

**Terms of Reference for Chief Information Security Officer (CISO)
of Cyber Security Unit, Bangladesh Bank.**

Context:

Bangladesh Bank (BB), the authority regulating Bangladesh economy's monetary and financial sector, uses an extensive, integrated range of Information Technology (IT) solutions, inter alia including Core Banking system (CBS), Enterprise Resources Planning (ERP), Enterprise Data Warehouse (EDW), Automated Clearing House (ACH), Electronic Fund Transfer (EFT), Real Time Gross Settlement (RTGS), National Payments Switch (NPS), Credit Information Bureau (CID), AML/CFT Financial Intelligence Unit (FIU) system and Cross Border Dealing and Payments (CBDP) system.

With a view to enhancing the security safeguards of the IT solutions and services across its entire range of functional areas, BB intends to hire a well qualified experienced professional as Chief Information Security Officer (CISO) to lead its proposed new Cyber Security Unit (CSU). Reporting to the senior management (Deputy Governor, Governor), the CISO will (i) steer execution Of BBs ongoing cyber security strengthening program and conduct subsequent annual reviews thereof, bringing up modification needs in light of unfolding new security threats, if any; and (ii) steer reorganization of BB's cyber security resources and capabilities into a strong, effective CSU proactively addressing the security concerns of IT facilities and services in all of BB's functional areas, conforming to relevant national and global norms and best practice standards.

The CISO will lead a team dedicated for conducting security related issues within Bangladesh Bank as well as provide necessary directive to the banking and financial sector of Bangladesh.

Roles and Responsibilities: The CISO will be responsible for developing and implementing information security programs, which include procedures and policies designed to protect IT systems/platforms, enterprise communications, and assets (mainly data) from both internal and external threats, with strong focus on process and risk management. His/her duties and accountabilities will include (but not necessarily be limited to):

1. Overseeing the design and implementation of BB's information security infrastructure to monitor IT installations and systems for detection and prevention of unauthorized access and use; steering to completion of BB's ongoing cyber security strengthening program and conducting annual reviews thereof to identify, assess and coordinate remediation of weaknesses in BB's IT security systems;

2. Shaping up a robust new CSU covering the areas of Security Engineering (SE), Security Threat and Vulnerability Management (STVM), Information Security Operations Center (ISOC), Security Information and Event Management (SIEM), Financial Sector wide Critical Incident Response Team (CIRT) and Cyber Security Intelligence (CSI); putting in place adequate documented processes, procedures and internal technical controls in all these areas;
3. Assessing knowledge/skill enhancement needs for staff in the new CSU, setting up appropriate training routines of cyber security capacity building with up-to-date understanding of emerging trends in information security technology;
4. Ensuring BB's response-preparedness to IT security incidents through development and regular exercise of incidence response processes & procedures, fostering leadership skills in getting things done in inter-departmental/inter-agency team environments;
5. Fostering and facilitating a cyber security risk aware culture among all staffers in BB offices and departments, ensuring effective, efficient and balanced protection of all BB information assets;
6. Guiding and assisting the development of security standards for IT platform in conformance with BB's IT architecture, risk profile, and policy requirements;
7. Interfacing with business units and IT stakeholders in identifying requirements and assessing their applicability to BB's IT infrastructure;
8. Identifying efficiencies to improve the performance and responsiveness of BB's IT security work programs;
9. Reviewing and offering suggestions on setting of technical requirements in procurements of IT equipments/consumables in conformance with BB's Information Security architecture and risk profile;
10. Designing short-term and long-term security policy and implementation plan for Bangladesh Bank;
11. Taking necessary measure to upgrade and maintain security infrastructure of Bangladesh Bank according to the implementation plan;
12. Guiding and facilitating regular security testing on the ICT infrastructure of Bangladesh Bank, auditing existing systems and providing comprehensive risk assessments;
13. Ensuring regular review of logs of user activities in order to recognize suspicious behavior;
14. Designing automatic (machine learning based) monitoring and financial fraud detection policy;
15. Designing monitoring plan of the implementation process of security policy by Banks and NBFIs of Bangladesh;
16. Guiding Banks and NBFIs of Bangladesh to take appropriate preventive measures in case of any security threat/incident at any of the financial institute in Bangladesh or relevant organization abroad;
17. Facilitating security awareness program for all employees of the bank at regular interval;

18. Preparing a team for digital forensic investigation to investigate any incident.
19. Integrating IT systems development with security policies and information protection strategies;
20. Collaborating with key stakeholders to establish an IT security risk management program;
21. Anticipating new security threats and stay-up-to-date with evolving infrastructures;
22. Acting as a focal point for IT security investigations and directing a full investigation with recommended courses of action;
23. Prioritizing and allocating security resources correctly and efficiently;
24. Leading the following activities of Bangladesh Bank:
 - i. Management of Security staff and Security Operations Centre (SOC).
 - ii. Security and Business Continuity and Disaster Recovery Planning (BCDR).
 - iii. Authentication, identity and access management.

Eligibility:

(A) Nationality: Bangladeshi Nationals are eligible to apply.

