Nessus Pro, Acunetix Pro
BCP & DRP, IS Audit, CSCF (Cyber Security Cyber Forensic)	RHCE, RHCT, IBM-AIX-CS, IBM-AIX, SCSA, HP-UX-CSA, RHL EX-423, RHL EX-429, VSG Video Solution, Polycom VSG Video Solution Technical, Polycom Voice Over IP [VoIP]
CDCE, CTDC, CDCS, CDCP	
ISO Lead Auditor: ISO 20000, ISO 27001, ISO 9001 Lead Implementer: ISO 27001	SCSECA, SCNA, SCSA, OCP, OCE, MCITP, MCITP, MCTS (Lync, Virtualization, Exchange, SharePoint, HPC), ITIL V3,
Blockchain Certified Professional	CIPM® – Certified International Project Manager, MPM® – Masters Project Manager, PRINCE2
CCNA, JNCIA, JNCIS, CND, CCNA Cyber Ops, CCNP	

2.7 Our Mission (Goal):

Our mission is to protect our clients' digital assets and ensure their business continuity by providing comprehensive cyber security solutions. We aim to stay ahead of the constantly evolving threat landscape and leverage the latest technologies to deliver effective and efficient services to our clients. We strive to build long-term relationships with our clients based on trust, transparency, and superior performance, and to be recognized as a trusted partner in their digital transformation journey.

2.8 Our Moto:

"Together we make the world happier".

2.9 Our Philosophy

We believe that cyber security is a critical component of every organization's success, and we are committed to empowering our clients to protect their valuable digital assets. We believe in taking a proactive and holistic approach to cyber security, leveraging cutting-edge technologies and best practices to mitigate risks and prevent threats. We believe in building a strong partnership with our clients, understanding their unique needs and challenges, and working collaboratively to develop customized solutions that address their specific requirements. Above all, we believe in honesty, integrity, and transparency, and strive to maintain the highest standards of professionalism in all our interactions.

2.10 Our People

Expert human resource is a key element in Right Time Limited’s success. Our professionals possess the knowledge and expertise to develop effective solutions that safeguard clients' digital assets. They are updated with the latest trends and threats in the industry and possess excellent communication and problem-solving skills. People at Right Time Limited ensures delivery of top-notch services to its clients and maintains a competitive edge in the market.

2.11 Clients

For running a software company client are primary components all of the time. As a cyber security consulting and assessor firm, RightTime has a part of local and international clients. Our company tries to extend our client’s number.

IFC (WBGs)-Dhaka Custom House, Bangladesh Organization Limited, Sonali Organization Limited, Agrani Organization Limited, Rupali Organization Limited, Bangladesh Police, AL-Arafah Islami Organization Limited, Shahjalal Islami Organization Limited, NRB Organization Limited, Mutual Trust Organization Limited, Meghna Organization Limited, South Bangla Agriculture Organization Limited, IFIC Organization Limited, NRBC Organization Limited, Padma Organization Limited, SSF, Ministry of ICT (CCA & SKHTPA), Index IT Limited, Advance System Technologies, DohaTech Newmedia Limited, Mango Teleservices Limited, Data Edge, New Horizon Computer Learning Center, Dhurbo Ltd, Transparency International Bangladesh (TIB), Naya Diganta, CloudWell, Foster Corporation, Walletmix, SmartDate, ADDIE Soft Limited, Genweb2, Circle Fintech BD Limited, Shurjomukhi Limited, InfoSec Solutions and Japan Bangladesh Group.

2.12 Company Information

Level: 06 & 14 (west) BDBL Bhaban,
12 Kawran Bazar, Tejgaon, Post Code: 1215, Dhaka, Bangladesh
Phone: +880 2 55012235, Fax: +880 2 55012235
Email: info@righttime.biz

CHAPTER 3

Company Culture and Carrying Out

3.1 Working Environments and Protocols

The working environment is a crucial factor in achieving a thriving career. I am fortunate to work in an office with an exceptional working environment, where my colleagues are all delightful to work with. Each individual has their own designated personal area, which contributes to a sense of privacy and comfort. Additionally, our company provides essential amenities that make our work experience even better.

3.2 Working Team

To ensure the timely completion of projects, each department has established collaborative working groups. Recognizing that the workload cannot be handled by a single individual, an experienced employee who has previously worked in that department is assigned to lead the team. Our employees work cohesively as a team, leveraging each other's strengths and expertise to achieve our goals

3.3 Rules & Regulations

3.3.1 Office Time

Our company's standard office hours are from 9:00 AM to 6:00 PM, which includes a designated break time for both lunch and snacks. We encourage all employees to take their breaks to ensure they have sufficient time to recharge and refresh themselves during the day. Additionally, we require all employees to arrive on time to ensure the smooth operation of our daily routines and to avoid any unnecessary delays or interruptions to our work processes. Punctuality is critical, as it ensures that we meet our deadlines and maintain our high standards of productivity.

3.3.2 Responsibilities

- Every employee is responsible for their designated tasks, and it is crucial to take ownership and be accountable for their work. In addition to this, there are a few extra responsibilities that we take seriously:

- Tools and equipment are essential to our daily work. Any carelessness with these items can cause harm or damage to office property. Therefore, it is essential to handle them with care to prevent any accidents or mishaps.

- If any significant loss or damage to company property occurs, it must be reported immediately to the relevant authorities. This helps us take corrective action and prevent similar incidents from happening in the future.

- We value personal boundaries and expect everyone to respect their colleagues' belongings and privacy. Personal things must not be touched without permission.

- Employees are required to obtain permission from their group leader before taking time off from work. This ensures that our work processes are not hampered, and our projects remain on track.

- In the event of an emergency, employees must inform the CEO or their supervisor as soon as possible. This enables us to take prompt action to ensure everyone's safety and well-being.

- By following these extra responsibilities, we can maintain a productive and safe work environment, ensuring that our daily operations run smoothly.

3.3.3 Meeting

Attending meetings on time is a crucial aspect of our work culture. It is mandatory for all employees to be punctual and attend meetings at the scheduled time. Our meetings are an opportunity to discuss the company's plans and goals and to provide updates on the progress of ongoing projects.

To make the most of our meetings, it is important to be prepared and engaged. This means coming equipped with relevant information and insights, actively participating in discussions, and taking notes to ensure that we have a clear understanding of what has been discussed.

Our meetings are an excellent platform for collaboration and teamwork, enabling us to leverage each other's expertise and strengths to achieve our goals. By being present and engaged in our meetings, we can ensure that we remain on track, and our projects remain aligned with our company's mission and vision.

3.4 Handling Clients

Customers are the most important component of every business. Each company has its unique approach to dealing with clients. Clients who handle operations are not the same as those who work for the company. Each company has its own approach to dealing with customers. RightTime Private Ltd focuses on the needs of the client. Where a non-technical person can comfortably do their task. This company collects customer requirements and is designed in such a way that anyone can quickly speed up their work. If the client has to change the company after deployment, the dynamic product does so quickly. As a result, the company gains customer satisfaction.

3.5 Comparative Analysis of Office Culture

The company provides internship opportunities. Instead of other companies, our country has a fantastic culture. They hire people who are compatible with the culture. The decision maker generates ideas from various sources. Realizing that I am not cut off from the company.

3.6 Internee Life Cycle

The internee life cycle based on a few criteria. There was a internee life cycle.

Here are six possible stages of internee life cycle under a cyber security service provider:

1) **Update Resume**: The first step is to update your resume to reflect your relevant skills and experience, as well as your interest in cyber security. This includes highlighting any coursework or certifications related to cybersecurity.

2) **Identify Internship:** Next, research and identify suitable internships in the cyber security industry. You may look for internships on job boards, company websites, or by reaching out to your network for referrals.

3) **Write Cover Letter:** Once you have identified a potential internship, write a targeted cover letter that highlights your relevant skills and experience, and why you are interested in working in the cyber security industry.

Apply and Interview: Apply for the internship, and prepare for the interview by researching the company and practicing your responses to common interview questions. During the interview, highlight your passion for cybersecurity and your eagerness to learn and contribute to the company.

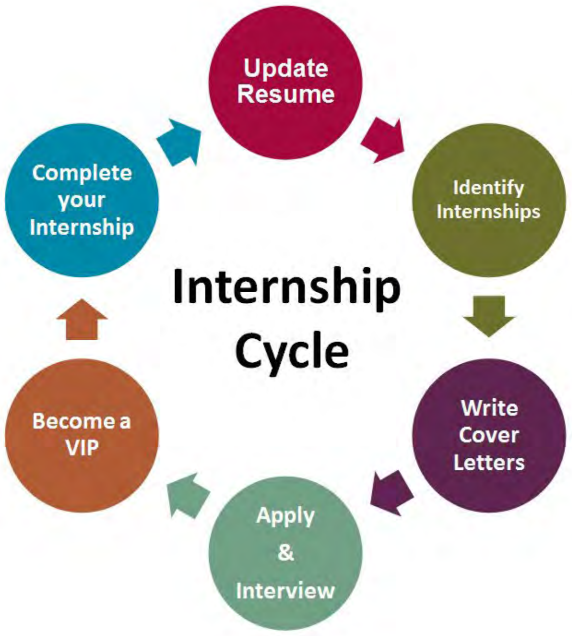


Figure 3.6.1: Internship Cycle

4) **Become a VIP**: If you are selected for the internship, the next stage is to become a valuable intern. This involves being proactive, asking questions, and taking on responsibilities. Demonstrate your willingness to learn, take feedback positively and show initiative in tackling challenging tasks.

5) C**omplete Your Internship**: Finally, complete your internship and reflect on your experiences. Use this opportunity to learn as much as you can about the industry, make connections, and gain practical experience. It is also essential to thank the company for the internship opportunity, and to stay in touch with your contacts in the company. This can be important if you wish to pursue a career in the cybersecurity field.

3.7 Recruiting Policies

RightTime has its own unique recruiting methods for selecting candidates for various positions. After submitting an online application for an internship position, I received a phone call for an interview. During the interview, the company representatives asked me questions related to my educational background, work experience, and interest in cybersecurity.

As a result of my qualifications and performance during the interview, I was offered the internship position. The company emphasizes selecting individuals who are motivated to learn and contribute to the success of the organization. If I perform well during my internship, there is a possibility of continuing work with the company.

Overall, it's important to note that each organization may have its own specific recruitment process depending on the position being filled. However, RightTime places a strong emphasis on selecting talented individuals who are motivated to learn and grow with the company.

3.8 Getting Started

Since beginning my internship at RightTime on July 01, 2022, I have gained valuable experience and learned a variety of cybersecurity skills. Over the last several months, I have been introduced to a new working environment, which has been extremely beneficial as I start my career in the IT industry. Additionally, I have had the opportunity to work on client sites, which has given me valuable real-world experience.

Through this internship, I have gained a better understanding of the specific tasks and responsibilities associated with a career in cybersecurity. This experience has been invaluable in helping me to determine my future career goals.

I am incredibly grateful for the opportunity to work as an intern at RightTime and am excited to continue developing my skills and knowledge in the field of cybersecurity.

CHAPTER 4

Technology Employing

4.1 Overview:

RightTime's one of the core services is Standard Implementation. Some of the standard is an already compliance for its nature (mandatory and noncompliance gets penalty) and some are best practice. The known standard which are given below:

4.2 Mostly used standards in Information Technology enabled Services Organizations:

4.2.1 Standards which became Compliance for specific industry:

- ISO 27001- Information Security management standard (ISMS)
- SWIFT CSP (Customer security Program) Independent Assessment (yearly).
- Payment Card Industry data security Standard (PCI DSS)

4.2.2 Standards which are strongly recommended but still are not under mandate/ compliance shade:

- ISO 9001- Quality Management System (QMS)- IT is said the mother ISO.
- ISO 20000 – Information Technology Management System (ITSM)
- ISO 14001- Environmental Management System (EMS)
- ISO 22301 – Business Continuity Management System (BCM)
- ISO 27005 – Risk management related to IS Security
- TIA 942- DC & Telecommunication Infrastructure related Certification.

4.3 My Task in Standard Implementation (ISO 27001, SWIFT & PCI DSS):

My involvement in the below Standard Implementation for which my job role mostly was as assistant to the security assessor/auditor. A short description of the project methodology, lifecycle towards standard certification, Technical Documentation needed for the individual certification which is treated as the administrative control of Business Continuity management System is briefly shared/included in the subsequent section.

