SERVICE SCHEDULE

BMIT THREAT MANAGEMENT SERVICE

Last Update: 21 August 2025

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

2. **Service Description.** The Threat Management Service is designed to identify, assess, and mitigate potential cyber security risks within the Customer's IT environment. More specifically, the Threat Management Service consists of the following deliverables:

   a. **Vulnerability Scan.** BMIT shall perform a monthly external vulnerability scan on the Customer's environment using a third-party tool, as documented in the relevant Work Order agreed upon between the Parties. This exercise consists of:

      i. **Vulnerability Identification.** BMIT shall conduct an external scan to attempt identifying vulnerabilities on the Customer's environment.

      ii. **Triage.** BMIT shall propose the triage of the identified vulnerabilities based on BMIT's considered severity, potential impact, relevance and exploitability.

      iii. **Report.** BMIT shall provide the Customer with a detailed report outlining the findings, including recommended remediations.

   b. **Penetration and Security Testing.** BMIT shall perform a single external infrastructure Penetration Test as defined in clause 3.c.i. This Service aims to identify cyber security threats and vulnerabilities through a human-led test performed by a qualified analyst. This consists of:

      i. **Identification.** BMIT will identify the objectives, rules of engagement, scope and test scenarios that are most applicable to the Customer which shall be previously agreed with the Customer prior to the performance of the said Penetration Test. Such scenarios will be built through threat modelling and the methodologies to be used throughout the testing.

      ii. **Report.** BMIT will issue to the Customer a report which captures the Penetration Testing's findings. The report will outline risks and threats identified and exposed during the Penetration Testing and may also highlight IT risks that may require a different level of response for mitigation. Response services are not included in this Service but upon Customer's request, BMIT may agree to provide such needed services upon a separate agreement.

   c. **Additional Service Options:** The following additional services may be delivered by BMIT if accepted by BMIT following the Customer's request:

      i. Internal vulnerability scan, within the Customer's IT environment, including the procurement of any required additional licences.

      ii. Internal Penetration Test within the Customer's IT environment.

      iii. Web application Penetration Test.

      iv. Social engineering Penetration Test.

v. Any mutually agreed Penetration Tests.

Such Penetration Tests are further defined in clause 3 of this Service Schedule and will be conducted as previously agreed between both Parties. Should the Customer request BMIT to carry out any of the above additional services, BMIT will accordingly scope the specific engagement and provide an estimate of effort and cost, which will need to be formalised in a duly executed Statement of Works before commencement of any such work.

3. **Security Tests.** The Threat Management Service may involve the execution of various tests, including Penetration Testing and other security testing services, as stated in the Work Order. The precise scope of these tests shall be mutually agreed upon by the Customer and BMIT and documented accordingly.

   a. **Scope**. BMIT will engage with Customer to understand business objectives, agree the testing scope and rules of engagement between both Parties.

   b. **Information Gathering.** BMIT may request Customer for additional information, based on the methodology used. Information may also be gathered by targeting the Customer network using passive and active tools.

   c. **Infrastructure Penetration Testing.** Infrastructure Penetration Testing is conducted using the PTES framework. Customer may opt for external and/or internal infrastructure for testing purposes as defined in a Work Order and subject to the prerequisites or conditions specified in this clause and further in this Service Schedule.

      i. **External Penetration Testing:** This security test assesses the Customer's IT security controls, specifically those which are exposed to the public internet. It assists by identifying IT risks and vulnerabilities and, based on the methodology used, simulates a real-world attack scenario.

Included service	Service description / prerequisites
Active probing & exploitation	Customer network is actively probed to gather information on the full set of Customer services running on network. Based on the type of identified services, special payloads are crafted and sent to Customer's public services, in an attempt to exploit vulnerabilities. The comprehensive security exploitation testing techniques used on the targeted protocols include, but are not limited to, injection attacks, privilege escalation and security misconfigurations.
Post exploitation	If access through a public service is gained, and/or an exploitation has been identified, post-exploitation measures may be taken to secure stable access to your network. At this stage, the penetration tester will attempt to exploit the reachable services on the internal network, such as, but not limited to, database

	servers or domain controllers, which may also be vulnerable.

ii. **Internal Penetration Testing:** An internal Penetration Test assesses the Customer's internal security controls. Its objective is to evaluate the defence and security measures that are in place.

Included service	Service description / prerequisites
Onsite / Over VPN connection testing	The penetration tester takes the role of an attacker who has gained a degree of access to the internal network. This may be via a VPN connection or onsite, where the tester's testing machine may be connected to an office network or specific sensitive VLANs.
Internal systems testing	Internal systems are tested using specific roles, and for this purpose, Customer shall pre-provision access to the penetration tester. This may be for example equivalent to a typical employee's non-administrative Microsoft "Active Directory" role. Tests include identity and access management, network access controls, authentication mechanisms and other related security protocols.
Lateral movement	The penetration tester will attempt to move laterally within the network, including attempting to access higher privileged systems or sensitive data.
Cloud services	Testing with regards to certain cloud services can also be included in the agreed scope and in such case the penetration tester will assess and attempt to gain access to data residing on cloud services which Customer manages and/or subscribes to.

d. **Web Application Penetration Testing.** This type of Penetration Testing targets public-facing applications, especially those connected directly to a database that may contain sensitive data. The penetration tester will use different techniques based on the technology and components of the web application to identify and exploit vulnerabilities to extrapolate data in different scenarios. The testing will target different security aspects such as authentication, authorisation, session management and secure resource access:

