SERVICE SCHEDULE

BMIT VIRTUAL CHIEF INFORMATION SECURITY OFFICER SERVICE

Last Update: 21 August 2025

1. **General.** This is a Service Schedule setting out specific terms of Service in respect of BMIT's **vCISO Service.** The vCISO Service shall be considered to constitute a Professional Service, pursuant to Annex A5.

2. **Service Description.** The vCISO Service is a service through which BMIT endeavours to provide the Customer with information security strategic leadership and advisory services that enhance the Customer's information security posture. The vCISO Service shall be performed by BMIT through a vCISO. For the avoidance of doubt, the vCISO shall remain under the direction, control and responsibility of BMIT. BMIT may change the vCISO allocated to the Customer at any time, immediately upon informing the Customer in writing. BMIT shall ensure that the allocated vCISO holds the necessary experience and/or qualifications to serve as the primary contact to a Customer in respect of the vCISO Service. The vCISO Service includes, but is not limited to, evaluating the Customer's existing security practices, designing and implementing robust governance frameworks, conducting risk assessments and internal audits, facilitating crisis simulations, advising on relevant information security standards and information security compliance obligations, and enhancing the Customer's overall cybersecurity awareness. More specifically, the vCISO Service incorporates one or more of the following deliverables as may be agreed between the Parties and defined in the vCISO Service Delivery Plan:

    a. Governance and Planning

        i. **vCISO Scoping and Planning.** The vCISO shall work with the Customer to define the scope of security responsibilities, determine key priorities, establish cybersecurity goals, and outline a roadmap for implementing and maintaining an effective security framework.

        ii. **IT Governance Framework, Policies, and Procedures.** The vCISO shall assist in developing, reviewing, and updating the Customer's ICT governance frameworks, policies, and standard operating procedures, ensuring alignment with industry best practices and applicable laws. This may include defining roles, responsibilities, and escalation paths for security-related matters.

    b. Risk Management and Assessment

        i. **IT Risk Assessment.** The vCISO shall perform or oversee the evaluation of IT assets, identifying vulnerabilities and threats, and providing recommendations for risk mitigation strategies tailored to the Customer's specific business operations.

        ii. **Internal IT Audits.** The vCISO shall coordinate or conduct periodic internal audits of the Customer's IT infrastructure, processes, and controls, measuring compliance against established policies, standards, and regulatory requirements, and suggesting improvements where necessary.

        iii. **Critical IT Asset Management and Inventory.** The vCISO shall guide the Customer in creating and maintaining an accurate inventory of critical information technology assets, ensuring proper classification, ownership,

and protection of such assets, and providing ongoing oversight to address changes in the Customer's IT environment.

iv. **System Assessment and Hardening.** The vCISO shall advise on system assessments to determine configuration weaknesses and recommend hardening measures to reduce the Customer's exposure to cyber threats. This may include patch management, network segmentation, and review of access controls.

c. Incident Response and Continuity

i. **Cyber-Crisis Simulation Tabletop Exercises.** The vCISO shall design and facilitate crisis simulation exercises to test the Customer's preparedness for cyber incidents. This includes developing realistic scenarios, guiding participants through response protocols, and identifying gaps for continuous improvement.

ii. **Business Continuity and Disaster Recovery Planning.** The vCISO shall advise on or assist in the creation and maintenance of the Customer's business continuity and disaster recovery plans, ensuring critical business functions can be maintained or restored promptly in the event of service disruptions or security breaches.

iii. **Incident Response Planning.** The vCISO shall collaborate with the Customer to develop or refine an incident response plan, defining the chain of command, communication channels, escalation procedures, and remediation steps to contain and mitigate cybersecurity incidents.

d. Standards and Training

i. **Advisory on Standards and Compliance.** The vCISO shall provide guidance on information security compliance with relevant laws, regulations, and industry standards (e.g., GDPR, DORA, PCI-DSS, ISO 27001, NIST, NIS2), ensuring that the Customer is aware of and can implement the necessary controls, documentation, and reporting measures to achieve and maintain compliance.

ii. **Security Awareness and Training.** The vCISO shall advise on or deliver security awareness programs tailored to the Customer's personnel and operational environment, aiming to educate employees on cybersecurity threats, safe practices, and the importance of following the Customer's security policies and procedures.

3. **Initial and Service Delivery Engagement.** The Customer shall have a vCISO Hourly Bundle in place to define the Service Delivery Plan. During the initial service delivery phase, the vCISO will assess the Customer's cybersecurity requirements, risk posture, and strategic priorities, and based on this assessment, the parties will jointly define the scope of the vCISO Service and agree on a vCISO Service Delivery Plan. If the agreed scope requires effort beyond the vCISO Hourly Bundle, Customer shall purchase an additional vCISO Hourly Bundle for BMIT to continue the Service delivery under the Service Delivery Plan.