4.3.1 ISO 27001 - Information Security management standard (ISMS)

4.3.1.1 Training on ISO 27001

Professional Group: IT Security, IT Systems & IT Operations, Audit and Management

a. Awareness cum Implementation Training

- Number of Delegates: xx Staff officers of Customer/Client
- Number of Batch: in xx batch(s)
- Duration of the Course: xx day- xx hours

b. **Lead Auditor (LA), ISO 27001:2022, Information Security Management Standards (ISMS):** Information Security and International Standards, Information System Security Requirements, Security Policy, Security Organization, Asset Classification and Control, Personnel Security, Physical and Environmental, Security, Communication and Operations Management, Access Control, System Development and Maintenance, Business Continuity Management, Compliance, Identification of ISO 27001 Controls.

Use: Any organization that is using IT (Information Technology) as the delivery and processing backbone requires a stable and secured system. Often it is found that the organizations end up patronizing vendor based technical solution. The ISMS define the domains of security requirement of an organization and allows them to take a structure approach to management of IT Risk. The ISMS forms the layer under which the technology layer must operate and be monitored. Besides, for getting official recognition on Information System Security Grade- ISO 27001, individual, departments and the total organization should know total process of ISMS and this awareness training shall act as extra boosting in the confidence level.

Duration: 40 Hours (05 Days)

Number of Participants: xx

Framework to Follow/ Curriculum: Latest curriculum of IRCA (International Register of Certificated Auditors) with Certification (IRCA Body) will be followed.

c. **Lead Implementer (LI), ISO 27001:2013, Information Security Management Standards (ISMS):** Information Security and International Standards, Information System Security Requirements, Security Policy, Security Organization, Asset Classification and Control, Personnel Security, Physical and Environmental, Security, Communication and Operations Management, Access Control, System Development and Maintenance, Business Continuity Management, Compliance, Identification of ISO 27001 Controls.

Use: Any organization that is using IT (Information Technology) as the delivery and processing backbone requires a stable and secured system. Often it is found that the organizations end up patronizing vendor based technical solution. The ISMS define the domains of security requirement of an organization and allows them to take a structure approach to management of IT Risk. The ISMS forms the layer under which the technology layer must operate and be monitored. Besides, for getting official recognition on Information System Security Grade- ISO 27001, individual, departments and the total organization should know total process of ISMS and this awareness training shall act as extra boosting in the confidence level.

Duration: 40 Hours (05 Days)
Number of Participants: 02
Framework to Follow/ Curriculum: Latest curriculum of IRCA (International Register of Certificated Auditors) with Certification (IRCA Body) will be followed.

4.3.1.2 End-end- Preparatory consultation and Certification

ISO certification not only ensures quality of the product and its reliability in the eyes of its consumers, but boosts sale and ensures promise of a business enterprise it will push you closer to the top of the list when in competition with other companies to get a certain customer or client. ISO Certification provides a basic fundamental for customer satisfaction globally.

Within the service scope, we – RightTime shall provide Preparatory Consultation Services for achieving the organizational Accreditation on the below ISO -

1) Information Security Management Standard (ISMS), ISO 27001 – Preparatory Consultation for ISO 27001 (security) Certification for Organization. And consultation will be extended for:

- Initial Certification
- Certificate Maintenance Year 01
- Certificate Maintenance Year 02
- Recertification after 03 years cycle

ISO 27001 (Information System Security) Implementation Consulting Service:

ISO 27001 is one of the most popular international standards published by ISO. Adopted from its earlier form BS 7799, a British standard, ISO published it as ISO 27001 in 2005, in 2013 version 27001:2013. Today it is in its 4th edition e.g. ISO 27001:2022.

ISO 27001 offers a framework for developing an Information Security Management System (ISMS) for an organization that wants to protect its information assets from all possible risks. Any type of an organization can refers to this framework and develop its own information security management system. Once all applicable requirements are addressed, the organization can get this information security management system certified from a third-party certification body.

Area/Domain: Gap Analysis, ISMS Awareness and Implementation Training, Domain Analysis /Control Area Analysis, Process Documentation for Client, Document Review, Training Material Development, Provide Training to Client, Implementation Support, Risk Assessment (Asset Risk Assessment), Training on Asset Risk Assessment (Tool Development), ISO 27001 Internal Audit Training,

Business Continuity Planning / Disaster Recover Planning, Verification and Testing of BCP and DRP, Readiness Check (Pre-Audit), Get the client certified by the Certification Body, Certification Retention, Compliance Monitoring (on regular intervals e.g., after one or two months. An ongoing activity).

Use: Most organizations develop an information security management system because

- There is a need to assure their customers that the organization has appropriate processes, systems and practices in place to ensure confidentiality, integrity and availability of information. A certification to ISO 27001 will provide that confidence to the organization's customers.

- The organizations need to fulfil compliance needs in terms of applicable statutory and regulatory requirements pertaining to privacy and data protection. An application of ISO 27001 offers a framework to the organization where such statutory and regulatory requirements are addressed within the internal control mechanism.

ISO 27001 helps the organizations build a complete model in order to assure protection of information assets as well as for meeting compliance needs.

Applicability: The ISO 27001 standard applies to all types of organizations including commercial organizations, non-profit organizations, Governments, Educational Institutes, NGOs, Financial Institute(s) e.g. Organization etc.

Technical Documentation.

Technical Documentation (Interface Between User and Machine):

1) Making Documentation on Information System Security, Policies, Process & Standards etc. (covering IT Enabled Services - ITES). <u>More that 100 types of technical documentation</u> are needed for the achievement of IS0 27001

As part of Business Continuity as well as second line of protection, organization has decided for documenting ("Technical Documentation") of its all-Information Technology Enabled Services (ITES). And for meeting this (<u>service in scope</u>) with reduced time frame and also decrease the man day, we RightTime, having core competence as well as similar expertise in assessing/ evaluating and assisting a technical team (from service taking organization) is proposing for preparing "Technical Documentation" of IT Enable Service (ITES) of the organization.

Policy & Process Review

Prior to assisting making necessary Technical Document(s) we shall review the stated documents and there after based on the prioritization approach we shall commence this scoped service.

The scope to include the following areas of operations and processes related to Information Technology:

<u>Policy Doc Table for ISO 27001</u>

Remediation Consultation Services (based on Gap Analysis Report of ISO effort):

At this stage we shall assist the ISO implementation team to remediate the gaps.

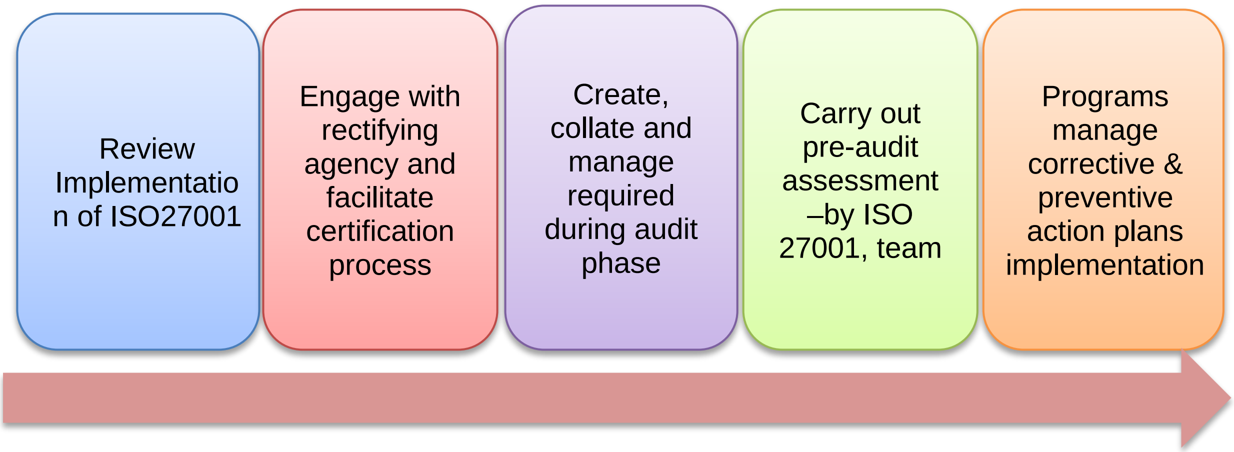

Review Implementatio n of ISO27001
Engage with rectifying agency and facilitate certification process
Create, collate and manage required during audit phase
Carry out pre-audit assessment –by ISO 27001, team
Programs manage corrective & preventive action plans implementation

Figure 4.3.1.2.1: ISO Stages

Scope

For all the ISO Accreditation Services, the scope will be Head office's Information Technology Division (including DC, DRS & Mobile Organizationing Infrastructure) .

ISO Accreditation/Certification

ISO 27001 - Information Security Management System (ISMS): Arranging ISO Accreditation Audit for Organization's certification. Scope: Initial Certification and Also Certificate maintenance (surveillance audit) for Year 01 and Year 02 after initial Certification.

After successful preparation, under the management of RightTime, external ISO Audit firm will conduct audit for clearing the organization for ISO Certification (if any). In this regard, ISO 27001

Scope

- Initial Certification
- Certificate Maintenance Year 01
- Certificate Maintenance Year 02
- Recertification after 03 years cycle

Deliverables

We shall first assess the existing environment, do a gap analysis then ensure the third-party audit, recommend against the observation, follow up the remedies by the organization and remain in the loop for ISO 27001Accreditation.

Time frame of the deliverables

1) The accreditation services will start within 30 days from the date of placing the order for the accreditation (ISO).
2) As per the service scope, the accreditation services will not be time bound. Being prepared rightly, after clearance from the auditee organization, third party audit must be completed by approximately 10-man days.
3) RightTime will engage ISO Audit firm and shall complete ISO Accreditation Audit latest by 04 calendar months i.e. 120 Days (treating the service starting day after the work order as the first day) for ISO 27001 certification.

4.3.2 SWIFT CSP Assessment based on CSCF – (Customer Security Control framework) 2023

4.3.2.1 SWIFT end-to-end consultation and assessment service.

4.3.2.1.1 Overview of SWIFT

The Society for Worldwide Interorganizational Financial Telecommunication, better known as SWIFT, is an organization founded in Brussels in 1973 with the aim of establishing common processes and standards for financial transactions worldwide. Used for the exchange of 37.7 million daily messages in 2020, with a growth of 10.3% compared to 2019, the SWIFT circuit counts in February 2023 the membership of more than 11,000 global institutions connected by 200 different countries.

4.3.2.1.2 SWIFT Reference Architecture

In order to guarantee proper levels of security throughout the circuit, member entities must

formally and periodically demonstrate that they have arrange, applied and maintained the necessary **security controls**, according to the reference architectures.

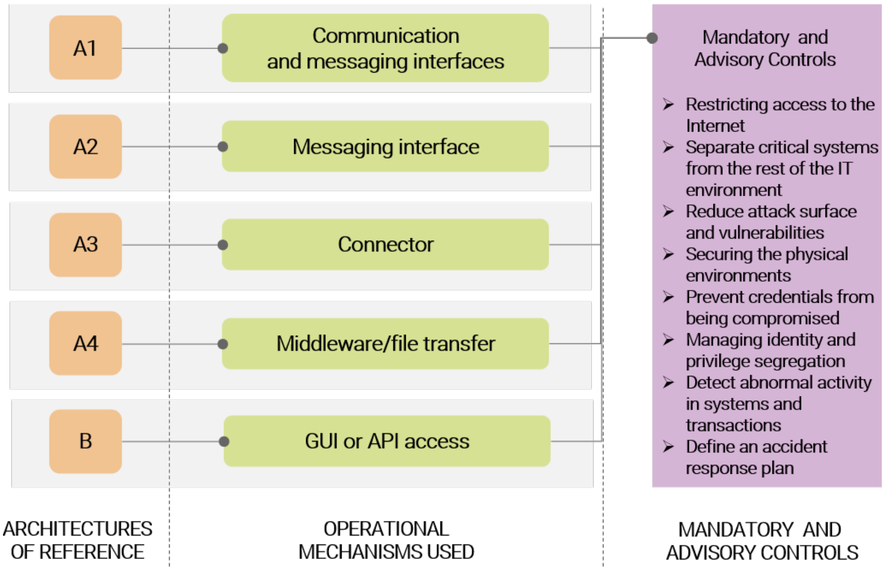

A1
Communication and messaging interfaces
A2
Messaging interface
A3
Connector
A4
Middleware/file transfer
B
GUI or API access
Mandatory and Advisory Controls
➢ Restricting access to the Internet
➢ Separate critical systems from the rest of the IT environment
➢ Reduce attack surface and vulnerabilities
➢ Securing the physical environments
➢ Prevent credentials from being compromised
➢ Managing identity and privilege segregation
➢ Detect abnormal activity in systems and transactions
➢ Define an accident response plan
ARCHITECTURES OF REFERENCE
OPERATIONAL MECHANISMS USED
MANDATORY AND ADVISORY CONTROLS

Figure 4.3.2.1.1: SWIFT Architecture

With the Customer Security Program (**CSP**), SWIFT classifies reference architectures through the identification of **interfaces**, **applications** and **tools**, specifying how different implementations can however be characterized by a substantial level of customization, compared to the groups identified below:

Table 4.3.2.1.1: SWIFT Architecture

SWIFT Architecture	Al	A2	A3	A4	B
Mandatory Controls	23	23	22	19	15
Advisory/Additional Controls	08	08	08	10	08
Total	**31**	**31**	**30**	**29**	**23**

4.3.2.1.3 Customer Security Program

Customer Security Controls Framework (CSCF) is an initiative process introduced by SWIFT to create a security baseline with set of Security controls which need to be implemented. SWIFT has introduced a core set of security controls that every SWIFT customer must implement. **Organization(s) need to implement the controls that are relevant to your organization, and attest your level of compliance before 32 December (end of) 2023**.

