# Report On

# Performance and Security Alignment in ICT Operations: An Analytical Study of Shahjalal Islami Bank PLC's ICT Security infrastructure

By

MOHAMMAD RAFQUAT HAIDER
23164003

An internship report submitted to the BRAC Business School in partial fulfillment of the requirements for the degree of
Master of Business Administration

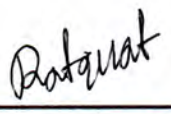
BRAC Business School
BRAC University
February 2025

## Declaration

It is hereby declared that

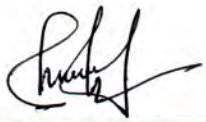
1. The internship report submitted is my own original work while completing degree at BRAC University.
2. The report does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The report does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. I have acknowledged all main sources of help.

**Student's Full Name & Signature:**



**Mohammad Rafquat Haider**
23164003

**Supervisor's Full Name & Signature:**



**Dr. Najmul Hasan**
Assistant Professor, BRAC Business School
BRAC University

## Letter of Transmittal

Dr. Najmul Hasan
Assistant Professor,
BRAC Business School
BRAC University

Subject: Internship report on "Performance and Security Alignment in ICT Operations: An Analytical Study of Shahjalal Islami Bank PLC's ICT Security infrastructure.

Dear Sir,

This is my pleasure to display my internship report regarding "Performance and Security Alignment in ICT Operations: An Analytical Study of Shahjalal Islami Bank PLC's ICT Security infrastructure." for which I was appointed, as a partial fulfillment for my master's degree.

I have attempted my best to finish the report with the essential data and recommended proposition in a significant compact and comprehensive manner as possible.

In the instance for the requirement of additional information regarding the report, do feel free to refer back to me. I will be delighted to discuss the topic in details.
I trust that the report will meet the desires.

Sincerely yours,

Mohammad Rafquat Haider
ID 23164003
BRAC Business School
BRAC University
Date: February 20th, 2025

## Non-Disclosure Agreement

This Agreement is made and entered into by and between Shahjalal Islami Bank PLC and the undersigned student at BRAC University, Mohammad Rafquat Haider, ID of 23164003.

## Acknowledgement

At first, Thanks to Almighty Allah (SWT).

I want to express my gratitude especially to my honorable supervisor Dr-Najmul Hasan, PhD

Assistant Professor, BRAC Business School, BRAC University; for inspiring me to write the report. He has supported me greatly, helped me understand crucial focus points, coached me with immense patience and helped me to go beyond my boundaries. I am really grateful for his immense support.

I am appreciative to Shahjalal Islami Bank PLC as they provided me with the facility needed to complete my internship course. I am grateful to Zahid Hasan, Senior Vice President & Head, ICT Security Department, Shahjalal Islami Bank PLC, Head Office; for giving me his valuable time and cooperated me by providing all necessary knowledge and information about the department and the organization. Moreover, I am thankful to all of the members of the ICT Security Department; Zabedul Hoque Chowdhury, Md. Shahanur Alam Emran & Ratul Ali as they helped me with a friendly working environment, guidance, valuable advice and co-ordination for internship and in the preparation of this report. It was a great chance for me to learn and it also helped me to develop my professional skills.

Thank You

Mohammad Rafquat Haider

ID 23164003

## Executive Summary

This report is the outcome of three months internship program at Shahjalal Islami Bank PLC. It has been prepared for the partial fulfillment of the MBA degree. Throughout this internship, I worked in the ICT Security Department. My main responsibilities involved assisting with the role based access management, understanding the information security policies of the bank alongside that of the central bank (Bangladesh Bank), suggesting areas for further improvement, assisting in ongoing projects such as ISO 27001 & PCI-DSS and at the same time understanding the network infrastructures of the bank. For ease of understanding and to keep the separation of topics simple, the report has been classified into 3 chapters only.

# Table of Contents

## List of Figures

## Acronyms

| | |
|---|---|
| SJIBPLC | Shahjalal Islami Bank PLC |
| ICT SD | ICT Security Department |
| ITD | Information Technology Division |
| BB | Bangladesh Bank |
| SOC | Security Operations Center |
| PAM | Privilege Access Management |
| VA | Vulnerability Assessment |
| PT | Penetration Testing |
| DB | Data Base |
| DC | Data Center |
| OS | Operating Systems |
| ISO | International Organization of Standardization |

# Chapter 1

## Student Information

I, Mohammad Rafquat Haider (student ID: 23164003), is an MBA student of BRAC Business School, majoring in Information Technology Management. Enrolled in the spring 2023 semester and currently I have completed all courses for MBA except the internship as of fall 2024. Previous to that, I completed my B.SC in Electronics and Communication Engineering, Communications Major, from BRAC University as well. Before enrolling for MBA, I worked at an IT Firm as an executive officer in their network team for 2 years. Following that, I joined Shahjalal Islami Bank PLC in the year 2022, and have been working here in the ICT Security department till date. Hence, my internship is based on Shahjalal Islami Bank PLC's ICT security department, mainly focusing on ways to improve the sector overall. My main responsibilities involved assisting with the role based access management, understanding the information security policies of the bank alongside that of the central bank, (Bangladesh Bank), suggesting areas for further improvement, assisting in ongoing projects such as ISO 27001 & PCI-DSS and at the same time understanding the network infrastructures of the bank. This internship experience has also provided valuable industry insights, exposing me to current trends, challenges, and best practices in ICT security. All in all, my internship tenure has not only solidified my career aspirations in this field but has also equipped me with the practical skills and corporate understanding necessary to thrive in this dynamic industry.

# Chapter 2

## Organizational Information: A Brief of Shahjalal Islami Bank PLC

Shahjalal Islami Bank PLC (SJIBPLC) is a sharia compliant private sector commercial bank headquartered in Dhaka, Bangladesh (Shahjalal Islami Bank, n.d.). The Bank was incorporated on 10 May 2001. The Shahjalal Islami Bank Foundation is the corporate social responsibility unit of the bank. Currently, Mr. A K Azad, Chairman of Hameem Group of Industries; has been unanimously elected as Chairman of the Board of Directors of Shahjalal Islami Bank PLC. At the same time, Mr. Akkas Uddin Mollah and Mr. Fakir Akhtaruzzaman were elected as Vice-Chairmen respectively of the Board of Directors of the Bank (Shahjalal Islami Bank PLC., 2022). Alongside them, all the members of the board of directors committee are all well established and renowned personnel of Bangladesh. The bank itself has made massive contributions for the country in difficult times, say for example in the recent Noakhali region flood it helped all the flood affected people. Shahjalal Islami Bank PlC at present carries out all its operations through 140 domestic branches and 131 ATM booths. With its head office situated in Gulshan Avenue, has more than 800 employees and staff only at the head office and in total more than 2500 employees all over the country.

