SERVICE SCHEDULE

BMIT Virtual Chief Information Security Officer Service (vCISO)

Last Update: 14 October 2026

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.**

   [For regulatory compliance engagements requiring a named individual, see Clause 3 (Fractional vCISO Add-On).]

   The vCISO Service comprises the provision by BMIT, through one or more designated BMIT personnel, of information security leadership and advisory functions that enhance the Customer's information security posture. BMIT shall designate a vCISO as the primary contact for the Customer in relation to the vCISO Service. For the avoidance of doubt, all BMIT personnel providing the vCISO Service shall remain under the direction, control and responsibility of BMIT.

   BMIT may change the vCISO designated as primary contact at any time upon written notice to the Customer. BMIT shall ensure that the designated 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 of recurring and one-time services to implement and maintain 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:

BMCL: Public

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.
v. Threat Management. The vCISO shall coordinate and conduct periodic vulnerability scans and/or penetrations tests of the Customer's IT infrastructure or web applications, as defined or scoped between parties.

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. Fractional vCISO Add-On. Where expressly stated in the applicable Work Order, the Customer may subscribe to a "Fractional vCISO Add-On" (the "Fractional vCISO Add-On"), an add-on service to the standard vCISO Service.

The Fractional vCISO Add-On is not a standalone service and may only be procured in conjunction with an active vCISO Hourly Bundle, which shall govern the core advisory and delivery capacity of the vCISO Service. The Fractional vCISO Add-On is designed for Customers

BMCL: Public

subject to regulatory requirements (including but not limited to DORA) that require the designation of a named individual for information security governance purposes. Under the Fractional vCISO Add-On:

a. Designation of Named Resource. BMIT shall designate a specific individual (the "Fractional vCISO") to be assigned to the Customer for the duration of the Service Term. The identity of the Fractional vCISO shall be set out in the applicable Work Order and may be disclosed by the Customer to regulatory authorities, as required.

b. Nature of Service. The Fractional vCISO Add-On constitutes a structured retainer-based engagement designed to support Customers subject to regulatory obligations requiring the designation of a named individual.

c. Regulatory Acknowledgment. The Customer acknowledges that the Fractional vCISO may be identified for regulatory purposes where a named individual is required to support the Customer's information security governance obligations.

d. Status and Responsibility. The provisions relating to the status of BMIT personnel and the Customer's responsibility, as set out in Clause 9 shall apply equally to the Fractional vCISO. For the avoidance of doubt:
   i. the designation of a Fractional vCISO, including where such individual is identified or disclosed for regulatory purposes, shall not transfer or delegate ultimate responsibility for the Customer's information security posture, governance, or compliance with applicable laws and regulations to BMIT or the Fractional vCISO;
   ii. the Customer shall remain solely responsible for all decisions, approvals, and risk acceptance relating to its information security environment; and
   iii. the Fractional vCISO shall not assume executive authority or operational control over the Customer's organisation unless expressly agreed in writing under a separate agreement.

e. Service Allocation. The Fractional vCISO Add-On includes a pre-agreed level of proactive scheduled services ("Proactive Services"). Such Proactive Services:
   i. shall be planned and tracked for visibility and reporting purposes;
   ii. shall not be deducted from the Customer's vCISO Hourly Bundle; and
   iii. are intended to complement, and not replace, the advisory and operational capacity provided under the vCISO Hourly Bundle.

f. Service Deliverables. The Proactive Services shall be consumed through the delivery of the following scheduled services:

   Monthly Services. BMIT shall provide:
   i. A written report covering:
      3.f.i.1 updates relating to the Malta Financial Services Authority (MFSA) and other relevant regulatory bodies;
      3.f.i.2 broader regulatory updates (including, where applicable, DORA);
      3.f.i.3 emerging cybersecurity threats and risks;
      3.f.i.4 relevant industry cybersecurity incidents;
   ii. high-level observations relating to the Customer's security posture and governance framework;
   iii. a tracker outlining outstanding items and agreed actions; and

BMCL: Public

iv. recommendations for improvement and risk mitigation.

