Virtual CISO Proposal

Version: 1.0

Date: 17-Feb-2026

Prepared By:

Trusted Vision for Governance and Consultation

1. vCISO Task

Job Title	Responsibilities
Virtual CISO	**CISO responsibility is to ensure the full alignment with CRF Requirements, including:** 1. Ensure all security standards, controls, and procedures are developed, approved, implemented, updated and aligned with CRF requirements. 2. Ensure all financial requirements, investments, and cybersecurity resource needs are communicated clearly to senior management to support CRF implementation. 3. Coordinate with stakeholders to align business continuity and disaster recovery capabilities with CRF-mandated requirements. 4. Oversee the remediation of vulnerabilities identified through CRF assessments across systems, applications, and network environments. 5. Direct and oversee cybersecurity staff assigned to CRF implementation, ensuring effective task delegation and accountability. 6. Validate that all CRF-required documentation, processes, and technical controls are accurately mapped, implemented, and approved. 7. Deliver cybersecurity solutions based on risk prioritization, ensuring alignment with CRF expectations for people, processes, technology, and governance. 8. Build and mentor cybersecurity teams to ensure they understand and apply CRF requirements within business operations. 9. Lead CRF compliance activities across the organization, including: • Continuous monitoring of controls • Monitoring adherence to policies, standards, and regulatory requirements • Overseeing incident investigations • Analyzing relevant threat intelligence • Performing CRF maturity assessments and security reviews 10. Allocate and optimize resources for roles essential to CRF program implementation. 11. Support departments with CRF compliance activities, including: • Performing CRF-based data and asset classifications • Determining CRF requirements for major business and IT initiatives • Conducting CRF-driven security assessments 12. Promote awareness of CRF policies, controls, and responsibilities among management and operational teams.

13. Measure and report CRF-related KPIs/KRIs, including:
    - Strategy and governance effectiveness
    - Control performance
    - Policy and procedure compliance
    - Program performance (awareness, classification, risk management, etc.)
14. Collaborate with stakeholders to develop CRF-aligned cybersecurity policies, architecture, and supporting documentation.
15. Ensure the organization's cybersecurity strategy is fully aligned with CRF principles, business strategy, and risk appetite.
16. Conduct cybersecurity and risk assessments in alignment with CRF frameworks and requirements.
17. Work with stakeholders to develop and enhance CRF-compliant policies, processes, and procedures for cybersecurity and privacy.
18. Ensure appropriate CRF controls are implemented to mitigate risk and protect sensitive information.
19. Implement and maintain a cybersecurity risk management program that meets CRF expectations.
20. Integrate CRF objectives and principles into the organization's mission, goals, and governance structure.
21. Obtain and manage resources necessary to implement and sustain CRF control requirements.
22. Communicate the organization's CRF compliance status and cybersecurity posture during audits, regulatory reviews, and legal inquiries.
23. Demonstrate and promote the value of CRF adoption and cybersecurity governance to internal stakeholders.
24. Coordinate communication with third parties and regulators during CRF-related cybersecurity incidents.
25. Assess and report on the effectiveness of CRF controls in relation to strategic objectives and regulatory expectations.
26. Oversee the periodic review, update, and maintenance of CRF-related cybersecurity policies and documentation.
27. Ensure timely incident response activities and risk mitigation in accordance with CRF requirements.

28. Advocate CRF initiatives with senior leadership to ensure strategic prioritization and resource allocation.
29. Ensure CRF requirements are consistently embedded in cybersecurity policies, technical standards, and operational procedures.
30. Identify and validate CRF requirements for IT systems, ensuring proper classification and protection measures.
31. Develop and maintain CRF cybersecurity documentation to ensure compliance and infrastructure security.
32. Collaborate with internal and external stakeholders to identify emerging requirements and future enhancements for the CRF program.
33. Identify, recruit, and develop personnel with the skills needed to support CRF implementation and long-term sustainability.
34. Secure resources required to maintain CRF-aligned business continuity and cybersecurity readiness.
35. Develop and maintain cybersecurity strategies that align fully with CRF expectations and organizational priorities.
36. Ensure IT security requirements comply with the CRF strategic objectives and control framework.
37. Communicate identified CRF-related threats, risks, and mitigation actions to external stakeholders when required.
38. Manage budgeting, financial planning, and oversight for all CRF-related cybersecurity initiatives and resource needs.