Moving onto its Islamic banking and relevant products of SJIBPLC, Islamic banks primarily work upon three modes of finance, namely, rental arrangement (Ijarah), trade/ sale basis (Murabaha, Musawammah, Salam, Istisna & Tijarah) and partnerships (Mudarabah & Musharakah).

- Ijarah or rental arrangement is where the usufruct of a durable asset is leased out to a customer against a certain rental payment for a mutually agreed tenor.
- Murabaha: It is that sale where bank (seller) discloses the cost and profit to the customer (buyer).

- Musawammah: It is an ordinary sale where bank (seller) does not disclose cost and profit to its customer (buyer).
- Salam: It is a sale where 100% payment is made in advance and goods delivery is set on a future date. Also, it has a limitation to be done upon homogenous goods.
- Istisna: Sale transaction with spot or part payment for manufactured goods. An order is placed with the manufacturer to make a specific commodity to the purchaser.
- Tijarah: It is a sale and agency-based financing facility where finished stock is sold by customer (seller) to bank (buyer) to generate working capital for further business operations. Banks may offer this facility to manufacturer/producer/trader who sell finished goods on credit basis.
- Musharkah: is a partnership where all the partners invest capital in a joint business and become owners of the business with their ratio of investment They share profits as per agreed profit sharing ration and share loss as per investment ratios.
- Mudarabah: is a partnership where one party invests capital (Rab Ul Maal) and the other party renders services (Mudarib) in a joint business. Mudarabah Islamic banks operate all types of savings/ remunerative accounts and term deposits on Mudarabah basis.

Islamic banks invest customer's deposits in Shariah-compliant avenues and share the profits with customers as per profit sharing ratios agreed on monthly basis.

- Kafalah: It refers to the guarantee an Islamic bank provides to a third party on behalf of its customer, in case they fail to pay the third party in due time.
- Wakalah: It is usually a paid agency contract, where a customer hires a particular service from an Islamic bank for a certain price.

Moving forward, let us have a brief look at the financial aspect of this bank.

First, the closing price graph of SJIBPLC's is below.


*Figure 1 Price Graph for SJIBPLC's last 1Year*

Then let us look at the trading potential of SJIBPLC for the last 1 year.


*Figure 2 Trade Graph for SJIBPLC's last 1Year*

Finally, the total share volume graph for the past 1 year.

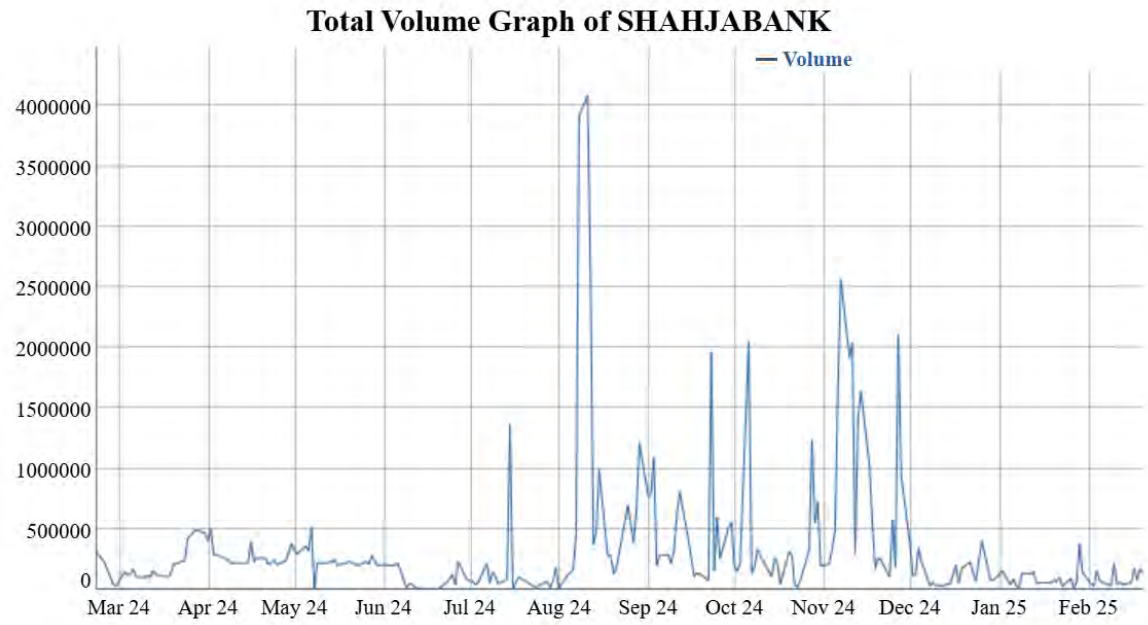



*Figure 3 Share Volume Graph for SJIBPLC's last 1Year*

Do have a look at the following stats (Display Company Information | Dhaka Stock Exchange, 2025) to understand the market value of SJIBPPLC in 2024.

Authorized Capital: 15,000 Million Paid Up Capital: 11,129.68 Million

Face/Par Value: 10.00 Tot No. of Outstanding Sec.:1,112,968,351

Before concluding, let us have a look at the Mission of the bank, they are as follows:

- Uncompromised quality service and customer care.
- Setting high standards of integrity.
- Inclusive and innovative banking.
- Sustainable value for all stakeholders.
- Continuous development of professionals and system up gradation to face the challenges and drive for excellence.

- System Automation and digitization adopting the state-of art technology with full proof security to ensure fast and accurate customer service.
- Human Resources Development based on morality and ethics.

