



### Job Description

<b>Post Title</b>	ICT Consultant
<b>Duty Station</b>	CBS Headquarter with frequent travel to regions
<b>Assignment Duration</b>	12 months with option to extend
<b>Reports to</b>	General Manager
<b>1- Main purpose for the job</b>	
<p>The aim of this position is to adequately transform the Organization to digital environment and protect the IT assets of the Central Bank of Somalia by recommending and implementing best practice technology, cybersecurity, policies, procedures, and guidelines. The advisor should align the bank's business plans with security controls, processes, and policies, Oracle implementation and Oracle Cloud implementation. The candidate is responsible for setting, developing, and maintaining CBS software, information security management systems policy and program and should be based on ISO/IEC. He/she should ensure the implementation &amp; enforcement of ISMS policies and guidelines. The information security advisor is an individual with a great theoretical and practical knowledge of information security methods, techniques, and products. The ICT advisor is responsible to ensure the bank's systems are maintained in a secure and fully functional mode. The advisor should propose security awareness training programs for business units to ensure the confidentiality, integrity and availability of the information systems are met. He/she must perform system-wide white box testing, evaluate the risk and report accordingly. The advisor must commend state-of-the-art cybersecurity methodologies to harden the security of the bank. Further, he/she is responsible for purposing a strategic information security program and evaluate the knowledge and capabilities of the current ICT security team. To maintain a strong understanding and maintaining objectivity that information security is part of the business, the ideal candidate is capable of leading, building and integrating IT teams and managing information security projects. Moreover, the candidate is a leader with the ability to coordinate personalities, drivers, and constraints. The advisor is an expert in driving and managing project teams and prioritizing work efforts to enable long-term strategic information security effort while balancing operational task.</p>	

## 2- Duties and Responsibilities

1. Establish, develop, and maintain a sound, adequate and up-to-date information security management policy, procedures, and guidelines.
2. Manage the dissemination, training and approval of security policies and practices.
3. Oversee the Bank's information security organization comprising of indirect reports of IT and business operations and direct reports.
4. Ensure information security governance by developing and enforcing hierarchal governance program.
5. Assessment and treatment of security risk by creating and implementing a risk-based process for risk management.
6. Recommend and oversee risk management and information security awareness training programs.
7. Develop a program for roles and responsibilities to ensure information classification, protection, accountability, and ownership.
8. Create strategic risk guidance for IT projects including but not limited to the evaluation and recommendation of technical controls.
9. Oversee incident responses to protect CBS reputation and IT assets.
10. Perform white box security testing to assess current security measurements.
11. Manage security audit testing and evaluate security engineering team.
12. Create a reporting and measurement framework to test the effectiveness and efficiency of ISMS program.
13. Coordinate among audit, HR, legal and information security teams as required to increase the maturity of the security.
14. Advice IT staff to comprehend security audit failures.
15. Advice security staff to guarantee that security is factored into the systems from ground up.
16. Create a strong and professional relationship with the IT security team to apply and develop security controls and implement configurations aligned with security policies.
17. Ensure that information security of the Bank is airtight by recommending third party vendors that provide information security services and products.
18. Awareness of current security trends, practices, laws, and regulations.
19. Ensure monitoring data, system logs, and audit trails are reviewed periodically to comply with policy requirements. Supports application configuration and security setup as needed
20. Plan, Develop and actualize DR and BCP sites
21. Work with Business Continuity management to ensure that the disaster recovery crisis management and business continuity plans drive disaster recovery DR strategy and procedures.
22. Establish and maintain the overall plans for executing all DR procedures and understand their inter dependencies
23. Establish and maintain detailed DR communications and command and control plans through a change management process

24. Work with the IT technical staff to ensure that disaster recovery solutions are adequate in place maintained and tested as part of the regular operational life cycle Develop and understand all testing necessary for a successful DR execution Schedule and lead all DR exercises
25. Provide ongoing feedback for risk management mitigation and prevention Represent disaster recovery cost requirements in the annual budgeting process
26. Regularly report Disaster Recovery activities to upper management Act as liaison for auditing and examination of disaster recovery processes

### 3- Deliverables

1. Provide strategic support to the GM support services as requested.
2. Lead and deliver the Core banking system upgrade
3. Lead and deliver the implementation of the Oracle ERP
4. Review and report on CBS cloud services in view of consolidation and reduce cost
5. Implement and action the IT security recommendation
6. Prepare Strategic change initiatives requiring focused implementation teams.
7. Initiative demands exceeding internal capacity.
8. Knowledge sharing and collaboration with internal teams.
9. Evaluate new tools and techniques and make recommendations to improve real-time and batch data access, transformation and movement across heterogeneous technologies and platforms.
10. Identify opportunities for new initiatives; make recommendations for increasing scalability and robustness of ETL platforms and solutions.
11. Draft, test the BCP plan working as required
12. Draft, test the DR Plan are working as required

### 4- Qualifications and Experience

1. At least Bachelor's Degree in Computer Science or IT; M.S. in information security is preferred.
2. 12+ years of Technology exposure including but not limited to project management, IT security, DR/BCP, IT Service Management and Enterprise Applications Support.
3. 7+ years IT Security as an advisory role in a public or private sector organization in large enterprises, preferably in global financial services
4. 5+ years' experience in technical design and architecture roles in applications or cloud based architecture.
5. Overall 5+ years' experience in Business Continuity and Disaster Recovery
6. Expertise in DR strategy and DR plan builds, Knowledge of IT infrastructure and Data center concepts
7. Knowledge of BC/DR Plan Implementation
8. Experience working on development of Interfaces in finance module, Custom Components, Extension, Shell script and PL/SQL.
9. Must have implemented & Subject Matter Expert for at least 2 Oracle Implementation & Oracle Cloud infrastructure and Core Banking Systems.

10. Current or previous experience in configuring, operating, architecting, and designing security solutions for business and technology initiatives
11. Familiarity and experience in formal security architecture aspects, methodology & frameworks
12. Must demonstrates a sound understanding of vendor technologies, roadmaps and negotiation, and remains current with key IT industry themes and emerging trends

**13. Professional certifications should possess are:**

- a. Certified Information Systems Security Professional (CISSP) recommended.
- b. Oracle Project Management
- c. Oracle Cloud Infrastructure Administration
- d. Check Point Certified Expert (CCSE)
- e. Fortinet Network Security Expert
- f. Cisco Certified Network Associate (CCNA)
- g. Knowledge in Certification Authority
- h. Certified Cloud Security Professional (CCSP)
- i. ITIL Certified

## **5- Key Skills and Competencies**

- 1- The Candidate should have work experience and in depth knowledge of Somalia generally and the sensitivity to the underlying state of fragility and the prevailing challenges in particular
- 2- Oral and written communication.
- 3- Ability to document and analyses requirement.
- 4- Ability to develop communication plans and project status reports.
- 5- Must demonstrates ability to build and maintain collaborative and trustful relationships with a variety of stakeholders
- 6- Quick to act potential opportunities and take the initiative within limits of authority.
- 7- Understanding of Cost control and vendor negotiation skills
- 8- Demonstrated ability to communicate effectively in Somali and English and lead a multi-disciplinary project management team, build effective working relations with colleagues and beneficiaries, and capable of working under pressure, with good experience in leadership and strategic management of project team.