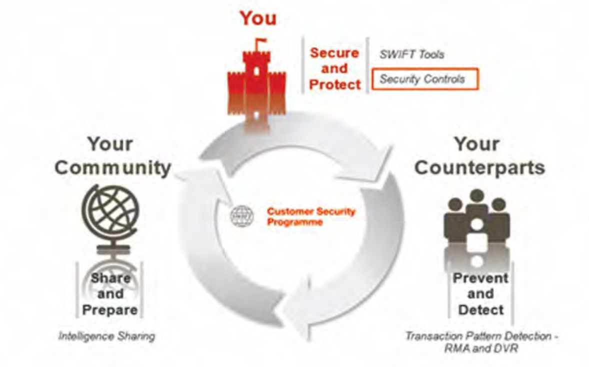


Figure 4.3.2.1.3.1: SWIFT CSP

The Customer Security Controls Framework (CSCF) describes a set of mandatory and advisory security controls for SWIFT users. The **Mandatory Security Controls** establish a security baseline for the entire community and <u>must be implemented by all users on their local SWIFT infrastructure</u>. **Advisory Security Controls** are additional security good practices that <u>SWIFT recommends</u> users to implement.

With the introduction of v.2023 of the CSCF, SWIFT has also published a timeline for members which provides a schedule for the introduction of changes to the framework and the reporting requirements. SWIFT member organizations will be expected to assess and implement these changes in accordance with the published timeline.

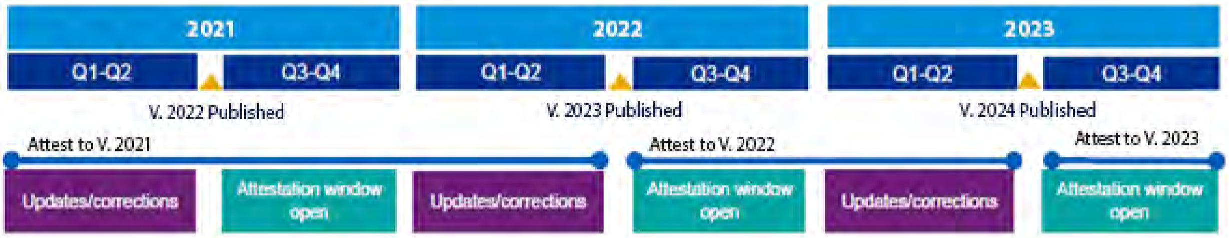


Figure 4.3.2.1.3.2: SWIFT Timeline

4.3.2.1.4 SWIFT Assessment Scope

The assessment of all mandatory controls as mentioned below and are applicable to the customer on the basis of their SWIFT architecture type and infrastructure is included in this assessment scope of activity. Advisory controls are not covered under this scope of assessment which should be separately dealt on mutual agreement.

High Level Scope: ICT Division, SWIFT Department. In addition, **we shall cover Head office and Main/Primary Information Processing Zone (Data Center) and DR Site as well.**

Table 4.3.2.1.4.1: SWIFT Mandatory Security Controls

Mandatory Security Controls (24) as per CSP 2023

Sl No	Control Name and Reference in SWIFT CSCF	Response
01	1.1 SWIFT Environment Protection	Shall Comply
02	1.2 Operating System Privileged Account Control	Shall Comply
03	1.3 Virtualization Platform Protection	Shall Comply
04	1.4 Restriction of Internet Access	Shall Comply
05	1.5 Customer Environment Protection	Shall Comply
06	2.1 Internal Data Flow Security	Shall Comply
07	2.2 Security Updates	Shall Comply
08	2.3 System Hardening	Shall Comply
09	2.6 Operator Session Confidentiality and Integrity	Shall Comply
10	2.7 Vulnerability Scanning	Shall Comply
11	2.9 Transaction Business Controls	Shall Comply
12	2.10 Application Hardening	Shall Comply
13	3.1 Physical Security	Shall Comply

Sl No	Control Name and Reference in SWIFT CSCF	Response
14	4.1 Password Policy	Shall Comply
15	4.2 Multi-factor Authentication	Shall Comply
16	5.1 Logical Access Control	Shall Comply
17	5.2 Token Management	Shall Comply
18	5.4 Physical and Logical Password Storage	Shall Comply
19	6.1 Malware Protection	Shall Comply
20	6.2 Software Integrity	Shall Comply
21	6.3 Database Integrity	Shall Comply
22	6.4 Logging and Monitoring	Shall Comply
23	7.1 Cyber Incident Response Planning	Shall Comply
24	7.2 Security Training and Awareness	Shall Comply

Advisory Security Controls (08) as per CSP 2023

Table 4.3.2.1.4.2: SWIFT Advisory Security Controls

Sl No	Control Name and Reference in SWIFT CSCF	Response
01	2.4A Back-Office Data Flow Security	Shall Comply
02	2.5A External Transmission Data Protection	Shall Comply
03	2.8A Critical Activity Outsourcing	Shall Comply
04	2.11A RMA Business Controls	Shall Comply
05	5.3A Staff Screening Process	Shall Comply
06	6.5A Intrusion Detection	Shall Comply
07	7.3A Penetration Testing	Shall Comply
08	7.4A Scenario Risk Assessment	Shall Comply

4.3.2.1.5 Standard Duration of the SWIFT Assessment

Table 4.3.2.1.5.1: SWIFT Assessment Duration

Task No	Particular	Time Period (Duration)
Task 1	Kick off and collection of information	1-7 Days
Task 2	Review of information collected such as former report, internal report and further collecting missing information (if any)	7-10 Days
Task 3	Technical Document review/formulation/fine tuning for SWIFT required docs.	20-30 Days
Task 4	Conducting Security Assessment (VA & PT)	15-20 Dyas
Task 5	Submission of Draft Report	10-15 Days after data collection (Task 2, Task 4)
Task 6	Draft Report Discussion (physical presence with audit-visual presentation)	1-2 Days
Task 7	Adjusting the findings and observation based on the Task 4 (if any)	1-3 Days
Task 8	Submission of Final Report	4-7 Days upon completion of task 5

4.3.3 Payment Card Industry data security Standard (PCI DSS)

4.3.3.1 Methodology and Approach

Overview

PCI DSS is a complex requirement that has an impact on most areas of the business, not just the technical or IT focused locations. Therefore, it is important to make sure that any methodology that is used to service the program has been tried and tested. The approach that Right Time Limited adopts for the PCI DSS program of works is as follows:

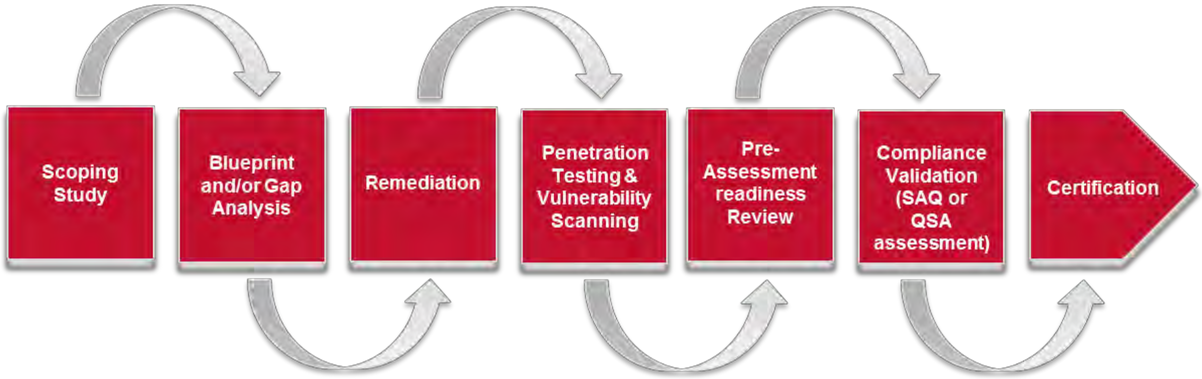

Scoping Study
Blueprint and/or Gap Analysis
Remediation
Penetration Testing & Vulnerability Scanning
Pre-Assessment readiness Review
Compliance Validation (SAQ or QSA assessment)
Certification

Figure 4.3.3.1: PCI DSS Workflow

The above picture is an outline of the total process and the drive through compliance.

We propose to offer following PCI DSS Compliance Consultation and Audit Services for Customer over the period of 1 year and subsequent year, if requested, in following phases:

Table 4.3.3.1.1: PCI Phases

Phase – I	:	Assessment
Phase – II	:	Remediation
Phase – III	:	Certify
Phase – IV	:	Maintain

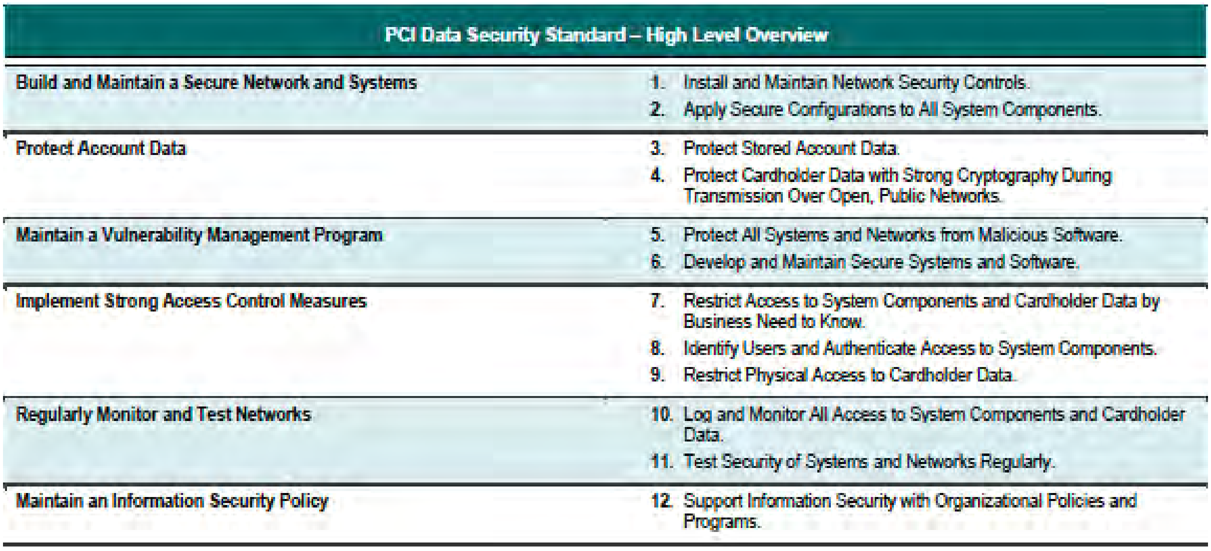
Service Offer

- **Compliance Validation Service (CVS) Includes:**
  - Remote Validation Service (Provided in Phase I, II and IV)
  - Onsite Validation Service (Provided in Phase III)
  - Remediation Guidance (provided in Phase II, III and IV)
  - External Vulnerability Scanning (Phase I)
  - Customer portal in RightTime web (provided throughout)
  - Trusted Commerce Security Seal (Provided in Phase III, once compliance is achieved)

- **Other Services to be Provided:**
  - External Vulnerability Scanning Service (Provided in Phase I, then monthly throughout)
  - PCI DSS Training

Compliance Validation Service (CVS) Domains

PCI DSS requires Customer to be compliant by showcasing evidence for the following requirements:



PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	1. Install and Maintain Network Security Controls. 2. Apply Secure Configurations to All System Components.
Protect Account Data	3. Protect Stored Account Data. 4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	5. Protect All Systems and Networks from Malicious Software. 6. Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	7. Restrict Access to System Components and Cardholder Data by Business Need to Know. 8. Identify Users and Authenticate Access to System Components. 9. Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	10. Log and Monitor All Access to System Components and Cardholder Data. 11. Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	12. Support Information Security with Organizational Policies and Programs.