# Chapter 3

# A Critical Analysis of the Internship Experience

## 3.1 Introduction

Background of the Study: In the modern banking sector, information and communication technology (ICT) has become a cornerstone for operational efficiency, customer satisfaction, and regulatory compliance. At the same time in a rapidly increasingly digitized and interconnected world, the importance of robust and effective IT security measures cannot be overstated. However, with the increasing reliance on digital systems, banks are now more vulnerable and exposed to cyber threats and operational vulnerabilities. Shahjalal Islami Bank, like many other financial institutions, operates within this dynamic and rapidly evolving environment, where the security of its ICT infrastructure is critical to maintaining trust and ensuring seamless services for all the entities involved.

This study explored the ICT security operations of Shahjalal Islami Bank to identify challenges, evaluate performance factors, and provide actionable recommendations for improvement. By understanding the current security infrastructure and pinpointing areas of concern, this research aimed at contributing to the enhancement of the bank's ICT security practices. As part of an internship course requirement for the B.Sc. program, this study also provided an opportunity to bridge theoretical knowledge with practical application. The focus was on conducting a gap analysis of the existing ICT security infrastructure, identifying key problem areas, and suggesting steps to address them. In doing so, the research conducted aligns with the broader goal of enhancing the bank's overall performance and resilience in the face of emerging threats.

Importance of the Study: The banking sector is a critical component of the national economy, and its security is paramount to maintaining financial stability, public trust and reputation of organizations. Due to increasing numbers of sophisticated cyber threats, ensuring the robust

security of ICT systems within banks has become an area of utmost concern and at the same time is getting extremely difficult without proper measures. This internship at Shahjalal Islami Bank PLC (SJIBPLC) focused on their ICT security department. The aim was to gain practical insights into the real-world challenges and effective strategies used in this area. Key security issues and regulatory requirements within the banking sector were observed. The report will further discuss potential areas for improvement in these aspects later on. The findings of this study are expected to enhance understanding of the current security practices in the industry and suggest ways to strengthen the overall security of the banking sector in Bangladesh. Furthermore, the practical experience will be invaluable in developing my own professional skills and knowledge in the field of ICT security along with the corporate sector.

Gaps of existing knowledge: It is vital to understand, that the ICT Security Department of SJIBPLC is fairly new. Basically, it started its full-on activities as a separate department from IT Division from the year 2021. This is a suggested recommendation by Bangladesh Bank and for many reputed certification bodies a must, to ensure that there is no conflict of interest between the 2 divisions. Hence, the department is working on developing itself and form a fully sophisticated ICT security team. Thus, the lack of previous research for this department's gaps are not much yet detailed out. This acted a crucial limitation barrier during my internship. However, there are existing literature on general cybersecurity principles and banking security guidelines provided by Bangladesh Bank and compliance certifying bodies, which in turn showcases vast number of the lacking in this industry. So, this report primarily focused on the gaps of the industry. Despite the limited publicly available research on the practical implementation of security protocols, the effectiveness of current security measures against evolving threats, and the specific vulnerabilities faced by banks; a clearly visible gap is the resilience in accepting new ICT trends. As in whenever a particular ICT security protocol is implemented, as most employees are of non IT Background, do not pay or do not want to pay

much heed to this protocols. Employee awareness trainings are carried out as per schedule. However, the acceptance of such schedules are not always welcomed. Another vital gap is that most banks are yet to separate their ICT Security team from the IT Division. This poses a vital area of concern as this can be a reason for conflict of interest. Furthermore, the lack of research in this field, the restrictions of banks from carrying out research or providing information for research particularly for this sector as this deals with highly sensitive & confidential data of the bank can also be considered as a major gap. So, to pinpoint the broad limitations for this report do see the following points:

- lack of previous research for this department's gaps are not much yet detailed out
- ICT security department's information are highly sensitive and confidential, thus it is not readily shared even for research purposes.
- Most organizations in Bangladesh very recently are separating their ICT security department from IT division, lot of research was collected from a bundle of IT researches.

This report aimed to focus on all this ICT security postures of the banking sector, address some of these gaps by providing firsthand insights, examining the specific threats it faces, and ultimately analyzing the effectiveness of security strategies.

Objectives: The objectives of this internship report are designed to clearly define the goals aimed to achieve, serving as a roadmap for my experience and demonstrating my contributions and personal growth. These objectives encompass a range of learning and practical outcomes, including project completion, hands-on experience, collaboration, problem-solving, knowledge acquisition, and professional development. Aligning these goals, the internship provided a structured framework to enhance skills and contribute meaningfully to the organization.

The specific objectives of this internship are as follows:

- To familiarize with overall ICT security operations of Shahjalal Islami Bank PLC.
- To identify the problems associated with security operations.
- To put forward some measures to overcome the problems.
- To accomplish the partial requisite of MBA Program and to achieve of good judgment with theoretical base.

Research/Study's Expected Questions: This internship will be guided by the following key research/study questions based on the objectives just mentioned.

- How effective are the existing security measures and protocols in mitigating these threats from the perspective of Shahjalal Islami Bank PLC's ICT Security Department?
- What are the primary ICT security threats and vulnerabilities faced in the current environment?
- What are the specific security challenges and considerations?
- What are the key areas for improvement in SJIBPLC's ICT security framework, and what specific recommendations can be made to enhance its security posture?

These research questions served as a framework for my internship activities and guided my observations, analysis, and recommendations. By addressing these questions, I hope to contribute to a deeper understanding of ICT security within the banking sector of Bangladesh and provide valuable insights for SJIBPLC.

Rational of the Report: Knowledge becomes truly meaningful when it combines both theory and practice. Theoretical learning reaches its full potential when applied in real-world situations. As our education system is predominantly focused on textbooks, incorporating practical orientation programs as an academic component provides a valuable opportunity for

hands-on experience. Such programs create a “win-win” scenario for both educational institutions and organizations by fostering mutual benefits. Students gain essential skills and preparation for the job market while organizations benefit from fresh perspectives and contributions. This report aims to analyze the practical experiences gained during the internship at Shahjalal Islami Bank PLC, Corporate Head Office. Specifically, it focuses on an appraisal of the bank’s ICT security operations. The primary objective is to gain a comprehensive understanding of ICT security practices and identify areas for improvement, bridging the gap between academic knowledge and professional application.