2. Privacy/Data Protection Officer -DPO-Tasks

Job Title	Responsibilities
Privacy/Data Protection Officer	1. Conduct Privacy Impact Assessments (PIAs) to ensure that Personally Identifiable Information (PII) is appropriately protected. 2. Work with others on policies, processes and procedures relating to cybersecurity and privacy. 3. Ensure that appropriate controls are in place to effectively mitigate risk and address privacy concerns during a risk assessment process. 4. Work with the organization's legal advisers and relevant third parties to ensure that all services comply with privacy and data security requirements 5. Work with the organization's legal advisers, management and other stakeholders to ensure the organization has and maintains appropriate privacy and confidentiality documentation. 6. Work with stakeholders to develop relationships with regulators and government departments responsible for privacy and data security issues. 7. Work with business teams and senior management to ensure awareness of best practices relating to information privacy and data security 8. Ensure all processing and data source are registered with the relevant privacy and data protection authorities where required. 9. Work with senior management to establish a committee responsible for the oversight of data privacy. 10. Provide leadership on the committee responsible for the oversight of data privacy 11. Develop training materials and other communications to increase employees understanding of company privacy policies, data handling practices and legal obligations. 12. Work with organization administration, legal advisers and other related parties to represent the organization’s information privacy interests with external parties. 13. Providing support and advice regarding all aspects of Personal Data protection, including contributing to developing policies and internal procedures related to Personal Data protection. 14. Report on a periodic basis regarding the status of the privacy program to senior management and other responsible individuals or committees. 15. Direct and oversee privacy specialists and coordinate privacy and data security programs with senior management to ensure consistency across the organization. 16. Work with legal and HR teams to develop appropriate sanctions for failure to comply with the organization's privacy policies and procedures. 17. Ensure compliance with privacy practices across the organization.

	18. Periodically review and update the privacy program to incorporate changes in laws, regulations or organizational policy. 19. Establish and maintain an internal privacy audit program. 20. Review the organization's data and privacy projects to ensure that they are compliant with the organization's privacy and data security policies. 21. Notifying SDAIA of Personal Data Breach incidents. 22. Ensure that the use of technologies maintains and does not erode, privacy protections on use, collection and disclosure of personal information. 23. Monitor systems development and operations to ensure compliance with privacy policies. 24. Review all cybersecurity plans to ensure alignment between cybersecurity and privacy practices. 25. Develop and manage procedures for vetting and auditing vendors for compliance with appropriate privacy, data security, legislative and regulatory requirements. 26. Ensure all complaints concerning the organization's privacy policies and related documentation are addressed in a timely manner by appropriate resource. 27. Identify and remediate areas where the organization is not fully compliant with privacy requirements. 28. Coordinate with the Chief Information Security Officer (or equivalent) to ensure alignment between cybersecurity and privacy practices. 29. Acting as the direct point of contact with SDAIA and implementing its decisions and instructions regarding the application of the provisions of the Law and its Regulations. 30. Ensure that privacy compliance monitoring activities are carried out on an ongoing basis. 31. Responding to requests from Data Subjects and addressing complaints filed by them in accordance with the provisions of the Law and its Regulations 32. Monitoring and updating the records of Personal Data Processing activities of the Controller. 33. Develop strategic plans with senior management to ensure that personal information is processed accordance with applicable privacy requirements. 34. Develop and maintain enterprise-wide procedures to ensure that new products and services are developed in accordance with organizational privacy policies and legal obligations. 35. Contributing to reviewing plans of response to Personal Data Breach incidents, and ensuring that such plans are adequate and effective.

	36. Preparing periodic reports regarding Controller activities related to processing of Personal Data, and providing recommendations to ensure compliance with provisions of the Law and its Implementing Regulations 37. Maintain awareness of applicable privacy laws, regulations and accreditation standards. 38. Following up on regulatory documents issued by SDAIA related to the protection of personal data, including any amendments, and inform the relevant departments to ensure compliance. 39. Support company participation in public events related to privacy. 40. Support and advise the data office manager and personal data processing staff.