Figure 4.3.3.2: PCI DSS Overview

We will provide customer with a Compliance Validation Service designed to help manage the overall compliance process and aid in achieving the compliance objectives.

Scope of CVS

Customer is one of the leading Organizations of Bangladesh having nationwide presence. The Organization has a nationwide distribution network of over 155 Outlet, 300 ATMs and over 3000 POS in the market.

The focus of our services will be on the cardholder data environment operations systems and processes within Customer. This environment is comprised of various applications which would also be in the scope.

The following table represents the estimated scope of the assessment. The Detailed Pricing schedule is based entirely on this estimation, therefore additional locations, devices, payment applications, 3rd party dependencies etc. will require an added cost set forth in an addendum hereto executed by both parties. It is assumed that Card Division of the Organization will have to certify.

External Vulnerability Scanning Service

We shall use automated vulnerability scanning engine compliant with the PCI Approved Scan Vendor (ASV) requirements. RightTime will provide monthly scans during the term of the agreement.

Scope of Service

Table 4.3.3.2.1: Service Scope

Description	Total
Number of Externally Facing IP Addresses	Up to 10

Training on PCI DSS

Onsite 2-day training program to 10 Brac Organization Limited officials on PCI DSS Compliance (Track 1, 2 and 3 of course details provided below) –

PCI DSS Compliance 2 (two) days training program developed for IT Professionals will provide a technical overview of the Payment Card Industry (PCI), its stakeholders, and the security measures taken to guarantee the security of payment card information globally. The course will benefit Brac Organization Limited officials that play a role in the processing, storage, availability, and protection of payment card data. The course explain payment card acceptance mechanism and sheds light on the inherent vulnerabilities and threat to payment card processing. Brac Organization Limited officials will learn the specific requirements for protecting payment card data as specified by the Payment Card Industry Data Security Standard (PCI DSS). The course will review each PCI DSS high level goal and all the associated security requirements and accepted minimum controls. The course will help prepare Brac Organization Limited official to plan and manage PCI DESS compliance validation process by breaking down a typical audit engagement into clear deliverables and phases.

PCI DSS training program is developed for senior executives, IT team members, legal team members, human resource managers, business function senior managers. The program will describe the PCI, PCI transaction and the need for the PCI DSS, explain the intent and compliance criteria behind the PCI requirements, identify PCI DSS compliance obligations and workflow and overview of the PIC DSS 6 goals/section and 12 requirements.

Training goals

Track 1 – Half day:

- Describe the PCI, PCI transactions and the need for the PCI DSS
- Understand the intent and compliance criteria behind the PCI requirements
- Identify PCI DSS compliance obligations and workflow
- Describe the PCI DSS 6 section/goals and 12 requirements

Track 2 – Half day:

- Identify PCI data risks and vulnerabilities and the associated data protection solutions
- Describe common strategies for segmenting data networks and controlling scope
- Describe the components a PCI DSS compliant ROC

Track 3 – Half day:

- Identify each PCI DSS security requirement and the accepted minimum controls to meet each requirement.

Detailed Project plan

PCI DSS Compliance Validation Services/ Consultation (CVS) consist of Project Initiation and four Compliance Validation Phases, and to ensure comprehensive and efficient service, the Brac Organization Limited (BBL) must fulfill their obligations within each phase before progressing to subsequent phases. Failure to do so may require an addendum to this contract that will include additional charges for any time or materials above and beyond those agreed in agreement/ Proposal.

- **Project Initiation Meeting**

We will commence the next stages of the project with an Initiation Meeting. The purpose of this meeting is to:

- Re-confirm the scope of the project and agree appropriate terms of reference, objectives and deliverables;
- Agree relevant contacts and reporting lines;
- Identify 3rd party providers;
- Agree appropriate timescales for delivery of the work;
- Obtain relevant documentation currently circulated within Brac Organization Limited
- Discuss any issues that need to be handled sensitively during the project;
- Any questions and answers.

- **PCI DSS Scoping Exercise**

For PCI DSS compliance it is necessary to include a scoping study exercise that establishes where card holder information is being processed, stored or transmitted by the organization. Typically in carrying out such a scoping exercise we would review the architecture, applications, business processes, and locations associated with card holder data for PCI DSS compliance at a high level. It is also important to identify any service providers and other third parties that are engaged by the organization who may also be processing card holder data on behalf of the service provider.

Fully understanding the PCI scope for an organization can be a complex issue that involves fact finding and research in order to:

- Ensure coverage of all card data flow channels and all external third parties and service providers that may be involved within them;
- Ensure that all applications, system and network elements within your IT infrastructure that store, process and transmit credit card related information are covered;
- Ensure that all relevant third party agreements held by Brac Organization Limited are included;
- Ensure that all external links into the IT infrastructure including remote user (or client) access are covered;
- In case non-compliance is discovered, to be able to provide a remediation plan that supports PCI DSS and adheres to best practice for information security.

By undertaking a scoping exercise at the beginning of the process you can be confident that the scope of the project has been correctly identified and reduced where possible. This will help to ensure that costs and resource requirements are kept to minimum moving forward.

At the end of the scoping exercise we will develop the report that may include ‘quick wins’ such as measures to descope the environment, for example via network segmentation. This is why we prefer to propose to conduct a scoping exercise and the gap analysis (addressed in the following section) as two separate steps of work.

- **Gap Analysis**

Following the completion of the scoping exercise, we will undertake a Gap Analysis against the applicable requirements of the PCI DSS. The Gap Analysis will be completed through means of a consultation process, comprising of one-to-one interviews and/or workshops with the key staff that will be confirmed during the project initiation meeting. Since the scoping exercise would have already been completed, you will be able to target the gap analysis more effectively.

The Gap Analysis is carried out against the PCI DSS Security Audit Procedures identifying areas of compliance, non-compliance, partial-compliance and non-applicability. All evidence and observations are collected at this stage to support the Gap Analysis Report and the Remediation Action Plan we will produce. Importantly, at this stage it will be identified where compensating controls may be required for your cardholder data environment(s) (areas where credit card and debit card data is processed either electronically or manually). Findings from these interviews will later on feed into the Gap Analysis report.

Consultation with the necessary employees is likely to include (but not be limited to):

- **IT Manager –** To gain an overview of systems that store, process and transmit payment card data, and of the main ways in which cardholder data is secured, such as use of encryption and access control;
- **Information Security –** To gain an understanding of the existing information security management processes and procedures in place;
- **Networks Support –** To understand the network topology, segregation and external links into the corporate IT network;

- **Finance Manager –** To ascertain which systems process and potentially store credit card information, in order to gain the business perspective on the use of cardholder data;
- **Physical Security Manager –** To gain an overall understanding of the arrangements for physical security of the IT installation, and in particular, the areas where cardholder data is accepted and transmitted;
- **Contact Centre Staff/ Customer Advisors –** To gain an understanding of the working practices of the staff who deal with credit card processing. We would seek to hold discussions with a sample of your staff who are working on client contracts that involve the processing of card transactions.

Note that one or more of the above roles may be fulfilled by one individual. We will confirm the exact individuals to be included and also a timetable for the relevant discussions during the project initiation phase. It is important that at this stage relevant staff are made available to the QSA but we understand how difficult it may be for the project stakeholders at Brac Organization Limited to identify and engage appropriate individuals. At the project initiation stage, the QSA will discuss what support. Right Time Limited can provide you with, to ensure that the required staff are made available with little or no disruption to business operations.

- **Gap Analysis Report and Remediation Action Plan**

On completion of the Gap Analysis activity, we will produce a report that states each of the PCI DSS controls and the level of compliance achieved by BBL. Observations and recommendations are included against all relevant requirements, providing guidance to those involved in reaching compliance against the Standard.

We will also produce a Remediation Action Plan outlining and prioritizing the work to be carried out and also the resource implications associated with this. We will aim at providing the most pragmatic remediation activities which will require the least disruption to BBL's business operation but will allow you to achieve compliance to PCI DSS.

On completion of the report, we will issue it to the project stakeholder for review and will address the questions should any arise. If necessary, amendments are made in the report following your review and its final version is submitted to you.

- **Remediation Consultancy**

Based on the Remediation Action Plan we produce, BBL will be required to carry out the remedial activities addressing the gaps. Many of our clients retain us as “trusted advisors” during this period to assist them with the remediation. We will be pleased to assist you at this stage if needed. As the degree of non-compliance is not yet known, we make no assumptions at this point with regards to the scope of work we can help you with. We typically assist clients in this phase of the program under the umbrella of a call off contract, delivering consultancy as and when required. A call-off contract is a convenient arrangement in this case since it gives the client freedom to access an appropriate consultant to address specific issues as they arise. Within the call-off contract, you will only be billed for the days utilized.

Examples of how we can assist you at this stage include:

- Development of the outstanding documentation currently not existing at BBL but required by PCI DSS;
- Validation and sign-off of compensating controls or identification of alternative ways to meet the intent of the PCI DSS requirements;
- Independent reviews of ASV and security testing reports;
- Supporting BBL to identify high-level options for minimizing the cost and risk associated with PCI DSS compliance;
- Holding direct contact with the card schemes on behalf of BBL;
- Holding regular progress reviews;
- Perform specific and focused audits of areas where further independent QSA investigation is required;
- Technical assistance e.g. design and configuration development or reviews (e.g. of voice solutions);

- Any other requirements that occur throughout the term of the project which can be addressed within the term of the call-off contract;
- Providing other specific technical and business resources from Right Time Limited when required.

- **PCI DSS Final Certification**

  Following the Remediation activities, when you are ready, we will carry out the final assessment and will issue a formal Report on Compliance (ROC) to confirm your compliance with the standard. This audit will be carried out against PCI DSS Version 3.0 of the standard and will involve detailed discussions with a similar range of individuals included in the gap analysis process and also the collection of evidence to support our findings.

- **Attestation of Compliance**

  Following the development of the ROC, an Attestation of Compliance (AOC) is completed and signed off by the QSA. This document is mandatory for PCI DSS and states your compliance status and provides a high-level of details on when and who performed an assessment. This document is presented to the card schemes for review.

Please note:

PCI DSS requires that organizations handling payment card data perform a full penetration test on their payment network at least once a year. This task is very important and ensures that any applications and/or their supporting networks are thoroughly tested for security weaknesses. It should not be confused with quarterly PCI scanning which offers a useful, but less comprehensive review of network security. This task is overlooked by some organizations and they do so at their peril. The requirement is in the PCI DSS for a very good reason; weaknesses in applications or the organization’s security perimeter can provide direct, and trusted, routes to the account data.

The cost of ASV scanning and penetration testing is quoted separately. Right Time Limited has most experienced penetration testing team, with excellent references from a variety of organizations including card vendors.

- **Project Management**

At Right Time Limited, we operate a robust account management process. And our expertise in the application of methodologies, standards and techniques including: PRINCE 2, PMP, ISO 20000, ISMS (ISO 27001), and ISO 9001 etc.