## 3.2 Literature Review

This section reviews existing literature relevant to ICT security in the banking sector, with a particular focus on the context of Bangladesh’s banking financial industry. It explores what is already known about the topic and identifies areas where further research and investigation are needed, aligning with the objectives of this internship.

Already published knowledge: Studies so far mainly emphasize the diverse range of threats facing banks, including malware attacks, phishing scams, denial-of-service attacks, and insider threats. A primary subject that always comes to limelight whenever ICT security of Bangladesh is talked about is “negligence in awareness of employees of Bangladesh Bank during the infamous Bangladesh Bank heist” (Bangladesh Bank Money Heist). Another issue is the lack of awareness of ICT security policy as highlighted by Abdullah Al Mamun, Jamaludin Bin Ibrahim and Sk Mamun Mostofa in their article Cyber security awareness in Bangladesh: an overview of challenges and strategies. They also highlight how Bangladesh Bank is now highly concerned about employee awareness and relevant procedures in their paper. Similar relevant studies have examined the specific challenges faced by the banking sector in developing countries, including Bangladesh. These studies suggest that banks in these regions often face unique challenges, such as limited resources, a shortage of skilled cybersecurity professionals,

and a rapidly evolving threat landscape. However, this area of research is still relatively very low in number and there is a need for more in-depth investigation.

Potential addressing points: hopefully, this report will be able to address if not all but some of the above mentioned points to a good extent. In bullet points I suggest the following:

- Increase research in this specific sector.
- Constant monitoring of evolving threat landscapes.
- Possible solutions for effective employee awareness.
- How ICT infrastructures plays important role for effective cyber security and how can they be improved.
- The need for field specific training to develop skilled ICT security officials.
- How to allocate the required budget for ICT security solutions.
- Possible ways to develop a good digital forensic analysis team and solutions.
- Where and how relevant compliance can be strengthened.

## 3.3 Details Methodology

This report employed a mixed-method approach, combining qualitative and wherever possible quantitative data collection and analysis techniques to gain a comprehensive understanding of the ICT security landscape at Shahjalal Islami Bank PLC (SJIBPLC).

Data Collection: Direct observation was the key component of the data collection process. The daily operations of the ICT Security Department, including security protocols, incident response procedures, network monitoring activities, and access control measures were primarily observed whenever it was possible. Notes were taken down during these observations to document key processes and identify potential areas of improvement.

Document Analysis: A review of existing documentation was a good scope. This included examining the bank's ICT security policies, procedures, risk assessment reports, vulnerability scan reports, penetration testing reports, incident response plans, audit reports (both internal and external), and relevant regulatory compliance documents. This analysis helped to understand the bank's established security framework, identify compliance gaps, and assess the effectiveness of current security measures.

Analytical Approach: As already mentioned the analysis focused on identifying the strengths and weaknesses of SJIBPLC's current ICT security framework. The findings from the data collection and analysis were triangulated to ensure the validity and reliability of the observations found. This involved comparing information from different sources (observations and documents analysis) to develop a comprehensive understanding of the issues. The analysis then considered relevant industry best practices, regulatory requirements, and emerging threats to provide context and informed recommendations based on the comparisons.

Interviews: Semi-structured and casual interviews were conducted with key personnel within the ICT Security Department. These interviews or frequently asked questions explored their perspectives on the bank's security posture, challenges faced, and potential solutions.

Sampling Population: The population for this study included all personnel involved in ICT security operations at SJIBPLC, however mainly focused on the relevant documentation pertaining to the bank's ICT security infrastructure and practices.

Also, for ethical reasons and as per SJIBPLC’s policy for maintaining confidentiality all information and relevant data collected will be treated as highly confidential and will not be published or used for reasons other than for this report only.

## 3.4 Departmental Functionalities

Usages of Information Technology is being rampantly increased by financial institutions in Bangladesh. Hereafter, considering the present context and business growth of such institutions, they have established an ICT Security Department that is responsible for safeguarding the bank's Confidentiality, Integrity and Availability (the CIA triad of information security) of electronic data in ICT enabled systems from potential cyber-attack, and will continuously work to make the bank resilient to cyber threats and other similar threats. Similarly, Shahjalal Islami Bank PLC have also established the ICT security department, which is completely separated from the IT division. The department's reporting line is completely different from that of the IT division to avoid conflict of interest in taking crucial decisions that requires a balance between rapid business growth decisions and ensuring security.

As per the SJIBPLC banking policy and guideline, ICT Security Department's primary objective is to make sure that the bank is compliant with the ICT Security policy Version 4.0 of Bangladesh Bank. At the same time, ICT Security Department is responsible for implementing, monitoring, and continuously improving security measures to protect the organization from evolving cyber threats and operational risks. The department is fully dedicated to handle all the compliance related projects such as the ISO 27001 certification, PCI-DSS certification being the prime ones. And, as per Bangladesh Bank's CIRT (Computer Incident Response Team) it handles additional activities like developing 4$^{th}$ Industrial

Revolution project and managing the SJIBPLC's CIRT response team. Moreover, the ICT Security Department promotes a security-awareness culture through comprehensive training and awareness programs for employees, ensuring they are equipped to recognize and respond to cyber threats. The following organogram proposes an idea of how the SJIBPLC's ICT security department is proposed to operate:

