Cyber Assessments Services

Service Schedule

June 2026 Edition

Effective from 15 June 2026

Lanmark Limited
Company number 02977539
Registered office: West Hill House, West Hill, Dartford, DA1 2EU
lanmark.com/terms-of-business

Part of the Lanmark Terms of Business suite, published 15 June 2026.

Document control

Field	Value
Document title	Lanmark Limited Cyber Assessments Services Schedule
Document reference	Lanmark Service Schedule: Cyber Assessments
Version	June 2026 Edition
Document date	Effective from 15 June 2026
Status	Published (June 2026 Edition)
Supersedes	The Vulnerability Assessment and Penetration Testing sections of the Lanmark Managed Cyber Security Services Terms of Service
Layer	Layer 2 (Service Schedule) of the Lanmark T&C suite
Sits under	Lanmark Master Services Agreement (as in effect from time to time, published at lanmark.com/terms-of-business)

Revision history

Date	Version	Reason
15 June 2026	June 2026 Edition	First publication of the Lanmark Terms of Business suite (June 2026 Edition).

1. Purpose and scope

1.1 This Service Schedule sets out the service-specific terms on which Lanmark provides Cyber Assessments to the Client. It supplements, and is to be read with, the Lanmark Master Services Agreement (MSA) and the Order Form.

1.2 The Service comprises two discrete cyber assessment offerings:

(a) Vulnerability Assessment (VA): an annual subscription that delivers four scheduled assessments per year, identifying potential vulnerabilities in the in-scope network, systems and web applications. VA does not exploit identified vulnerabilities;

(b) Penetration Testing (PT): a one-off project engagement that actively attempts, in a controlled manner, to exploit identified vulnerabilities to assess the real-world impact of a successful attack.

1.3 VA may be delivered either by Lanmark engineers using Lanmark's vulnerability assessment tooling, or by a Third Party Provider. The applicable delivery model for the Client's engagement is identified in the Order Form. PT is delivered through the Third Party Provider only.

1.4 The Service is scheduled and point-in-time. It is not a continuous monitoring service. Continuous monitoring is provided under the Managed Cyber Security Services Schedule where the Client subscribes to that Service.

1.5 Subject to Clause 1.3 of the MSA (order of precedence), this Schedule prevails over the MSA only in respect of the specific Service detail it covers and only where this Schedule explicitly states an override.

2. Definitions

The following definitions apply in this Schedule. Defined terms in the MSA have the meanings given to them in the MSA and are not redefined here.

Assessment Cycle means in respect of VA, the twelve (12) month period during which the four scheduled VA tests are delivered. The Assessment Cycle starts on the Service Start Date.

Assessment Report means the written report produced by Lanmark or the Third Party Provider (as applicable) after each VA test or each phase of a PT engagement.

Authorisation Form means Lanmark's standard authorisation form for VA and PT engagements, signed by an authorised signatory of the Client before testing begins, identifying the in-scope test targets and confirming the warranties set out in Clause 7.1 and acknowledging the operational responsibilities at Clause 7.2.

Business Day means any day other than a Saturday, Sunday or English bank holiday.

In-scope Test Target means each Internet Protocol address, network range, web application URL, email address, network device or system that is identified in the Authorisation Form as a target of testing.

PT means Penetration Testing: the Service capability described at Clause 3.2.

Service means in this Schedule, Cyber Assessments as described in this Schedule (comprising VA, PT or both, as identified in the Order Form).

Social Engineering Campaign means a one-off controlled email-based attack simulation forming part of a PT engagement, as described at Clause 3.2.2(c). Distinct from the ongoing Phishing Simulation and Security Awareness Training services governed by the Cyber Compliance and Training Services Schedule.

Support Hours means Monday to Friday, 8.00am to 6.00pm UK time, excluding English bank holidays. Support Hours apply to Lanmark's Client-side engagement management for the Service and to the scheduling and delivery of VA tests. PT activities may be performed outside Support Hours where the Authorisation Form expressly identifies a different testing window.

Third Party Provider Terms means the terms published by the Third Party Provider from time to time governing the use of its services, including any service level commitments, methodology statements, processing terms and data protection particulars.

VA means Vulnerability Assessment: the Service capability described at Clause 3.1.