Our QSA and trained security experts will also support Brac Organization Limited throughout the CVS process, to support your internal efforts to gain compliance. This includes:

- **Managing Consultant** – RightTime will assign a Managing Consultant (MC) to oversee all assessment activities. The Managing Consultant is responsible for ensuring the quality of all RightTime deliverables and for the following:

- Identification and assignment of RightTime resources
- Communicating expectations and responsibilities to the assigned consultants
- Dissemination of information to internal RightTime resources
- Scheduling of Kickoff, status and closeout meetings
- Primary Point of Contact for escalations

- **Onsite Assessor or Global Compliance Service (GCS) Consultant –** We will assign a Global Compliance Service (GCS) consultant who is certified by the PCI SSC as a Certified Security Assessor (QSA). This is the individual who will conduct the onsite validation of compliance for the environment and will be responsible for the following:

- Scheduling and conducting onsite assessment activities
- Compilation of assessment data into the initial report
- Delivery of any report deliverables, unless otherwise specified

- **PCI Consultant –** We will assign a Remote Validation Service (RVS) Consultant who is certified by the PCI SSC as a Qualified Security Assessor (QSA). This is the individual who will conduct the remote collection of the pre-requisite scoping documentation and will be responsible for the following:
  - Collection of all onsite pre-requisite scoping documents, Network Diagram, Dataflow Diagram & Narrative, and the asset inventory
  - Collection of all Report on Compliance "Executive Summary" narrative
  - Collection of Policy and Procedure documentation

We follow up all of our assignments with Client Satisfaction Reviews and the results of these reviews are monitored at Board Level. In this, we are consistently exceeding our satisfaction target of 75% with most indicators scoring more than 90%.

All of the above is underpinned by a seldom-used and seldom necessary formal escalation procedure which allows any item of client dissatisfaction to be escalated to the Managing Consultant.

- **Timescales**

The scheduling process can begin within 7 (Seven) days of receiving the authorization to commence work. We understand you want to be certified by the end of December 2014 and this seems a sensible timeframe. We will do our utmost to help you in this respect but there are a number of external factors such as remediation requirements and third parties outside of our control which means we are unable to guarantee this.

4.4 Information System/ Information Technology (IS/IT) Security Assessment:

Additionally, I took part in performing Security Assessment i.e. Vulnerability assessment & Penetration Testing (VA & PT) as an assistant under the supervision of RightTime's Senior Security Analysts. I became acquainted with various licensed and authenticated open source for performing manual and automated security assessment i.e. VA &PT. Some of the tool's names are given below:

Below is the sample list of tools for Security Assessment (VA & PT and

Configuration & Code Review (if any).

According to ICT guideline (version 3.0) published by Bangladesh Organization, and PCI SSC (Payment Card Industry Security Standard Council), USA - quarterly Vulnerability Assessment and Annual Penetration Testing (at least) is a must. Besides, performing VA & PT just after any significant change(s) also a regulatory/compliance requirement for ITES organization e.g. Financial Institutions (Organizationing and non-organization) specially for entity with card data environment.

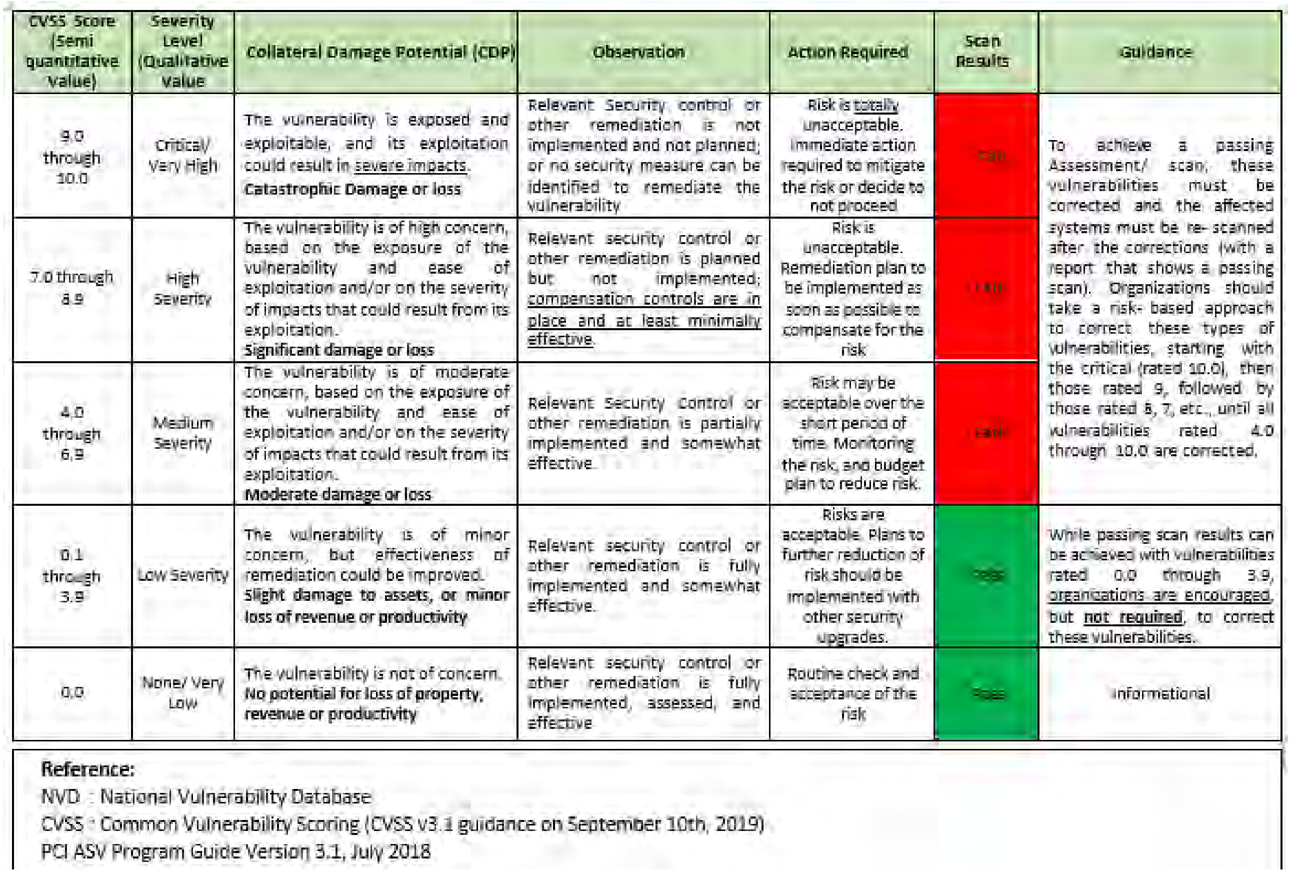
Automated as well as Manual Tools (Application Software) are needed to carry out Vulnerability Assessment and Penetration Testing. Besides our unique expertise with utmost pools of professionals, we use world class (most expensive) top rated licensed tools/application for finding more than **87,195** known vulnerabilities as well as unknown one and try to exploits the same. Not only that we also use different Branded VA & PT tools i.e. 02 VA & 02 PT for tally. Furthermore, use manual tools for further attestation of the findings and exploits. These has the Vulnerability Assessment Components and Penetration Testing Functional Areas coverage of Central Organization i.e. Bangladesh Organization as well as PCI DSS by PCI SSC (Payment card Industry security Standard Council), USA.

Please see next page

Risk Scoring as per NVD (National Vulnerability Database) & CVSS (Common Vulnerability scoring system)

Figure 4.4.1 NVD Scoring System

We take prior approval from the relevant authority of the client before using any application/tools in client's ITES (IT enabled Services) Infrastructure.



CVSS Score (Semi quantitative value)	Severity Level (Qualitative value	Collateral Damage Potential (CDP)	Observation	Action Required	Scan Results	Guidance
9.0 through 10.0	Critical/ Very High	The vulnerability is exposed and exploitable, and its exploitation could result in <u>severe impacts</u>. **Catastrophic Damage or loss**	Relevant Security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability	Risk is <u>totally</u> unacceptable. Immediate action required to mitigate the risk or decide to not proceed	Fail	To achieve a passing Assessment/ scan, these vulnerabilities must be corrected and the affected systems must be re- scanned after the corrections (with a report that shows a passing scan). Organizations should take a risk- based approach to correct these types of vulnerabilities, starting with the critical (rated 10.0), then those rated 9, followed by those rated 8, 7, etc., until all vulnerabilities rated 4.0 through 10.0 are corrected.
7.0 through 8.9	High Severity	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. **Significant damage or loss**	Relevant security control or other remediation is planned but not implemented; <u>compensation controls are in place and at least minimally effective</u>.	Risk is unacceptable. Remediation plan to be implemented as soon as possible to compensate for the risk	Fail	
4.0 through 6.9	Medium Severity	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. **Moderate damage or loss**	Relevant Security Control or other remediation is partially implemented and somewhat effective.	Risk may be acceptable over the short period of time. Monitoring the risk, and budget plan to reduce risk.	Fail	
0.1 through 3.9	Low Severity	The vulnerability is of minor concern, but effectiveness of remediation could be improved. **Slight damage to assets, or minor loss of revenue or productivity**	Relevant security control or other remediation is fully implemented and somewhat effective.	Risks are acceptable. Plans to further reduction of risk should be implemented with other security upgrades.	Pass	While passing scan results can be achieved with vulnerabilities rated 0.0 through 3.9, <u>organizations are encouraged</u>, but <u>**not required**</u>, to correct these vulnerabilities.
0.0	None/ Very Low	The vulnerability is not of concern. **No potential for loss of property, revenue or productivity**	Relevant security control or other remediation is fully implemented, assessed, and effective	Routine check and acceptance of the risk	Pass	Informational

Reference:
NVD : National Vulnerability Database
CVSS : Common Vulnerability Scoring (CVSS v3.1 guidance on September 10th, 2019)
PCI ASV Program Guide Version 3.1, July 2018

RightTime has developed an integrated methodology (custom) with the use of following sources:

1) **Licensed Vulnerability Analysis & Penetration Testing (VA & PT) Software**

Table 4.4.1: VAPT Tools

Activity		**RT Uses below Licensed Tools**
Vulnerability Analysis	Common Vulnerability Assessment	Mainly **Tenable Vulnerability Management/Nessus Professional**.
	Web Vulnerability Assessment	**Tenable Web Application Scanner** (Web Application Scanning) by Tenable
Penetration Testing	Common Penetration Testing	Mainly **Core Impact** (we may add Metasploit if Organization desires)
	Web Application Security, Testing, & Scanning	Mainly **Burp Suite** (we may add Acunetix if Organization desires)

2) **Open Sources:** Besides, we shall use world class authenticated open sources tools/applications (automated and manual) further verifying results i.e. OWASP ZAP, Kali Linux etc.

CHAPTER 5

ROLES & RESPONSIBILITIES

5.1. Initiation

I was fortunate enough to be given a wide range of tasks and experiences while working as a Security Executive Intern under the guidance of a senior security analyst at RightTime. In addition to my primary responsibility of learning and working as a Security Executive Intern, I was given the opportunity to assist in a variety of cyber security services.

To begin with, I had the chance to learn about different standards such as ISO 27001, SWIFT CSP, and PCI DSS, which helped me to understand the importance of adhering to industry best practices and regulatory compliance in information security. This knowledge proved invaluable in my role as a Security Executive Intern.

As part of my additional responsibilities, I was tasked with conducting security assessments, including Vulnerability Assessment & Penetration Testing (VA & PT), to identify potential vulnerabilities and risks in customer/client ITES Environment. Through this experience, I gained an in-depth understanding of the different types of threats that organizations face and the importance of proactive security measures.

Furthermore, I was responsible for monitoring and managing any attacks or intrusions in the network infrastructure. As a Security Specialist, it was crucial for me to recognize potential threats or attempted breaches and work with senior security analysts to close off vulnerabilities and build firewalls into the network infrastructure.

Overall, my experience at RightTime was invaluable in shaping my understanding of cyber security and providing me with practical skills and knowledge to pursue a career in this field.

As part of my role as a Security Executive Intern at RightTime, I had the opportunity to assist in the implementation of Payment Card Industry Data Security Standard (PCI DSS) compliance. This involved identifying gaps in the organization's current security controls and working with senior security analysts to remediate these gaps. Additionally, I helped to prepare technical documentation required for PCI DSS compliance, such as security policies, procedures, and guidelines. This experience provided me with valuable insights into the practical aspects of ensuring compliance with industry standards and regulations, which are crucial for maintaining the security and integrity of sensitive data.

5.2. Description

5.2.1 **PCI DSS**: As part of my role as a Security Executive Intern at RightTime, I had the opportunity to assist in the implementation of Payment Card Industry Data Security Standard (PCI DSS) compliance. This involved identifying gaps in the organization's current security controls and working with senior security analysts to remediate these gaps. Additionally, I helped to prepare technical documentation required for PCI DSS compliance, such as security policies, procedures, and guidelines. This experience provided me with valuable insights into the practical aspects of ensuring compliance with industry standards and regulations, which are crucial for maintaining the security and integrity of sensitive data.