Quarterly Services. BMIT shall provide:

v. executive-level awareness sessions, covering emerging threats, regulatory expectations and board-level cyber risk oversight;
vi. a structured review of the Customer's risk register;
vii. insights and lessons learnt from publicly disclosed cybersecurity incidents; and
viii. participation, where reasonably required, in governance or management meetings relevant to information security oversight.

Annual Services. BMIT shall provide:

ix. a strategic workshop with the Customer's management team, which shall include:
    3.f.ix.1 a review of the Customer's current cybersecurity posture;
    3.f.ix.2 an overview of relevant regulatory developments;
    3.f.ix.3 prioritisation of key security initiatives for the upcoming twelve (12) months;
    3.f.ix.4 the development of a high-level roadmap and action plan; and
    3.f.ix.5 an executive summary capturing key findings and recommendations.

g. Substitution Rights. The substitution rights set out in Clause 2 do not apply to the Fractional vCISO. BMIT may replace the Fractional vCISO only where required due to work exigencies. Any replacement shall have equivalent qualifications and experience. Where the Fractional vCISO is disclosed to regulatory authorities, the Customer shall remain responsible for updating such disclosures.

   For the avoidance of doubt, substitution or withdrawal shall not give rise to any claim, service credit, or termination right.

h. Fair Usage Policy. The Proactive Services provided under the Fractional vCISO Add-On are subject to a fair usage principle.

   Whilst BMIT shall endeavour to deliver the agreed Proactive Services as set out under Clause 3e and 3f. The Fractional vCISO Add-On is not intended to provide unlimited consultancy, project management, operational security support, or on-demand security resources.

   Where BMIT reasonably determines that the Customer's usage and requirements materially exceed the normal level of engagement anticipated for the Fractional vCISO Add-On, BMIT reserves the right, upon written notice, to:

   i. reclassify excess effort as advisory services and deduct such effort from the Customer's vCISO Hourly Bundle; or
   ii. invoice the Customer separately for such excess services at BMIT's prevailing rates; or
   iii. require the Customer to purchase additional vCISO Hourly Bundle capacity.

   BMIT shall continue to act reasonably and in good faith in exercising the above rights.

i. Enhanced Risk Acknowledgment. The Customer acknowledges that the designation of a Fractional vCISO may expose BMIT personnel to additional regulatory and operational scrutiny. The Customer shall cooperate in good faith with BMIT to ensure that the role scope, responsibilities, and limitations are always clearly defined and adhered to.

BMCL: Public

j. Suspension or Withdrawal of Named Resource. Notwithstanding any designation of a Fractional vCISO, BMIT reserves the right, at its sole discretion, upon written notice to suspend, limit or withdraw the named individual, including where:
   i. the Customer is in breach of its obligations under this Agreement;
   ii. there are outstanding payment issues;
   iii. the Customer fails to cooperate with BMIT in fulfilling the scope of the engagement; or
   iv. BMIT reasonably determines that continued designation exposes its personnel to undue regulatory, legal, or reputational risk.

   Such breaches may include:
   v. withdrawal of the designated vCISO;
   vi. suspension of scheduled deliverables; and
   vii. deferral or cancellation of planned activities.

   BMIT shall not be liable for any impact arising from such suspension. Where such designation has been disclosed to any regulatory authority, the Customer shall remain solely responsible for updating such disclosures.

4. **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 Hourly Bundle.

5. **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.

   Where a Fractional vCISO applies, the Service Delivery Plan shall include a defined allocation of proactive scheduled services (retainer-based).

6. **Threat Management Service Terms.** Threat Management services contracted under the vCISO service are governed by a separate Threat Management Service Schedule.

7. **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.

8. **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

BMCL: Public

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.

9. **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, officer, or statutory function holder of the Customer unless expressly agreed otherwise in writing.

   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.

10. **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.

BMCL: Public

The Customer acknowledges that these requests are necessary to enable BMIT to fulfil the Customer's own requirements.

11. **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.

12. **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.

13. **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.

BMCL: Public