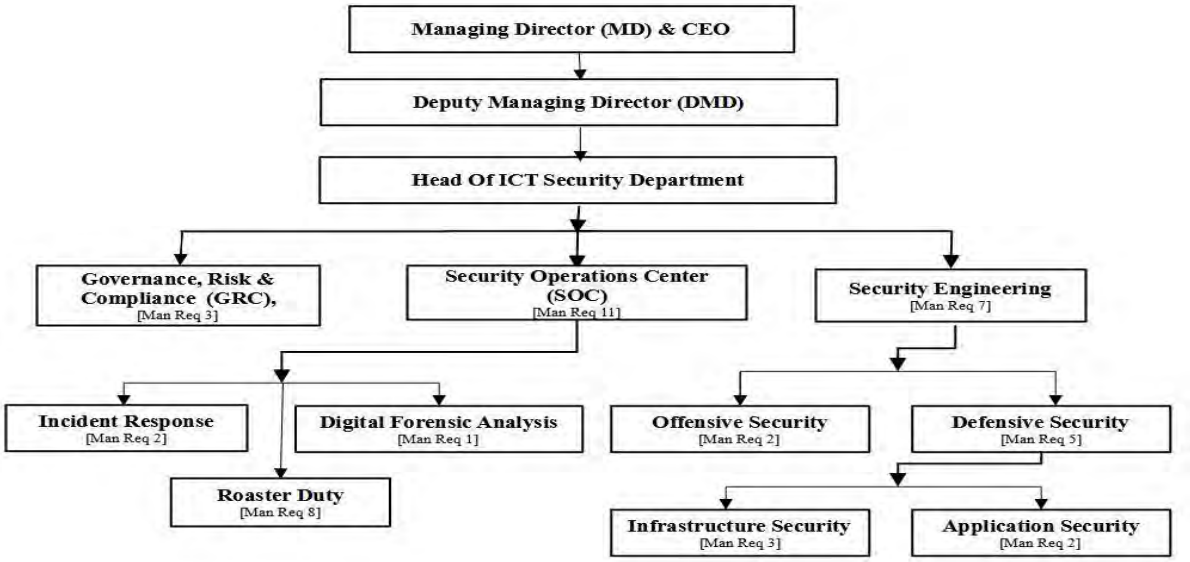



*Figure 4 Proposed Organogram of SJIBPLC's ICT SD*

Understand that the organogram only gives a proposed working manner of how the ICT security department of SJIBPLC is to operate. It does not outline or highlight all the activities that are carried out by the department say for example VAPT is not being shown anywhere in that diagram. However, VAPT falls in the 'Security Engineering' segment. Let's have a breakdown look at the functionalities as per the organogram:

1. Governance, Risk & Compliance (GRC):
    - Ensure compliance with regulatory requirements (e.g., Bangladesh Bank, PCI DSS, ISO 27001) and internal audit.
    - Develop and maintain security policies, standards, and procedures
    - Conduct regular risk assessments and implement mitigation strategies & others
    - Manage security awareness programs and training initiatives

- Oversee security budget allocation and resource management
- Manage security certifications and accreditation
- Vendor Management
- Perform departmental administration work.

2. Security Operations Center (SOC):

- Monitor ICT Infrastructure for threats and anomalies
- Conduct security incident detection and response
- Perform threat intelligence analysis and correlation
- Implement security incident response plans
- Conduct forensic investigations
- Manage security tools and technologies
- Provide security incident reporting and metrics
- Ensure 24/7 monitoring

#Incident Response:

1) Coordinate incident response activities and security incidents with ITD and related departments
2) Conduct case analysis; involving the incident identification, containment, eradication, recover, restore and finally resolve the as seen appropriate based on case.
3) Reduce Mean Time to Containment.
4) Ensure threats are eradicated and systems are maintained accordingly.
5) Conduct post-incident analysis and lessons learned
6) Develop and maintain incident response plans.

#Digital Forensic Analysis:

1) Collect, preserve, and analyze digital evidence
2) Support legal investigations

3) Develop forensic investigation methodologies via SOC tools

3. Security Engineering:

- Provide Offensive and Defensive security over digital infrastructure of the bank.
- Vendor management.
- Project implementation

#Offensive Security:

- Perform Vulnerability Assessments on system
- Perform Penetration Testing on systems
- Involve in Cyber Ethical Hacking

#Defensive Security:

1) Protects information assets
2) Protects systems from threats.

Endpoint protection, Static and dynamic application security testing tools, vulnerability scanners

*Infrastructure Security:

1) Ensures secured IT network infrastructure, servers, OS and endpoints.
2) Focuses on PAM, EDR/XDR, MFA and such.
3) Ensure Proactive security of system.

*Application Security:

1. Secures software applications and data.
2. Script checking and Source Code scanning of all applications.
3. Involves DB and OS layer security.
4. Ensure email security, web & network applications security at the 7th layer of OSI model.

The ICT Security Department at Shahjalal Islami Bank PLC serves as the backbone of the organization's cybersecurity framework, encompassing Governance, Risk & Compliance (GRC), Security Operations Center (SOC), and Security Engineering functions. It ensures regulatory compliance, implements robust security policies, and manages risk through proactive assessments and mitigation strategies. The SOC provides 24/7 monitoring, incident detection, and response while leveraging threat intelligence. Security Engineering focuses on protecting the bank's digital infrastructure, including offensive and defensive measures, such as penetration testing, vulnerability assessments, and endpoint protection.

Furthermore, the department ensures infrastructure and application security by safeguarding IT networks, servers, and software applications through advanced tools like PAM, MFA, EDR/XDR, and static and dynamic security testing. The above outlines a pretty good idea of the department functionalities as in the activities it carries out. However, it does not outline all the daily tasks to the pin point, say for example the department is responsible for role based access management of all the employees of the bank. The department provides permission of Access Service forms but is not highlighted in the above as it falls in the “governance, risk and compliance”. That being said the outlined model should give a good idea as to the departmental activities as a whole.

Moving on to the departmental achievements for the bank:

1. Compliance:

- Bangladesh Bank ITD infrastructure Rating 2.0. Remarks: Satisfactory,
- ISO 27001:2013 ISMS Standardization,
- Payment Card Industry- Data Security Standardization,
- SWIFT CSP
- SJIBPLC’s ICT Security Policy Version 8.0.

2. Technological Advancements/Software Implementation:

- PAM Implementation, continual process,
- WAZUH SIEM Implementation, continual process,
- Ensuring Vulnerability Assessments of the bank, continual process,
- Ensuring Penetration Testing of the bank, continual process,
- Physical Implementation OF SJIBPLC's SOC,
- Central Access Management, continual process,
- Third location Backup Storage Implementation, continual process,
- End-Point Security Monitoring under Trend Vision One, Apex One, Deep Security & Trelix

The above achievements are only a small description as to the performance of the department. By integrating compliance, operations, and engineering in the department ensures a secure, resilient, and compliant IT environment, effectively mitigating cyber risks while supporting the bank's digital growth.