3. Service description

3.1 Vulnerability Assessment (VA)

3.1.1 VA may be delivered as an annual subscription with four (4) scheduled tests per Assessment Cycle (the 'VA Subscription'), or as a one-off project engagement (a 'VA Project'), as identified in the Order Form. Each VA test identifies potential vulnerabilities in the in-scope environment, including missing security patches, unsupported or out-of-date operating systems and software, weak configurations, open and exposed ports, and similar weaknesses identifiable through non-exploitative scanning.

3.1.2 VA covers the following test categories. The Client selects one or more in the Order Form:

(a) External Facing IP: scanning of the Client's external-facing infrastructure (servers, firewalls and similar) identified by IP address;

(b) Internal Facing IP: scanning of the Client's internal infrastructure (systems, operating systems and servers) identified by IP address or network range;

(c) Web Application: scanning of the Client's web applications identified by URL.

3.1.3 VA is non-intrusive: it identifies vulnerabilities but does not exploit them. VA does not deliberately attempt to crash systems, exfiltrate data or simulate adversary behaviour. Some scanning activity may incidentally cause instability in poorly-configured systems; the Client acknowledges this risk in the Authorisation Form.

3.1.4 VA may be delivered under one of two delivery models, as identified in the Order Form:

(a) in-house delivery: Lanmark engineers perform the assessment using Lanmark's vulnerability assessment tooling;

(b) Third Party Provider delivery: the Third Party Provider performs the assessment using its own tooling and reporting framework.

3.1.5 Each VA test produces an Assessment Report categorising identified vulnerabilities by severity and including recommendations for remediation. Remediation work is out of scope of this Service and is provided (where Lanmark agrees) as separately-quoted work under the Project Services Schedule or against Lanmark's published rate card.

3.2 Penetration Testing (PT)

3.2.1 PT is a one-off project engagement, typically of two (2) months' duration from the start of testing to the issue of the final report. PT actively attempts, in a controlled manner, to exploit identified vulnerabilities to determine the real-world impact of a successful attack, using controlled testing techniques designed to simulate aspects of malicious activity. PT is not a full adversary simulation or a red team engagement; it operates within the scope of the test categories selected on the Order Form and the In-scope Test Targets identified in the Authorisation Form.

3.2.2 PT covers the following test categories. The Client selects one or more in the Order Form:

(a) External Facing IP: penetration testing of the Client's external-facing infrastructure (servers, firewalls and similar) identified by IP address;

(b) Web Application: penetration testing of the Client's web applications identified by URL;

(c) Social Engineering Campaign: a controlled email-based attack simulation targeting a defined population of Authorised Users. The Social Engineering Campaign is a one-off PT activity. It does not replace the ongoing Phishing Simulation and Security Awareness Training services governed by the Cyber Compliance and Training Services Schedule, which are designed for continuous staff training.

3.2.3 Internal IP penetration testing is not offered as part of the Service. Where the Client requires internal IP penetration testing, the requirement is treated as a separately-quoted project under the Project Services Schedule.

3.2.4 PT is delivered in two phases:

(a) initial test and report: the Third Party Provider conducts the agreed testing, attempts exploitation of identified vulnerabilities, and produces an initial Assessment Report identifying successful and attempted exploitations, recommended remediation steps and a risk assessment;

(b) retest and final report: following a remediation window (typically a defined number of weeks identified in the Order Form), the Third Party Provider retests the previously-identified vulnerabilities and produces a final Assessment Report confirming which vulnerabilities have been remediated.

3.2.5 Remediation work between the initial test and the retest is out of scope of the Service and is the Client's responsibility (potentially supported by separately-quoted work under the IT Support Services Schedule or the Project Services Schedule).

3.3 Methodology

3.3.1 VA and PT are conducted in accordance with industry-standard cyber assessment methodologies. Lanmark and the Third Party Provider may apply elements of recognised frameworks (including, without limitation, those of OWASP, PTES, OSSTMM, CREST or similar bodies) as appropriate to the test category and the in-scope environment. Lanmark does not commit the Service to a specific named methodology, in recognition that methodologies evolve and the Third Party Provider's approach may change from time to time.