5.2.2 As a Security Executive Intern at RightTime, I was involved in the assessment of the SWIFT Customer Security Program (CSP) based on the Customer Security Controls Framework (CSCF) 2023. This included identifying gaps in the organization's current security controls and working with senior security analysts to remediate these gaps in compliance with SWIFT CSP requirements. In addition, I assisted in preparing technical documentation required for SWIFT CSP compliance, such as security policies, procedures, and guidelines. This experience gave me practical insights into the SWIFT CSP framework, its requirements, and how organizations can effectively implement and maintain compliance with these standards.

5.2.3 During my tenure as a Security Executive Intern at RightTime, I had the opportunity to assist in the preparation of ISO 27001:2022 compliance. This involved conducting preparatory consultations and identifying gaps in the organization's current security controls. I worked with senior security analysts to remediate these gaps in compliance with the ISO 27001:2022 standard. Additionally, I assisted in the preparation of technical documentation such as security policies, procedures, and guidelines required for ISO 27001:2022 compliance.

5.2.4 As part of my role, I also coordinated with an external audit firm to engage them for conducting the ISO audit. This experience gave me practical insights into the process of preparing for an ISO 27001:2022 audit, working with external audit firms, and effectively implementing and maintaining compliance with ISO standards.

CHAPTER 6

EXPERIENCE & ACHIEVEMENTS

6.1 Overcome Problems and Difficulties

Before joining RightTime as a fresher, I acknowledged that I had some drawbacks in my skills that needed to be addressed to make me suitable for working in a company. Initially, during my internship, I faced some challenges that made the experience quite demanding for me. I struggled with punctuality and occasionally arrived late to the office. I made every effort to complete each day's tasks but found that sometimes I had to work from home to catch up.

In the beginning, the standard implementation i.e. ISO 27001, SWIFT CSP Assessment and PCI DSS posed a significant challenge to me as it was a new area of expertise. I struggled to solve some problems on my own and found it challenging to know where to begin. However, I overcame this hurdle with help from my project manager and by searching for resources on Google. Through this experience, I learned a lot about office environments, professional life, and colleague behavior. As a newcomer to the professional world, I faced some challenges, but I persevered and learned a lot from my experiences.

6.2 Ability to Learn

In today's fast-paced and ever-changing world, people need to adapt to changes to remain relevant and competitive. I believe that I have undergone a significant transformation, which has enabled me to adapt to the changing environment around me. I have always been passionate about learning and growing, and this passion has enabled me to become more adaptable and flexible.

During my internship at RightTime, I was exposed to several new tools and technologies that helped me to collaborate with other team members effectively. This collaborative approach to learning was highly effective in helping me learn about Cyber Security quickly. In addition, my exposure to various Cyber Security service areas and standards, such as ISO 27001, SWIFT CSP, and PCI DSS, has broadened my knowledge and skillset in this field.

I believe that continuous learning is key to staying competitive and adapting to the changes around us. My experience at RightTime has taught me the importance of being open to learning new things and embracing change, and I am confident that these skills will serve me well throughout my career.

6.3 Technology Enhancement

In today's rapidly advancing technological landscape, the importance of Cyber Security cannot be overstated. While technology continues to evolve and innovate, it is also vulnerable to security breaches, which can result in significant losses for organizations.

During my internship at RightTime, I came to realize the critical importance of Cyber Security in real-life projects. I was tasked with providing security for various projects, and I learned firsthand how challenging it can be to ensure the safety of sensitive data and information.

As part of my internship, I also gained a deeper understanding of technical terms such as Security Operation Center (SOC) and Risk Management. Through my exposure to these concepts, I gained a better understanding of the importance of maintaining a robust security posture and the measures that must be taken to mitigate risks and protect against threats.

I believe that the growing importance of Cyber Security makes it essential for individuals and organizations to prioritize this area. As a result of my experience at RightTime, I have developed a greater appreciation for the importance of Cyber Security and the need to stay informed about the latest trends and technologies in this field.

6.4 Non-Technical Growth

Soft skill development is an essential aspect of personal and professional growth. While technical skills are important, the ability to effectively communicate and work collaboratively with others is equally crucial in today's workplace.

During my internship at RightTime, I had the opportunity to focus on non-technical development, which included honing skills such as a strong work ethic, a positive attitude, good communication skills, time management abilities, and the ability to work well in a team.

By focusing on these non-technical skills, I was able to improve my overall performance and productivity in the workplace. I learned the importance of being dependable, taking initiative, and maintaining a positive outlook, even in challenging situations. Moreover, I realized that good communication skills and time management are critical in ensuring that projects are completed on time and within budget.

Working effectively in a team was another important aspect of my non-technical development. Through collaboration with my colleagues, I gained a better understanding of the importance of mutual respect, open communication, and teamwork in achieving common goals.

I believe that non-technical development is a crucial aspect of personal and professional growth, and it is essential to continuously work on improving these skills. My experience at RightTime has taught me the importance of focusing on non-technical development and the impact it can have on my overall success and well-being.

6.5 Achievement

Professional growth is a continuous process that requires effort and perseverance. During my tenure at RightTime, I encountered several challenges that helped me to grow both technically and non-technically.

Initially, I struggled with time management and meeting deadlines, but through hard work and determination, I was able to overcome these deficiencies. Additionally, I had the opportunity to work on technical projects such as ISO 27001 implementation, SWIFT CSP assessment, and PCI DSS compliance validation service (CVS), which helped me to gain valuable technical knowledge and experience.

One of the most significant challenges I faced during my internship was working with the Security Operation Center (SOC). Initially, I found it challenging to navigate the system and address security concerns effectively. However, with the help of my colleagues and managers, I was able to learn the ropes and become proficient in using the system.

Apart from technical skills, I also focused on developing my soft skills, such as communication, teamwork, and time management. These skills are essential in any professional setting and helped me to collaborate effectively with my colleagues and complete projects on time.

My experience at RightTime has taught me the importance of hard work, determination, and continuous learning. I am now more confident in my abilities and have gained the necessary skills to succeed in the professional world. I am grateful for the support and guidance of my supervisor, project manager, and teachers at Daffodil International University, who helped me achieve my goals.

CHAPTER 7

CONCLUSIONS & RECOMMENDATIONS

7.1 Summary:

Professional growth is a continuous process that requires effort and perseverance. During my tenure at RightTime, I encountered several challenges that helped me to grow both technically and non-technically.

Initially, I struggled with time management and meeting deadlines, but through hard work and determination, I was able to overcome these deficiencies. Additionally, I had the opportunity to work on technical projects such as ISO 27001 implementation, SWIFT CSP assessment, and PCI DSS compliance validation service (CVS), which helped me to gain valuable technical knowledge and experience.

One of the most significant challenges I faced during my internship was working with the Security Operation Center (SOC). Initially, I found it challenging to navigate the system and address security concerns effectively. However, with the help of my colleagues and managers, I was able to learn the ropes and become proficient in using the system.

Apart from technical skills, I also focused on developing my soft skills, such as communication, teamwork, and time management. These skills are essential in any professional setting and helped me to collaborate effectively with my colleagues and complete projects on time.

My experience at RightTime has taught me the importance of hard work, determination, and continuous learning. I am now more confident in my abilities and have gained the necessary skills to succeed in the professional world. I am grateful for the support and guidance of my supervisor, project manager, and teachers at Daffodil International University, who helped me achieve my goals.

7.2 Findings & Contribution

Before starting my internship, I gained a solid foundation in cyber security concepts and practices through my university classes, which proved to be extremely beneficial in my internship tasks with this organization. During my internship, I had the chance to put my theoretical knowledge into practice and work on a variety of real-world problems and projects, which helped me to understand the cyber security life cycle in-depth.

This internship also exposed me to the professional work culture, where I learned about the importance of teamwork, communication, and time management. I was able to work on different projects, which helped me to develop my analytical skills, critical thinking, and problem-solving abilities. I learned how to approach new technological problems and find effective solutions through team discussions and brainstorming sessions. Additionally, I gained a good understanding of business processes and how to identify and address various challenges in a professional environment.

Overall, this internship was a great learning experience for me, and I am grateful to have had the opportunity to work with such a dynamic and knowledgeable team. I believe that the skills and knowledge I have gained during this internship will be invaluable for my future career in the cyber security field.

7.3 Recommendation for Future Work

In countries like Bangladesh, it is challenging for freshers to secure employment. With a large number of students graduating each year, competition is high, and many are unable to secure the positions they desire due to a lack of professional experience. However, internships provide an opportunity for recent graduates to overcome this obstacle and gain valuable experience in a professional environment. As a newcomer, I also faced several challenges during my internship, but it has helped me learn and grow both professionally and personally."

APPENDIX

PCI DSS – Payment Card Industry Data Security Standards

ISO – International Organization for Standardization

SWIFT - Society for Worldwide Interbank Financial Telecommunications

VAPT – Vulnerability Assessment and Penetration Testing

CVSS - Common Vulnerability Scoring System

CVE - Common Vulnerabilities and Exposure

CWE - Common Weakness Enumeration

NVD - National Vulnerability Database

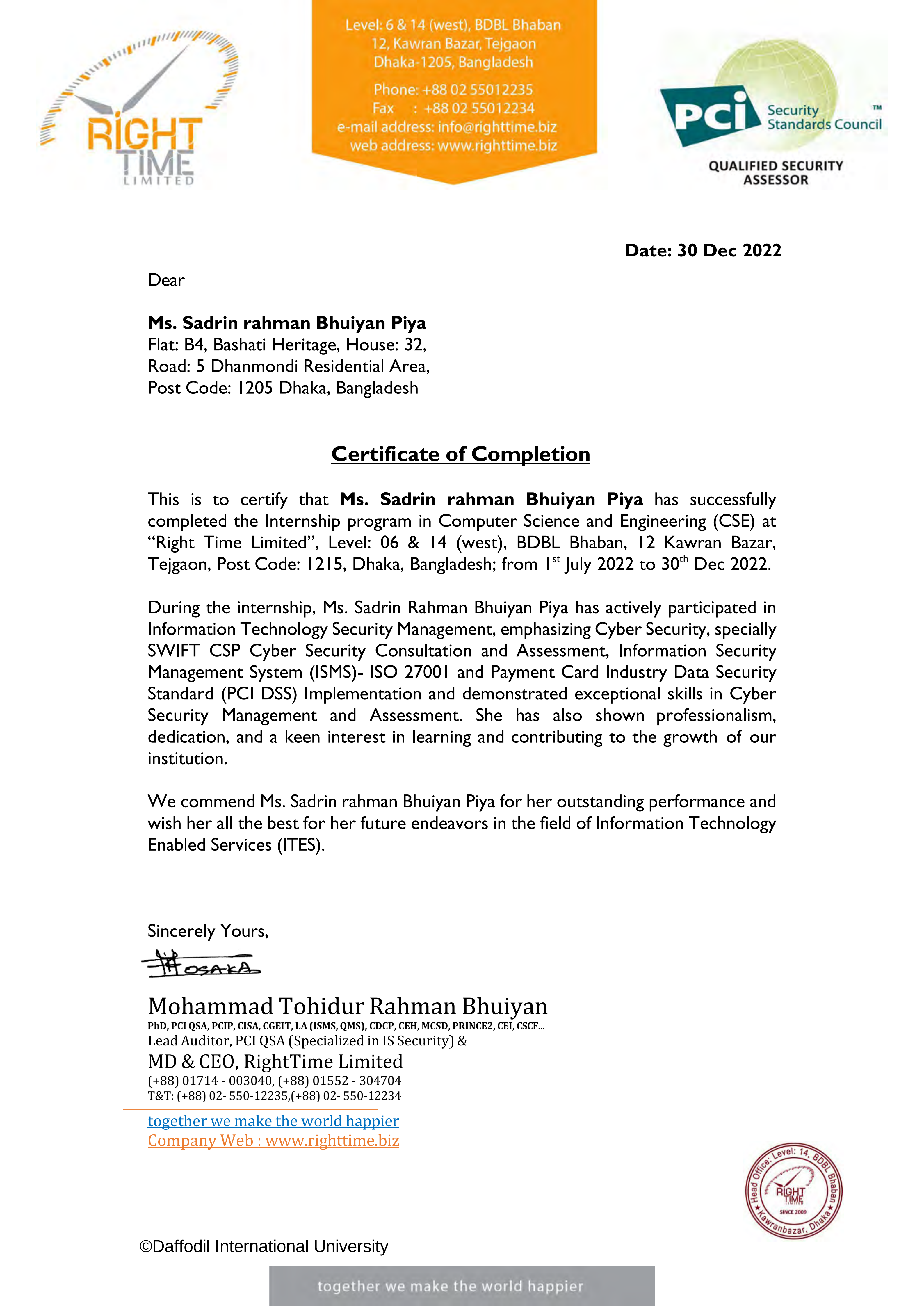
REFERENCES

[1] Learn about internship organization, available at << https://righttime.biz //>>

[2] Learn about PCI DSS, available at << https://pcisecuritystandards.org //>>

[3] Learn about SWIFT, available at << https://www.swift.com //>>

[4] Learn about ISO Standards, available at << https://www.iso.org //>>



RIGHT TIME LIMITED

Level: 6 & 14 (west), BDBL Bhaban
12, Kawran Bazar, Tejgaon
Dhaka-1205, Bangladesh

Phone: +88 02 55012235
Fax : +88 02 55012234
e-mail address: info@righttime.biz
web address: www.righttime.biz

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

Date: 30 Dec 2022

Dear

Ms. Sadrin rahman Bhuiyan Piya
Flat: B4, Bashati Heritage, House: 32,
Road: 5 Dhanmondi Residential Area,
Post Code: 1205 Dhaka, Bangladesh

Certificate of Completion

This is to certify that **Ms. Sadrin rahman Bhuiyan Piya** has successfully completed the Internship program in Computer Science and Engineering (CSE) at "Right Time Limited", Level: 06 & 14 (west), BDBL Bhaban, 12 Kawran Bazar, Tejgaon, Post Code: 1215, Dhaka, Bangladesh; from 1st July 2022 to 30th Dec 2022.