(B) Educational Qualification:

A Bachelor's/Master's degree in CSE from a reputed university with at least 12 years experience on IT and network security (at least 10 years experience in case of Master's Degree holders). Third division/Class at any level of education will not be considered.

(C) Knowledge & Experience:

1. At least 10/12 years of working experience in the domain of network and information security and IT risk management of a central bank, any internationally reputed bank, large public/private bank, large financial organization, or telecommunication sector;
2. Experience in designing IT and network security infrastructure for a large financial organization, leading VAPT and/or forensic investigation as employee or external testing team for an IT-rich large organization.
3. following hard skills are required from the CISO:
 - i. Windows, UNIX and Linux operating systems.
 - ii. Firewall and intrusion detection/prevention protocols
 - iii. Secure coding practices, ethical hacking and threat modeling
 - iv. Network security architecture development and definition
 - v. knowledge of third party auditing and cloud risk assessment methodologies.
 - vi. Knowledge/experience in software development, security testing of applications should be considered added qualification.
 - vii. Knowledge/experience in research on automatic vulnerability/fraud detection mechanisms is preferable.
4. The following soft skills are required from the CISO:
 - i. Ability of organization, process-oriented thinking, strategic planning and creative attack.

- ii. Interpersonal and negotiation skills.
 - iii. Capability of directing a team, collaborating with high-level executives and building relationships with a diverse set of departments.
 - iv. CISOs must be able to juggle the pressures of legal/regulatory requirements, financial constraints and technological adoption.
5. Strong knowledge of emerging technology and state-of-the art IT practices in a decentralized institution with stakeholders in multiple business lines of varying extent of risk appetite and tolerance;
 6. Up-to-date best practice experience with IT infrastructure, security systems & services, and emerging technologies (i.e. Cloud/Mobile Computing);
 7. Demonstrated experience in strategic technology planning and leading enterprise security infrastructure design, implementation, and operations for a large financial organization ensuring alignment with strategic objectives;
 8. Must have industry certification related to security. Certificate should be from the following list: LPT, CASP, CCNA, CyberOPS, CSA+, CISSP, CISM, GSEC, CEH, CHFI, CIPP, MBCP, CISA, GSLC, CCISO, CGEIT;
 9. Proven managerial skills including staffing and resource utilization, performance management, issue resolution, motivating others, forecasting and planning;
 10. Well-developed interpersonal skills and ability to interact effectively with all levels of the organization;
 11. Demonstrated knowledge and experience in systems and business processes, policies and procedures, relevant software application systems, operating systems. security appliance. hardware configuration and network architecture of a central bank/other internationally reputed bank or financial institution;
 12. Demonstrated conceptual, analytical and innovative problem-solving ability;
 13. Demonstrated success working as a leader to facilitate the success of others beyond his/her unit, preferably in a multi institutional environment;
 14. High people management and leadership skills evidenced by a proven track record and positive references;
 15. Demonstrated ability to deliver key strategic programs and projects with quality results under tight deadlines, and to provide focus, vision and leadership on tasks at hand. Demonstrates a high level of motivation, confidence, integrity, and responsibility;
 16. A sustained record of achieving significant operational impact/results and leading and managing complex programs and projects requiring cross-functional and cross-institutional collaboration;
 17. Proactively identifying and acting upon risks and opportunities for continuous improvement and risk mitigation;
 18. Excellent communication skills, demonstrated ability to express technical and business concepts, ideas, feelings, opinions and conclusions in a clear, objective and engaging manner in high-level settings;
 19. Highest personal and professional integrity, as demonstrated through strong personal values, as well as consistent words and actions;

20. Can-do attitude and willingness to take accountability and hold others accountable for results;
21. Strong organization skills to ensure alignment across units and optimal impact on the organization as a whole;
22. A team player with the ability to distinguish between what is and is not critical, and to balance on both strategic and short-term issues.

(D) Language proficiency: Applicants for this position must have proficiency in Bangla and English.

(E) Age limit: Applicant's age must be in the range of 40 to 55 years as on **May 05, 2019**.

Salary/benefits: Consolidated Salary BDT 4,00,000.00 (Including Tax) Per Month. Bangladesh Bank will pay the VAT payable on the salary. Full time transport facilities from Bangladesh Bank's transport pool will be provided.

Terms of Appointment: Initially for up to three years (renewable).

Application process: Interested candidates are requested to send their CV(Annexure-'A') mentioning all educational qualifications and skills related to the job with related documents **no later than June 12, 2019 to General Manager, Human Resources Department-1, Bangladesh Bank, Head Office or e-mail(gm.hrd@bb.org.bd)**. Candidates must have to send attested copy of their certificates of all educational qualification, experience and professional certificates, nationality certificate, National ID card/Smart Card, 3(three) copies of passport size Photographs and related all documents along with the CV. Please note that only Short listed candidates will be notified and invited to participate in the selection process. Applicants have to go through a Viva-Voce process. Incomplete or applications with wrong information will be rejected without any contact with the candidates. Bangladesh Bank reserves the right to accept or reject any or all applications.