4. In scope and out of scope

4.1 In scope

The Service includes:

(a) the test categories identified in the Order Form (and only those test categories);

(b) the In-scope Test Targets identified in the Authorisation Form (and only those targets);

(c) the production of an Assessment Report after each VA test, and after each phase of a PT engagement;

(d) Lanmark Client-side engagement management for the Service during Support Hours, including scheduling, communication with the Client and routing of Assessment Reports;

(e) the Service Levels at Clause 5.

4.2 Out of scope

The following are out of scope of the Service and are not provided as part of the Service Fees. Where any of the following is required, it is provided (where Lanmark is able to provide it) as separately-quoted work or under a separate Service Schedule:

(a) remediation of any vulnerability identified by VA or PT (always separately quoted as project work, under the Project Services Schedule, or under the IT Support Services Schedule where the Client subscribes to that Service and Lanmark agrees the remediation work is within the operational scope of the IT Support Service);

(b) internal IP penetration testing (not offered);

(c) ongoing security awareness training, ongoing phishing simulation programmes and Cyber Essentials assessment and certification activity (covered by the Cyber Compliance and Training Services Schedule);

(d) Managed Detection and Response, Identity Threat Detection and Response and Managed SIEM (covered by the Managed Cyber Security Services Schedule);

(e) regulatory breach notification preparation or submission, regulatory reporting, and engagement with law enforcement;

(f) forensic investigation, evidence preservation or expert witness work in connection with any vulnerability identified during testing;

(g) testing of any asset, target or system that is not identified as an In-scope Test Target in the Authorisation Form;

(h) additional VA tests beyond the four scheduled tests within an Assessment Cycle, except where separately ordered;

(i) anything stated as out of scope in the Order Form.

5. Service Levels

5.1 VA Service Levels

5.1.1 VA tests are scheduled within each Assessment Cycle. Lanmark, or the Third Party Provider (as applicable), will agree the schedule with the Client at the start of the Assessment Cycle. Each quarterly test is delivered during the relevant quarter, on a date confirmed with the Client at least seven (7) Business Days in advance, save where the Client requests a different schedule.

5.1.2 The Assessment Report for each VA test is provided to the Client within fifteen (15) Business Days of completion of the test, save where the test reveals matters that warrant immediate notification (for example, a critical vulnerability requiring urgent attention), in which case Lanmark will notify the Client without undue delay through the Service Tooling.

5.2 PT Service Levels

5.2.1 PT engagement timing is identified in the Order Form. The Third Party Provider will agree the test window with the Client before testing begins, by reference to the Authorisation Form.

5.2.2 The initial Assessment Report is provided to the Client within fifteen (15) Business Days of completion of the initial test phase. The final Assessment Report is provided within fifteen (15) Business Days of completion of the retest phase. Where the test reveals a critical vulnerability requiring urgent attention, Lanmark or the Third Party Provider will notify the Client without undue delay.

5.2.3 Where the Third Party Provider's testing team or Lanmark observes any matter during PT that, in their reasonable opinion, warrants immediate escalation (for example, an active compromise, evidence of pre-existing breach, or a control failure that creates an imminent risk), Lanmark or the Third Party Provider will notify the Client without undue delay and may pause testing pending Client instructions.

5.3 Third Party Provider Service Levels

5.3.1 Where VA or PT is delivered by the Third Party Provider, the Third Party Provider's own service standards apply to its delivery of the testing. Lanmark does not commit to Service Levels different from, or more onerous than, those operated by the Third Party Provider. Where the Third Party Provider fails to meet its operational standards, Lanmark's obligation and liability in respect of that failure is limited to using reasonable endeavours to pass through, or assist the Client in pursuing, any remedies available under the Third Party Provider Terms. This Clause 5.3.1 is a Service-specific application of Clause 17.4 of the MSA.

5.4 Service Level measurement and exclusions

5.4.1 Lanmark's records of test scheduling, delivery and reporting (held in the Service Tooling and in Lanmark's records) are the authoritative record of Lanmark Service Level performance, save in the case of manifest error. The Third Party Provider's records of testing activity and reporting are the authoritative record of Third Party Provider Service Level performance.