During the internship, Ms. Sadrin Rahman Bhuiyan Piya has actively participated in Information Technology Security Management, emphasizing Cyber Security, specially SWIFT CSP Cyber Security Consultation and Assessment, Information Security Management System (ISMS)- ISO 27001 and Payment Card Industry Data Security Standard (PCI DSS) Implementation and demonstrated exceptional skills in Cyber Security Management and Assessment. She has also shown professionalism, dedication, and a keen interest in learning and contributing to the growth of our institution.

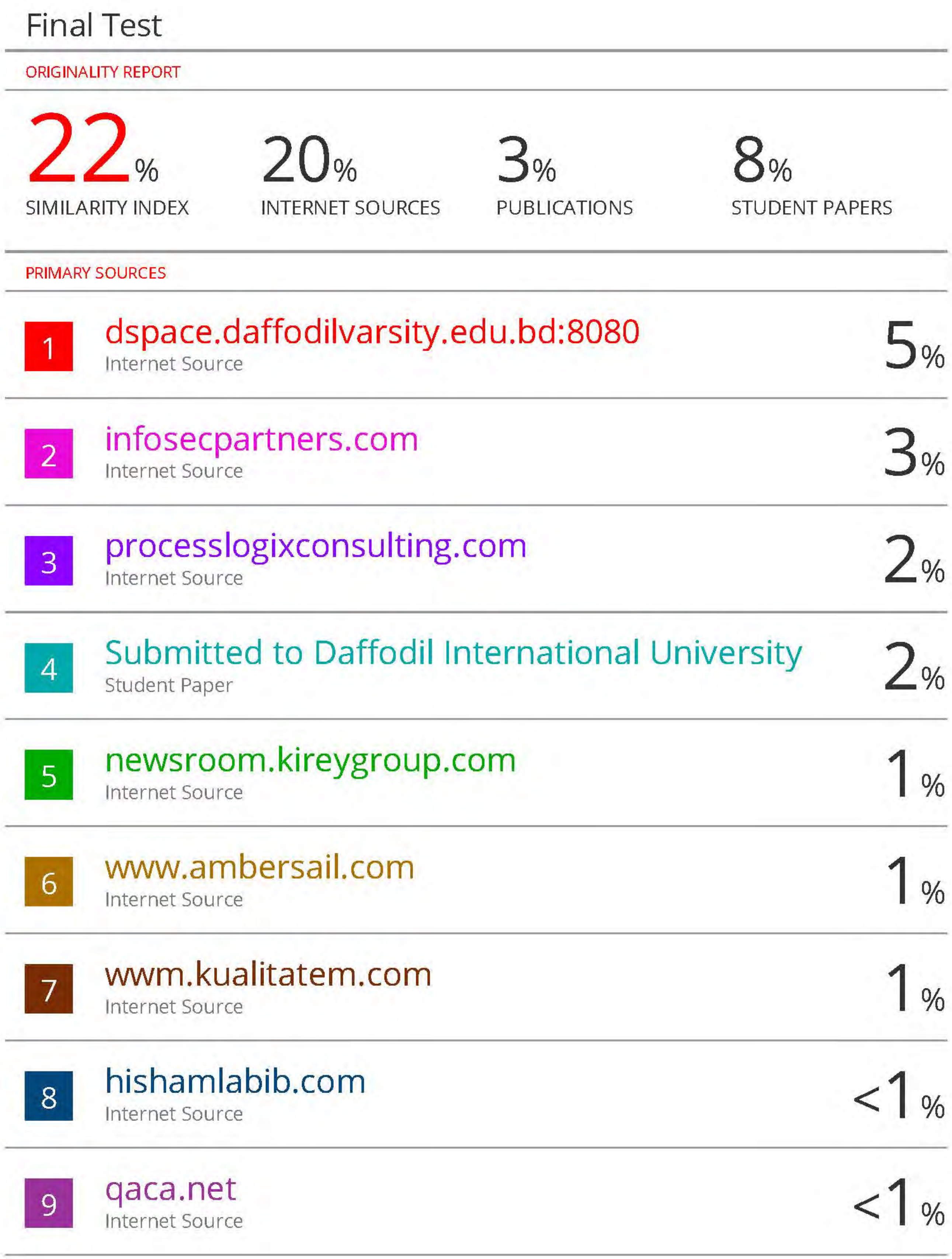
We commend Ms. Sadrin rahman Bhuiyan Piya for her outstanding performance and wish her all the best for her future endeavors in the field of Information Technology Enabled Services (ITES).

Sincerely Yours,

Mohammad Tohidur Rahman Bhuiyan
PhD, PCI QSA, PCIP, CISA, CGEIT, LA (ISMS, QMS), CDCP, CEH, MCSD, PRINCE2, CEI, CSCF...
Lead Auditor, PCI QSA (Specialized in IS Security) &
MD & CEO, RightTime Limited
(+88) 01714 - 003040, (+88) 01552 - 304704
T&T: (+88) 02- 550-12235,(+88) 02- 550-12234

together we make the world happier
Company Web : www.righttime.biz

Head Office: Level: 14, BDBL Bhaban ★Kawranbazar, Dhaka★
RIGHT TIME LIMITED
SINCE 2009