Included service	Service description / prerequisites
Anonymous testing	For this test, the penetration tester would have no knowledge of the web application's architecture or platform. Unless sign-up is allowed via an access portal, the penetration tester will target any available page functionality and attempt to gain access to the application's assets and connected sensitive data.
Authenticated testing	Customer shall give the penetration tester the appropriate credentials to the application. This

	test simulates a malicious user intent or compromised user scenario. The tester will target page functionality, assess the security of these pages and any potential abuse on business functionality.

e. **Social Engineering Penetration Test.** This type of Penetration Test seeks to identify employees that may be susceptible to manipulative tactics that could lead to cybersecurity breaches using one or more of the following social engineering techniques:

Included service	Service description / prerequisites
Phishing campaign	The tester will use trending (i.e. more popular at the time of testing) techniques used to target business users. The testing campaign will run between 2 to 12 weeks, depending on the scale and the scope agreed between Parties. The tester will simulate a real attack using crafted emails, portals and other components.
Quality of security awareness	The tester will request the training material used by Customer for general security awareness and assess the quality of such training material. The tester can also optionally evaluate the level of security education of the Customer employees.
Evaluation of web and email safeguards and tools used	The tester will evaluate the current safeguards, tools and any mechanisms in place to identify and protect against phishing attacks.

f. **Reporting.** The final report will contain the following:

i. An executive summary describing the findings and the general security posture.

ii. An attack surface map.

iii. List of external facing services which are accessible on the public internet (as at date of test).

iv. For each observed finding:
3.f.iv.1. a description of the finding;
3.f.iv.2. classification and severity;
3.f.iv.3. evidence of any gained access;
3.f.iv.4. steps to replicate; and
3.f.iv.5. suggested remediation.

g. **Rules of Engagement**: Both Parties must agree, in writing, on the Penetration Testing's rules of engagement. Customer must provide any information that will be requested by BMIT, for the purpose of defining the said rules of engagement. These rules consist of, but are not limited to:

i. **Customer information and point of contact.** Customer agrees to have a person nominated as a point-of-contact during the Penetration Testing engagement to restore any system that becomes unavailable.

ii. **Customer objectives.** Customer must provide an overview of the requirements, and the desired outcome objectives.

iii. **Scope.** Targets must be owned and in full control of the Customer.

iv. **Sensitive and critical targets.** Penetration Testing typically includes a wide range of network-based activity including host discovery. It is the responsibility of the Customer to provide BMIT with:

3.g.iv.1. a list of the critical and sensitive hosts or network segments.

3.g.iv.2. a list of hosts and network segments which are not to be contacted. Alternatively, Customer shall previously clearly document its instructions to BMIT on how to proceed during the performance of Penetration Testing Services in such regard.

v. **Testing methodologies.** BMIT can adopt these testing methodologies:

3.g.v.1. **Black Box Testing**: For these Penetration Tests, BMIT will perform tests with no prior knowledge of Customer's environment, to simulate real-life scenarios and unbiased results.

3.g.v.2. **White Box Testing**: For these Penetration Tests, BMIT would have full knowledge and information regarding the internal structure and systems. This allows the tester to assess the internal logic, security controls, and architecture of the system and applications.

3.g.v.3. **Grey Box Testing**: For these Penetration Tests, BMIT will use a combination of methodologies, where the penetration tester is provided with partial knowledge of the internal workings of a system or critical components.

vi. **Testing time periods.** The Parties shall agree on a time window during which testing can be performed.

h. **On-site Testing**: If any Penetration Testing Services require BMIT to be present on-site at the Customer's location, Customer agrees that it will provide BMIT with all necessary access to Customer's site and/or network to provide the Services, and will provide in writing, and in-advance, any restrictions that may impact BMIT's ability to provide the Services. BMIT may decline to provide the Penetration Testing Services if restrictions in place inhibit BMIT's Penetration Testing team to undertake the Penetration Testing Services in an effective manner.

4. **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. **Changes in Customer IT Environment.** 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 Threat Management Services.

b. **Access to Customer information and Systems.** To perform the Threat Management Services effectively, BMIT may require access to the Customer's systems, documentation libraries, key personnel, and other relevant data. The Customer shall provide such access promptly and acknowledges that any failure to do so may limit or inhibit BMIT's ability to fulfil the Service.

c. **Remediation Services.** As part of its Threat Management Services, BMIT may recommend specific remediation measures in response to its assessments or findings. The Customer is responsible to implement remediation actions in a timely manner. Should the Customer wish to have BMIT assisting in the implementation of such remediation by the Customer, the Customer shall request such assistance from BMIT without undue delay from BMIT's finalization of the respective Service and BMIT will accordingly scope the Customer's requested engagement and provide an estimate of effort and cost. Assistance from BMIT in any remediation shall first need to be formalised and agreed by the Parties in a duly executed Work Order before the commencement of any remediation work by BMIT.

5. **Prerequisite/s or Conditions.** The following are additional conditions applicable to any Service defined in this Service Schedule.

a. **Vulnerabilities detection.** The Customer acknowledges and agrees that BMIT provides no guarantee that all vulnerabilities in the Customer's systems will be identified during the tests. The Customer also acknowledges and agrees that vulnerability scans may produce false positives and false negatives, thereby potentially misidentifying or failing to identify certain vulnerabilities.

b. **Material, licences, and third-party licences and services**. Unless expressly stated in a Work Order, any additional material, licences, or third-party services required for the performance of the 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.

c. **Service Exclusions.** The Service shall not include:

i. Testing or scanning of third-party systems or applications not under the Customer's control.

ii. Remediation of identified vulnerabilities or security gaps, unless agreed in a separate Work Order.

iii. Any activities falling outside the agreed scope of work as defined in the Work Order.