5.4.2 Time spent waiting for Client action (including signing of the Authorisation Form, confirmation of test targets, response to scheduling requests, response to escalations during testing, or any other Client-controlled matter) does not count towards any applicable Service Level.

5.4.3 The Service Levels at this Clause 5 are service management targets. They do not give rise to service credits, fee reductions, repayment of Fees or any similar monetary remedy. Where Lanmark or the Third Party Provider fails to meet a Service Level, the Client's remedy is service review and escalation through the IT Support Services Schedule (where the Client subscribes to it in parallel) or through Lanmark's commercial contact for the engagement. Subject to Clause 18 of the MSA, this Clause 5.4.3 states the Client's full and exclusive remedy, and Lanmark's only obligation and liability, for non-performance or non-availability of the Service Levels at this Clause 5.

5.4.4 Where a scheduled quarterly VA test cannot be performed during the relevant quarter because of Client delay (including delay in signing the Authorisation Form, delay in confirming In-scope Test Targets, delay in granting access, or repeated rescheduling by the Client), Lanmark may, acting reasonably, reschedule the test within the same Assessment Cycle where this is reasonably practicable. Lanmark is not required to carry an unused VA test into a later Assessment Cycle, and an unused VA test that has not been rescheduled within the relevant Assessment Cycle is forfeit, save where Lanmark agrees otherwise in writing.

6. Operational arrangements

6.1 Authorisation Form

6.1.1 Before VA testing begins for an Assessment Cycle, and before each PT engagement begins, the Client will sign the Authorisation Form. The Authorisation Form identifies the In-scope Test Targets, the requested testing time window (where applicable), and confirms the warranties at Clause 7.1 and acknowledges the operational responsibilities at Clause 7.2.

6.1.2 The Authorisation Form is incorporated into the Agreement solely for the purpose of identifying the In-scope Test Targets, the testing time window, the operational testing parameters and the Client's authorisations and warranties for the relevant Assessment Cycle (for VA) or PT engagement (for PT). The Authorisation Form does not vary, override or disapply any provision of the MSA, this Schedule or the Order Form. Any deviation from the MSA, this Schedule or the Order Form requires a formal variation executed in accordance with Clause 28.1.3 of the MSA and does not take effect through the Authorisation Form. Where the Authorisation Form has not been signed (or, in the case of VA, has not been signed for the current Assessment Cycle), Lanmark and the Third Party Provider will not commence testing of the In-scope Test Targets.

6.1.3 Where the Client wishes to add to, remove from or otherwise change the In-scope Test Targets during the Assessment Cycle or during a PT engagement, the Client will sign a revised Authorisation Form. Material changes to the In-scope Test Targets may affect the Fees or the test schedule and are subject to Lanmark's confirmation.

6.2 Onboarding

6.2.1 Onboarding for the Service comprises an initial consultation and the setup of any access required to perform the testing. Where the Order Form provides for an onboarding Fee, the Fee is identified in the Order Form.

6.2.2 Onboarding requires Client cooperation, including signing the Authorisation Form, providing accurate test target information, granting any access required and confirming the testing schedule.

6.3 Reporting

6.3.1 Assessment Reports are provided to the Client through the Service Tooling, or by email to the Client's nominated cyber security contact, as agreed at onboarding.

6.3.2 Assessment Reports are confidential information of both parties (and, where the Third Party Provider has delivered the testing, of the Third Party Provider). Clause 14 of the MSA (Confidentiality) applies.

6.4 Critical findings

6.4.1 Where any test reveals a critical vulnerability or an active threat that, in the reasonable opinion of Lanmark or the Third Party Provider, requires urgent Client action, Lanmark or the Third Party Provider will notify the Client without undue delay through the Service Tooling and (where appropriate) through the Client's nominated cyber security contact direct.

6.4.2 Where the test reveals evidence of a pre-existing compromise or breach, Lanmark and the Third Party Provider will pause further testing of the affected target pending Client instructions. The Client should consider whether the matter requires escalation to the Managed Cyber Security Service (where subscribed) or to a separate incident response engagement.