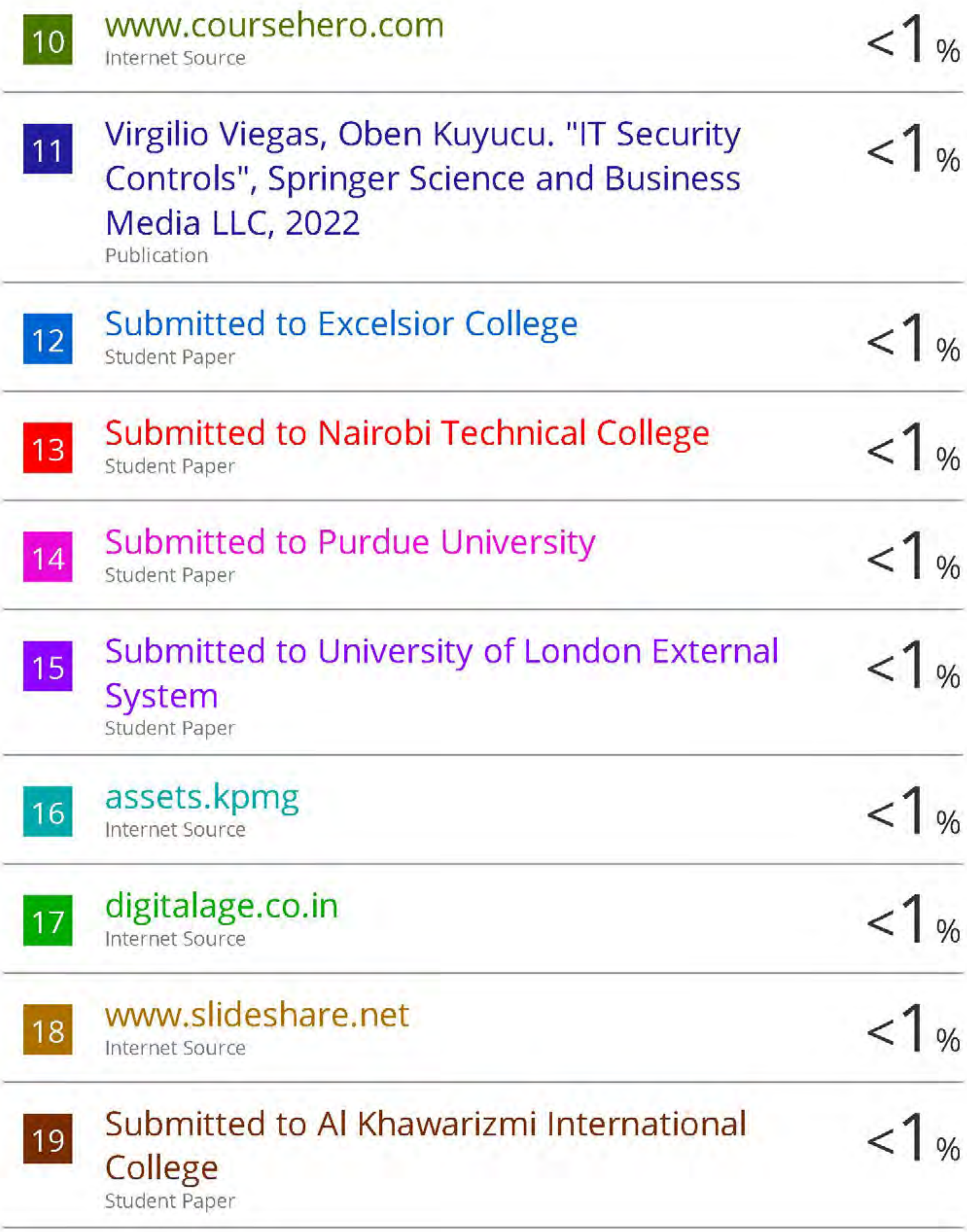
Final Test

ORIGINALITY REPORT

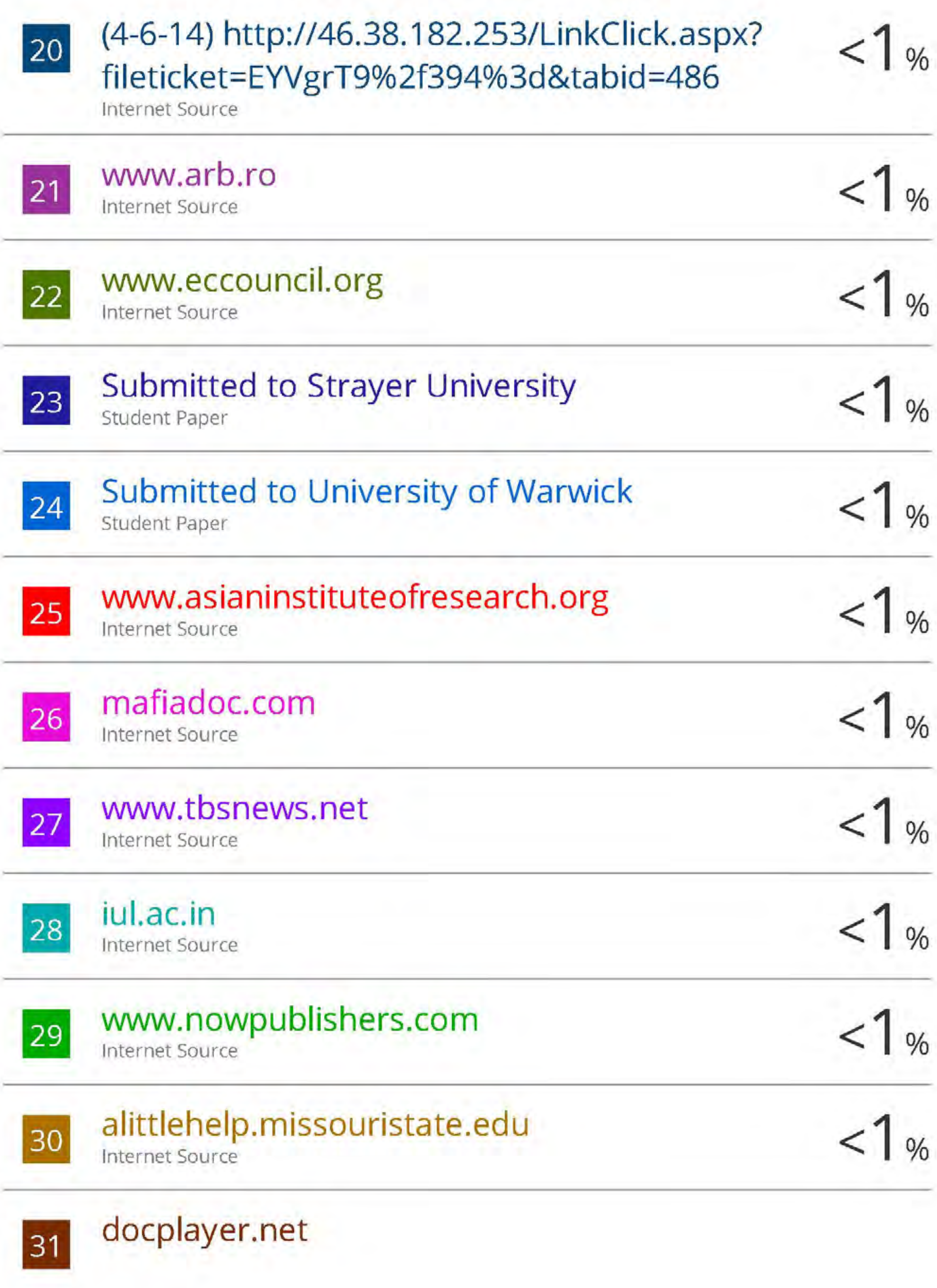
22%	20%	3%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

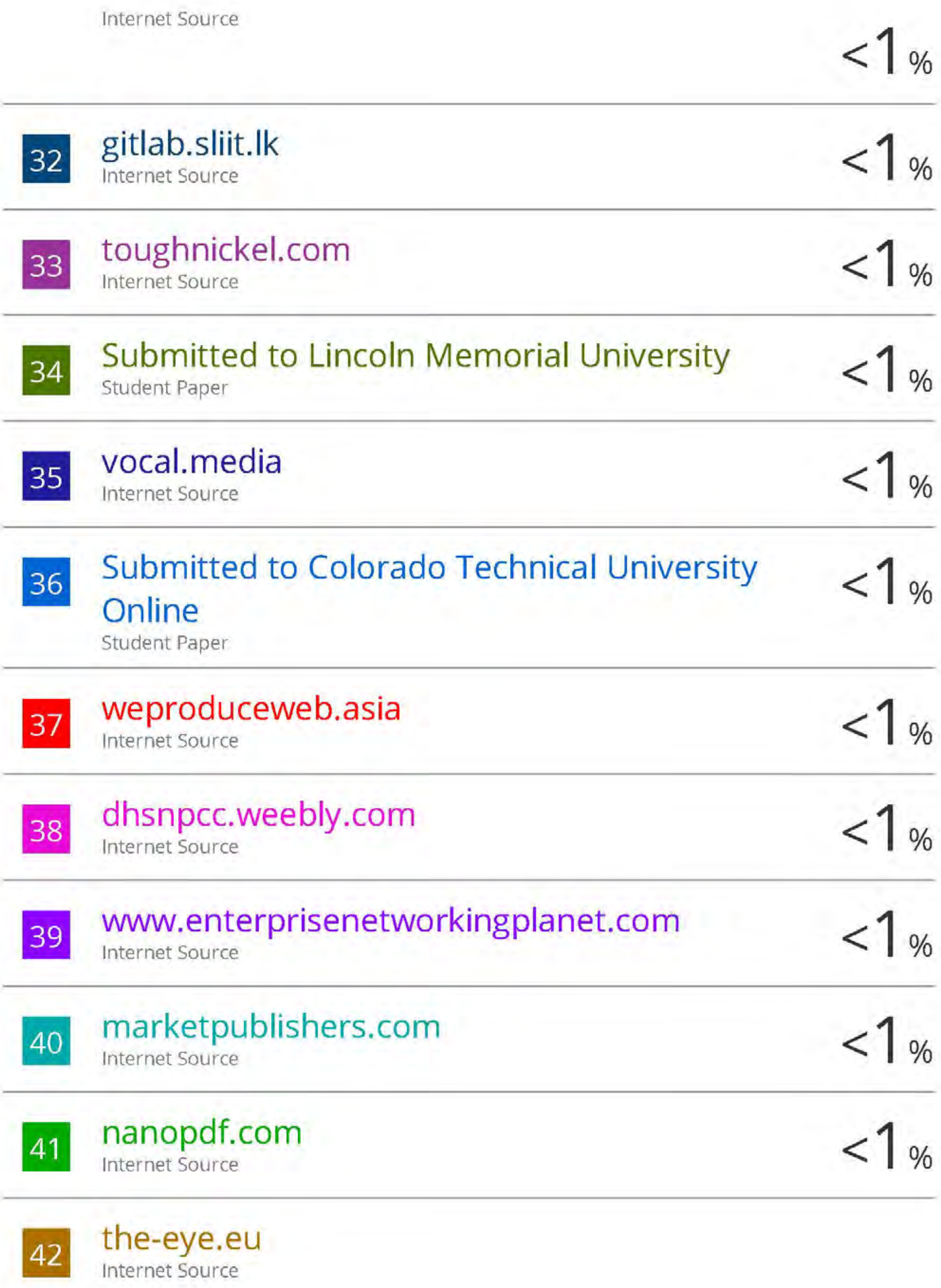
1	dspace.daffodilvarsity.edu.bd:8080 Internet Source	5%
2	infosecpartners.com Internet Source	3%
3	processlogixconsulting.com Internet Source	2%
4	Submitted to Daffodil International University Student Paper	2%
5	newsroom.kireygroup.com Internet Source	1%
6	www.ambersail.com Internet Source	1%
7	wwm.kualitatem.com Internet Source	1%
8	hishamlabib.com Internet Source	<1%
9	qaca.net Internet Source	<1%



10	www.coursehero.com Internet Source	<1 %
11	Virgilio Viegas, Oben Kuyucu. "IT Security Controls", Springer Science and Business Media LLC, 2022 Publication	<1 %
12	Submitted to Excelsior College Student Paper	<1 %
13	Submitted to Nairobi Technical College Student Paper	<1 %
14	Submitted to Purdue University Student Paper	<1 %
15	Submitted to University of London External System Student Paper	<1 %
16	assets.kpmg Internet Source	<1 %
17	digitalage.co.in Internet Source	<1 %
18	www.slideshare.net Internet Source	<1 %
19	Submitted to Al Khawarizmi International College Student Paper	<1 %



20	(4-6-14) http://46.38.182.253/LinkClick.aspx?fileticket=EYVgrT9%2f394%3d&tabid=486 Internet Source	<1 %
21	www.arb.ro Internet Source	<1 %
22	www.eccouncil.org Internet Source	<1 %
23	Submitted to Strayer University Student Paper	<1 %
24	Submitted to University of Warwick Student Paper	<1 %
25	www.asianinstituteofresearch.org Internet Source	<1 %
26	mafiadoc.com Internet Source	<1 %
27	www.tbsnews.net Internet Source	<1 %
28	iul.ac.in Internet Source	<1 %
29	www.nowpublishers.com Internet Source	<1 %
30	alittlehelp.missouristate.edu Internet Source	<1 %
31	docplayer.net	



	Internet Source	<1%
32	gitlab.sliit.lk Internet Source	<1%
33	toughnickel.com Internet Source	<1%
34	Submitted to Lincoln Memorial University Student Paper	<1%
35	vocal.media Internet Source	<1%
36	Submitted to Colorado Technical University Online Student Paper	<1%
37	weproduceweb.asia Internet Source	<1%
38	dhsnpcc.weebly.com Internet Source	<1%
39	www.enterprisenetworkingplanet.com Internet Source	<1%
40	marketpublishers.com Internet Source	<1%
41	nanopdf.com Internet Source	<1%
42	the-eye.eu Internet Source	

		<1%
43	www.fbnholdings.com Internet Source	<1%
44	www.gyrtechnology.com Internet Source	<1%
45	www.themanufacturer.com Internet Source	<1%
46	"Index", Elsevier BV, 2015 Publication	<1%
47	cpl.thalesgroup.com Internet Source	<1%
48	www.ars-nc.com Internet Source	<1%
49	www.diva-portal.org Internet Source	<1%
50	Submitted to University of Wales, Lampeter Student Paper	<1%
51	whitehats.sis.smu.edu.sg Internet Source	<1%
52	Submitted to TAR University College Student Paper	<1%
53	acikbilim.yok.gov.tr Internet Source	<1%

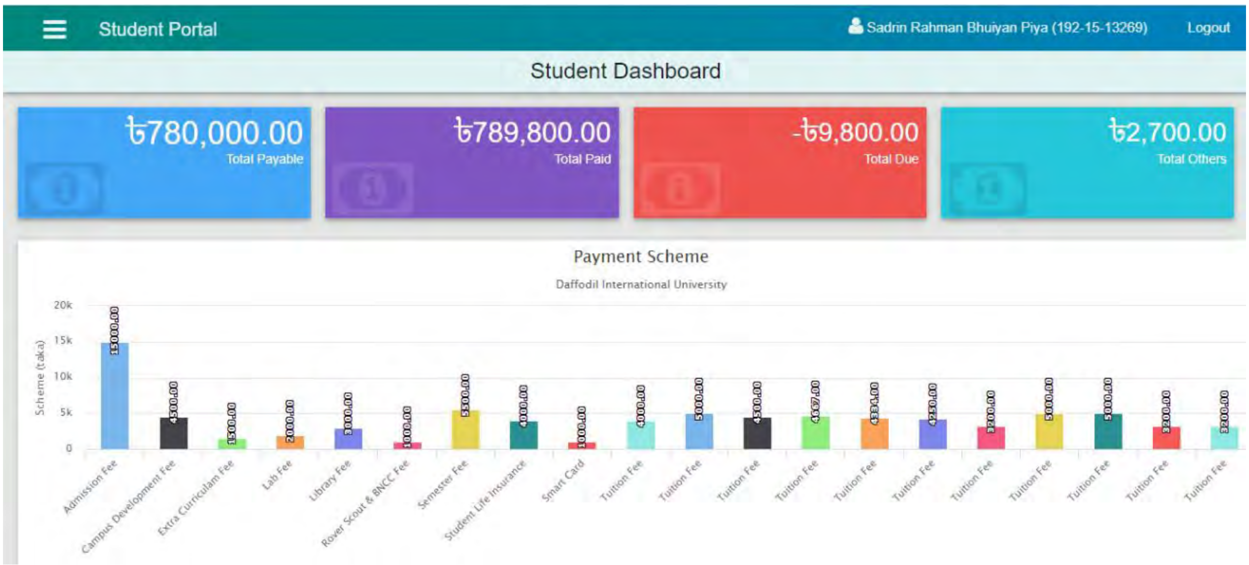
54	d1.awsstatic.com Internet Source	<1 %
55	dokumen.pub Internet Source	<1 %
56	isss.co.in Internet Source	<1 %
57	virtocommerce.com Internet Source	<1 %
58	www.aibms.com Internet Source	<1 %
59	Blerton Abazi. "A novel approach for information security risk assessment maturity framework based on ISO 27001", Corvinus University of Budapest, 2020 Publication	<1 %
60	Morey J. Haber. "Privileged Attack Vectors", Springer Science and Business Media LLC, 2020 Publication	<1 %
61	Stuart Jacobs. "Security Management of Next Generation Telecommunications Networks and Services", Wiley, 2013 Publication	<1 %

Exclude quotes Off

Exclude bibliography On

Exclude matches Off

Account Clarence (Screen Shot):



Student Portal

Sadrin Rahman Bhuiyan Piya (192-15-13269)

Logout

Student Dashboard

৳780,000.00 Total Payable

৳789,800.00 Total Paid

-৳9,800.00 Total Due

৳2,700.00 Total Others

Payment Scheme

Daffodil International University

End of Report