Unless otherwise agreed in writing, time spent on scoping or drafting the vCISO Service Delivery Plan shall be deducted from the Customer's vCISO Advisory Allocation.

4. **Service Delivery Plan.** A vCISO Service Delivery Plan, will be developed and mutually agreed upon with the Customer. The Customer shall cooperate in good faith with BMIT to define and develop the vCISO Service Delivery Plan.

   Any amendments or additions on the agreed scope to reflect evolving priorities, regulatory changes, or emerging risks, or changes whatsoever are subject to a mutual agreement. Such changes shall be communicated in writing and may require the issuance of a revised vCISO Service Delivery Plan and/or a revised Work Order, in each case, subject to prior mutual agreement.

5. **Out-of-Scope Services.** Any Customer request for any service that is not explicitly covered by the vCISO Service Delivery Plan will be considered out of scope of the vCISO Service.

6. **vCISO Service Request Process.** The Customer acknowledges that BMIT cannot guarantee the immediate or continuous availability of the vCISO Service. Accordingly, the Customer agrees to submit requests for any vCISO Service in a timely manner and in accordance with any minimum notice period and process set out herein.

   a. **Request Process.** If the Customer requires any additional vCISO Service, a Service Request must be submitted, including:

      i. A description of the requested service;

      ii. Any business objective and expected outcomes; and

      iii. Any urgency or timeline constraints.

   b. **Assessment & Proposal.** The vCISO will assess the request and provide:

      i. A recommended approach;

      ii. Estimated Service Hours envisaged as required; and

      iii. Any associated costs (if applicable).

      A formal vCISO Service Delivery Plan will be issued for mutual agreement before proceeding.

   c. **Approval & Execution.** Additional vCISO Services will only commence upon written approval by the Customer.

   d. **Minimum Notice Period:** The Customer shall submit requests for additional vCISO Services at least ten (10) Business Days in advance of the desired start date or any relevant milestone. If the Customer submits a request within this ten (10) Business Day period and BMIT's resources are unavailable, BMIT may refuse or defer the request without incurring any liability. For the avoidance of doubt, BMIT may refuse to accept any additional vCISO Services in its sole discretion, and without any need to disclose a reason and/or a cause to the Customer.

e. **Forfeiture of Hours.** If the Customer requests vCISO Services that are outside the agreed Service Delivery Plan during the final thirty (30) Business Days of the Service Term and BMIT is unable to accommodate such Customer request, any remaining unused vCISO Service Hours shall be forfeited. No refunds shall be provided, nor shall such hours be carried forward to any subsequent Service Term, unless otherwise agreed in writing.

7. **Customer Responsibility and Acknowledgment.** The Customer acknowledges that it retains ultimate responsibility for decisions related to its information security posture and the management of its IT environment.

   a. The Customer remains solely responsible for the final approval of the scope.

   b. By providing vCISO Services, BMIT and its personnel are acting solely as external advisors to the Customer and shall not, for any purpose, be deemed an in-house executive, employee, or officer whatsoever of the Customer.

   c. The Customer is responsible for promptly notifying BMIT of any changes or developments in its IT systems, security controls, or operational environment that may affect the scope or effectiveness of the vCISO Services.

8. **Access to Customer information and Systems.** In order to perform the vCISO Services effectively, BMIT may request access to the Customer's systems, documentation libraries, key personnel, and other relevant data. The Customer shall furnish such access in a timely manner. The Customer acknowledges that these requests are necessary to enable BMIT to fulfil the Customer's own requirements.

9. **Material, licences, and third-party licences and services.** Unless expressly stated in the Work Order, any additional material, licences, or third-party services required for the performance of the vCISO Services are not included in the Service Fees. BMIT shall notify the Customer in writing of any such requirements and associated costs. Subject to the Customer's prior written approval, the Customer shall bear all related costs.

10. **Legal Counsel.** The vCISO Services rendered by BMIT shall not be construed as legal advice. The Customer shall be solely responsible to source its own legal advice. Any legal queries concerning compliance obligations or regulatory or legal interpretations whatsoever should be directed to qualified legal counsel, retained by the Customer.

11. **Remediation services.** As part of its vCISO Services, BMIT may recommend specific remediation measures in response to its assessments or findings. Should the Customer elect to have BMIT implement such remediation and if such remediation work falls outside the scope of the vCISO Services agreed with Customer, a separate written agreement through a signed Work Order shall be required between the Parties prior to BMIT's acceptance of providing any such remediation services.