## 3.5 Assigned Internship Period Duties

This chapter provides a detailed account of the tasks and responsibilities I undertook during my internship in the ICT Security Department at Shahjalal Islami Bank PLC. Throughout the internship, I was entrusted with various responsibilities, including and not limiting to assisting in the monitoring & evaluation of security systems, identifying potential vulnerabilities and ensuring compliance with organizational security policies. Additionally, I collaborated with the team members on ongoing projects the major one being the ongoing "ISMS ISO 27001" and "PCI-DSS" recertification process; at the same time contributed to the analysis of security incidents, and supported the development of preventive measures to mitigate risks. The activities assigned to me were carefully designed to align with the department's operational

priorities and offered valuable insights into the complexities of managing ICT security in a dynamic banking environment.

The activities not only enhanced my technical skills but also deepened my understanding of the strategic role ICT security plays in safeguarding organizational assets. This chapter outlines these tasks in detail' let's have a group wise look at this activities:

- **Roll-Based Access Management (RBAM) & Change/Maintenance Permission**: The primary and key daily task, I was dedicatedly assigned was the RBAM. RBAM involved managing user access permissions based on their job roles within the organization. Alongside this, I was also in charge of verifying all the system changes were properly taken approval of and executed to the full.
- **Monitoring and notifying about daily issues from end-points**: Alongside RBAM and Change maintenance; I also assisted in end point monitoring, as in, I monitored all the devices via security software like trend micro, apex central and others. From the endpoints, I was able to view, if anyone was trying to access any unauthorized portals, if anyone was connecting USB devices to their computers or if any endpoint had a non-approved software as an example. Henceforth, after detection, notify the dedicated departments about the issue and ask them to take proper action and ensure thereby after execution.
- **Vulnerability Assessment and Penetration Testing (VAPT) procedure assist:** VAPT is a two-fold process designed to identify vulnerabilities in systems, networks, and applications and assess their exploitability through controlled penetration testing. The VAPT process is essential in ensuring the security and resilience of Shahjalal Islami Bank's ICT infrastructure. SJIBPLC uses "Tenable,IO" software as their VA tool and "CoreImpact" as their PT tool. The reports generated after carrying out VAPT on systems or critical end points were then reviewed and the required actions were then forwarded to be taken by the required departments.

Alongside the above mentioned primary activities, I also assisted in the on-going projects as already mentioned. However, another activity that should be mentioned is ICT security awareness at branch level. The security awareness initiatives aims at to educate both IT officials and users on the importance of cybersecurity and best practices for maintaining a secure digital environment. A training program was also organized where I helped in the contents outline of the program. The content included password maintenance, internet & email security, SWIFT usage policy, cyber security laws and modern day fraud & cyber threats awareness. Besides the training program, I was also responsible for creating screen saver backgrounds with relevant awareness posts and so on. Furthermore, I also assisted with the drafting and reviewing reports based on the finalized reports by Bangladesh Bank. Additionally, I assisted in compliance and auditing tasks, ensuring that the organization adhered to regulatory requirements, internal policies, and industry standards. To sum up my activities, it was mainly involved with the access and changes of the system. However, I was also invested in giving time to the other mentioned activities; all this activities provided me with insights into the importance of practical experience of the ICT Security department's activities.

This opportunity not only enhanced my technical and analytical skills but also deepened my understanding of the strategic importance of ICT security in ensuring organizational resilience and regulatory compliance. The knowledge and experience gained during this internship will serve as a solid foundation for my future career in the field of ICT security.

## 3.6 Learning Outcomes

The learning outcomes of the internship experience at Shahjalal Islami Bank PLC encapsulates the knowledge, technical skills, and personal growth I have achieved. Each task and activity provided unique insights, contributing to my development as an aspiring IT security professional. Below is a detailed summary of the learning outcomes:

- Understood the basic ICT infrastructure of banking organization, how are all braches connected with the mainframe. Alongside, how are ATM devices and alongside all other peripheral devices are connected via different mainframe.
- The importance of compliance maintenance and how Bangladesh Bank is now directly involved and dedicated to the improvement of ICT security of the banking industry.
- The new ICT guidelines role in taking mandatory training sessions on awareness of ICT security threats and how to engage with employees at all levels to ensure that all known loopholes are covered and also to identify the unknown ones.
- Acquired practical skills in identifying and evaluating vulnerabilities in IT systems, applications, and networks.
- Gained expertise in penetration testing using Core Impact, including simulating cyberattacks to identify critical weaknesses.
- Gained insights into emerging security concerns, including cloud security, cybersecurity threats, and the challenges posed by emerging technologies
- Able to understand banking organization's ICT security policy, enhancing understanding of security frameworks and regulatory compliance
- Learned the importance of access control in ensuring organizational security. Gained experience in reviewing, evaluating, and processing access service forms to ensure proper role-based permissions.
- Developed an understanding of the importance of compliance in maintaining operational integrity and security.
- Understood the role of education in fostering a culture of security within an organization.
- Gained knowledge on critical topics, including password maintenance, email security, safe internet usage, fraud prevention, and cybersecurity laws

- Gained experience in identifying discrepancies and recommending corrective measures to strengthen compliance practices.
- Became familiar with the operational challenges of maintaining robust ICT security in a dynamic banking environment.
- Learned the importance of maintaining accurate and up-to-date documentation for regulatory and operational purposes. Improved my ability to align security policies with organizational needs and regulatory guidelines.
- Enhanced my technical skills in areas like security scanning, access management, and policy development. Worked closely with colleagues to address and resolve IT security challenges. Enhanced my technical skills in areas like security scanning, access management, and policy development. Alongside, gained soft skills such as communication, teamwork, and professionalism, which are critical for success in the corporate environment.
- The experience and skills acquired will enable me to contribute effectively to IT security operations in any professional setting
- To keep up to date with daily cyber threats and incidents occurring globally and keep the department notified as seen appropriate.

A well-rounded understanding of ICT security practices, ranging from vulnerability assessment and policy development to compliance and security awareness came into my knowledge base during this period. The skills and knowledge acquired during this experience will not only enhance my technical competence but also prepare me to contribute effectively to IT security operations in any professional setting.

## 3.7 Departmental Observations and Suggestions

This chapter presents a comprehensive analysis of the observations made during my internship in the ICT Security Department of Shahjalal Islami Bank PLC. It highlights the strengths and areas for improvement within the department's operations, processes, and security practices.

Drawing from firsthand experiences and practical exposure, the chapter also provides actionable suggestions aimed at enhancing the department's efficiency, compliance, and overall security posture. These recommendations are aligned with industry best practices and the evolving landscape of cybersecurity to ensure the department continues to meet its strategic objectives effectively. It is vital to understand that like any other department, trying to do their work properly, ICT security department also faces hurdles/inconveniences, has certain lacking and is not without its own challenges to operate properly.

Below I'll try to highlight certain crucial observations and findings, from my perspective, of the ICT security department.

1. **Strong Compliance with Bangladesh Bank guidelines**: It has demonstrated exceptional strength in maintaining compliance with regulatory requirements set by Bangladesh Bank. It is of high essential to note that, it has maintained its exceptional Grade 2 certification, two years in a row. This recognition showcases the department's diligence in ensuring all systems, processes, and practices meet or exceed regulatory expectations, thereby mitigating risks and fostering a secure operational environment.

   **Room for Improvement**: however, ICT security department of SJIBPLC is constantly opting to achieve better results and is targeting to achieve the top tier prestigious Grade-1 certification of ICT infrastructure compliance.

   A "Grade-1 certification" of ICT infrastructure will bring the bank to the front line among the leading banks of Bangladesh. It is highly vital that ICT security department keeps on trying to improve and that it will get the limelight via such certifications. Moreover, the compliance certification will also ensure higher reputation and trust in its clients
2. **Compliance accomplishments of international certification**: ICT security department has achieved ISMS ISO 27001 certification and PCI-DSS certification. This certification has hugely increased the reputation of the bank. At the same time, it has helped the bank to

enhance the security of the bank's data and the system. Also, the PCI-DSS certification, has ensured the card user safety of the bank.

**Room for Improvement**: ICT SD is now looking to achieve the newer versions of this certifications as they have recently been reviewed by their owned regulators.

The newer versions will ensure data security with the context of newer modern day platforms. Integration of AI threat protection and more

3. **Advanced threat monitoring capabilities:** The department has acquired top of the tier line security tools, being centrally operated from its Security Operations Center (SOC) room. With high level end point security tools like "Trellix" and "Trend Micro". The bank has a robust monitoring security infrastructure.

   **Room for improvement:** The department is at the moment working on acquiring a System Information and Event Management (SIEM) Platform solution. Alongside, the Privilege Access Management (PAM) solution has only recently been integrated and sent to live, waiting for a full capacity use level. Moreover, the department is looking forward to acquiring all sorts of security solutions like UEBA, SOAR, TIF and so on to further enhance itself.

   The solutions are necessary for creating a better impact in the security of the bank. However, acquiring this solutions are no easy feat, thus the bank is always constantly trying to understand how to acquire the best solutions.

4. **Security awareness initiatives amongst all its employee**: The initiatives are designed to educate staff and IT officials on the critical aspects of cybersecurity, equipping them with the knowledge and skills necessary to recognize and mitigate potential threats. It conducts awareness training sessions for IT officials and staff using both virtual (via zoom) and in-person platforms (at Training Academy). Online sessions are held via Zoom to ensure accessibility for employees across different locations, while physical training programs are

organized at the bank's dedicated training academy for more hands-on and interactive learning. The training focuses on essential topics, including password management, email security, internet usage best practices, fraud prevention, SWIFT usage, and awareness of cybersecurity laws. IT officers at branches are trained in a tiered manner, with IT Officers 1 and 2 receiving targeted instruction based on their roles and responsibilities. To foster ongoing awareness, specific roles are assigned to these officers, encouraging them to act as security champions within their branches, thereby extending the impact of the training initiatives across the organization. Understanding that there will always be resistance to change, as newer models of tech even though efficient and effective but still a somewhat unwanted in the workplace because of not being accustomed to it. Thus, encouraging everyone to accept the changes than to resist is highly important.

**Room for improvement**: Introducing more advanced and scenario-based training modules can better prepare employees for real-world challenges, such as phishing simulations and incident response exercises. Sending test phishing mails to employees of the bank is also a part being looked into. Incorporating an outline or course style or training style that brings together all this approaches would be highly helpful for the bank as a whole.

This holistic approach would enhance overall vigilance and reduce the likelihood of human errors, ultimately contributing to the bank's resilience against cyber threats. By refining and expanding its security awareness initiatives, the bank can not only mitigate risks more effectively but also empower its workforce to become proactive defenders of its ICT infrastructure.

5. **Budget Capabilities and trade-offs:** A crucial observation is the impact of budget constraints on the department's ability to implement comprehensive security solutions. These constraints often necessitate trade-offs, influencing the selection and deployment of critical security tools and technologies. A notable example of this is the department's

decision to acquire a standalone Security Information and Event Management (SIEM) solution instead of a more robust, integrated security package that includes Security Orchestration, Automation, and Response (SOAR), File Integrity Monitoring (FIM), and User and Entity Behavior Analytics (UEBA) alongside SIEM. While the SIEM solution enhances the department's ability to monitor, detect, and respond to security incidents, the absence of complementary tools like SOAR limits automation capabilities, and the lack of FIM and UEBA leaves gaps in detecting file-level changes and anomalous user behavior.

**Room for improvement:** To address these challenges, the department could explore phased implementation of additional tools, prioritizing solutions that align with the bank's risk profile and operational needs. Leveraging cost-effective alternatives like modular upgrades to the existing SIEM system can also help enhance functionality within budgetary constraints. This may in turn actually even provide more security than managing a lot of security solution at the same time to avoid complexity.

6. **Skilled man power and managing them accordingly:** Another critical observation in the ICT Security Department of Shahjalal Islami Bank PLC is the shortage of skilled manpower, which poses significant challenges to maintaining an efficient and secure ICT environment. The recruitment and retention of experienced security professionals are constrained by market competition and the specialized nature of cybersecurity roles. This shortage often results in increased workloads for existing staff, potentially impacting the department's overall efficiency and effectiveness. Additionally, onboarding and training new security officers require considerable time and resources.

   **Room for improvement:** To address this issue, it could benefit by collaborations with external training providers, certifications from recognized institutions, and the adoption of e-learning platforms can expedite the skill development process. Additionally focus on how to ensure good retention rate of the department is highly important. By strategically

addressing the shortage of skilled manpower and optimizing the training process, the ICT Security Department can enhance its operational resilience and ensure long-term sustainability in safeguarding the bank's assets

The observations highlighted in this chapter underscore the strengths and challenges of the ICT Security Department at Shahjalal Islami Bank Limited. While the department demonstrates commendable compliance with regulatory requirements and proactive security initiatives, budget constraints, manpower shortages, and training challenges reveal areas for improvement. Addressing these issues through strategic investments, skill development programs, and process optimizations can further enhance the department's ability to safeguard the bank's ICT infrastructure effectively.

## 3.8 Conclusion

The internship at Shahjalal Islami Bank PLC's ICT Security Department has been an invaluable experience, providing me with a firsthand understanding of the complexities and critical nature of IT security in the banking sector. This journey not only deepened my technical knowledge but also honed my analytical, collaborative, and communication skills, all of which are essential for a career in ICT security. I had the opportunity to observe and participate in several vital activities, such as Vulnerability Assessment and Penetration Testing (VAPT), roll-based access management, and the development of security awareness programs. These tasks helped me understand the importance of proactive security measures, compliance with regulatory guidelines, and the role of structured policies in safeguarding the bank's digital infrastructure. I also assisted in ensuring adherence to Bangladesh Bank's regulations and observed how strategic decision-making impacts the overall security posture of the organization. The experience exposed me to real-world challenges, including budget constraints, manpower shortage management strategies, and the evolving threat landscape. These insights emphasized

the importance of strategic planning, continuous training, and the adoption of advanced security technologies to address these issues effectively.

Alongside this, I would again like to take a moment to be thankful to all the people I have worked with during this time. All the experienced professionals have helped me very dearly and taught me how to adopt to the corporate culture. This not only further enriched my understanding of the ICT security domain but also real life scenarios and understanding of the work culture of Bangladesh. Moreover, the collaborative nature of the work environment improved my interpersonal and communication skills. Moving on to the MBA program, as a student of the MBA program majoring in Information Technology Management (ITM), this internship has been instrumental in bridging the gap between theoretical learning and practical application.

In conclusion, the internship at Shahjalal Islami Bank PLC has been a transformative experience. It has equipped me with the technical skills, practical insights, and professional values needed to excel in the field of ICT security. The knowledge and experience gained during this period will undoubtedly serve as a strong foundation for my future endeavors, enabling me to contribute meaningfully at any place. I am grateful for the opportunity to bepart of such a dynamic and essential department, and I look forward to building upon this experience as I continue my professional journey. These experiences have not only contributed to my professional growth but also instilled a deeper appreciation for the importance of cybersecurity in the banking industry.

## References:


1. Display Company Information | Dhaka Stock Exchange. (2025). Dsebd.org. https://www.dsebd.org/displayCompany.php?name=SHAHJABANK
2. Shahjalal Islami Bank. (n.d.). Sjiblbd.com. https://sjiblbd.com
3. Shahjalal Islami Bank PLC. (2022). Facebook.com. https://www.facebook.com/Shahjalal.Islami.Bank.Bd
4. Hossain, M. A., Sarker, M. D. A., Hossain, M. S., Shaon, M. A. R., Hossain, M. S., Rayhan, M. M. H., & Astudillo, J. G. S. Bangladesh Bank Money Heist: A Concern of Cybersecurity System of Bangladesh Bank and Way Forward
5. Al Mamun, A., Ibrahim, J. B., & Mostofa, S. M. (2021). Cyber security awareness in bangladesh: an overview of challenges and strategies. Int. J. Comp. Sci. Informat. Technol. Res, 9(1), 88-94.

# Appendix:

Informal Questionnaire set & response

1. How do you feel guidelines from Bangladesh Bank and international certifications translate into practical security operations? Does it make your job easier, or do you find any challenges in implementing them?

2. The department has some really advanced threat monitoring capabilities. What would you say is the biggest benefit of these systems, and on the flip side, what's one thing you wish they could do better or that would make your analysis even more effective?"

3. Cyber threats are always evolving. When you think about the most challenging threats you've faced recently, what kind of skills or new knowledge do you feel are most needed on the team right now to tackle them effectively?

4. The security awareness initiatives across the bank seem to be really well-received. What's your take on how these programs are working to make all employees more cyber-aware, and what kind of feedback do you get from other departments?

5. if you could have a 'wish list' for the department's resources for the next year—whether it's for new tools, training, or staffing—what would be at the top of that list and why?

Response from Transcript 1:

1."Our strong compliance with BB guidelines and international certifications is our foundation. It sets a clear framework and standard for our work. It doesn't eliminate challenges, but it gives us a clear path to follow and proves our commitment to stakeholders."

2. "Our advanced monitoring systems are excellent for real-time threat detection. They give us the visibility we need."

3. " The biggest need right now is for people with specialized skills in threat intelligence and advanced incident response—analysts who can hunt for threats, not just react to alerts."

4. "The programs are working very well. We've seen a noticeable drop in phishing click rates, and employees are reporting suspicious emails more frequently. Other departments see us as a partner in security, not just a blocker."

5. "Top of the wish list would be a dedicated budget for continuous, hands-on training and a plan to hire more specialized analysts. The talent is out there, but we need the resources to attract and retain them."

Response from Transcript 2:

1. Compliance is non-negotiable. It gives us a benchmark to measure against. The challenge is often translating the broad guidelines into very specific technical controls, but our certifications shows that we are performing.

2. The biggest benefit is the early warning we get. I wish we had more automation for routine tasks so our team could focus more on advanced threat detection, not only alerts.

3. Beyond technical skills, we need people who are great at problem-solving and can think like an attacker. It's a specialized mindset that you can't always find, and training for it requires significant investment.

4. The awareness programs have been a huge success. Employees are our first line of defense. They're more vigilant now, and it's built a culture where everyone feels they have a role in security

5. Budget is always key. We need to invest more in our human capital—hiring and training. New tools are important alongside the right people with the right skills are the biggest assets for our future security.