7. Client responsibilities

7.1 Authorisation and ownership warranties

7.1.1 By signing the Authorisation Form, the Client warrants and confirms to Lanmark that:

(a) the Client owns, or has the lawful right to test, each In-scope Test Target identified in the Authorisation Form;

(b) the signatory of the Authorisation Form has the authority to authorise the testing on behalf of the Client;

(c) where any In-scope Test Target is hosted on infrastructure operated by a third party (for example, a cloud hosting provider), the Client has obtained, or will obtain before testing begins, the authorisation of that third party for the testing, and can provide evidence of that authorisation on request;

(d) before testing begins, the Client has taken a full and verified backup of each system, application, data-bearing environment or other restorable asset identified as an In-scope Test Target, and the Client has tested its restore procedure so that the Client can restore each such asset to its pre-test state in the event of disruption. Where an In-scope Test Target is not a restorable asset (for example, an email address used in a Social Engineering Campaign), the Client has put in place appropriate alternative safeguards (such as user communications and reporting controls) to manage the testing risk for that target;

(e) the Client understands that testing necessarily involves the use of network tools and techniques designed to detect or exploit security vulnerabilities and that it is impossible to identify or eliminate every risk associated with the use of those tools and techniques.

7.2 Operational responsibilities

To enable Lanmark and the Third Party Provider to deliver the Service, the Client will:

(a) sign the Authorisation Form before each Assessment Cycle (for VA) and before each PT engagement (for PT);

(b) provide accurate and complete information about the In-scope Test Targets at the start of each Assessment Cycle or PT engagement, and promptly notify Lanmark of any change to the In-scope Test Targets during the engagement;

(c) grant Lanmark and the Third Party Provider the access required to perform the testing, including any credentials, network access or hosting provider authorisations;

(d) nominate a cyber security contact at the Client to receive Assessment Reports, critical findings notifications and other Service communications;

(e) respond promptly to Lanmark or Third Party Provider requests for information, scheduling confirmation, or instructions in connection with the Service;

(f) maintain a current backup of each In-scope Test Target that is a system, application, data-bearing environment or other restorable asset, and verify its restore procedure before testing begins; and, in respect of any In-scope Test Target that is not a

restorable asset (for example, an email address used in a Social Engineering Campaign), put in place appropriate alternative safeguards to manage the testing risk, in each case in accordance with Clause 7.1.1(d);

(g) act on, or have a third party act on, the recommendations in each Assessment Report (this Service identifies vulnerabilities; remediating them is the Client's responsibility);

(h) comply with the Third Party Provider Terms to the extent those terms apply to the Client's use of the Service.

Where the Client does not meet a responsibility under this Clause 7, and that failure causes or materially contributes to a delay in testing, a failure of the Service, a Client loss arising in connection with the Service, or a third-party claim, Lanmark and the Third Party Provider are not liable for the consequent loss or damage, and the Client's indemnity at Clause 8 applies to the extent set out in Clause 8.

8. Indemnification

8.1 The Client will indemnify Lanmark against any third-party claim made against Lanmark (including regulatory action by any regulator or supervisory authority, and including claims by employees, customers or counterparties of the Client, and by any third-party hosting provider operating infrastructure that hosts any In-scope Test Target), and against Lanmark's reasonable costs and expenses (including reasonable legal fees) incurred in connection with such third-party claim or regulatory action, where the claim or action arises out of or in connection with:

(a) any breach of the Client warranties at Clause 7.1, including (without limitation) the Client not owning or not being authorised to test any In-scope Test Target;

(b) the Client's failure to obtain authorisation from a third-party hosting provider before testing begins;

(c) the Client's failure to take or verify a full backup of a system, application, data-bearing environment or other restorable asset identified as an In-scope Test Target before testing begins, or (in respect of an In-scope Test Target that is not a restorable asset) the Client's failure to put in place appropriate alternative safeguards;

(d) the Client's provision of inaccurate, incomplete or misleading information about an In-scope Test Target;

(e) the Client's breach of any obligation under this Schedule, the MSA, the Authorisation Form or the Third Party Provider Terms.

8.2 The indemnity at Clause 8.1 does not apply to the extent that the matter giving rise to the third-party claim or regulatory action is caused by the gross negligence or wilful misconduct of Lanmark, or by Lanmark's breach of a non-excludable obligation under the Data Protection Legislation, the MSA or applicable law. For the avoidance of doubt, the indemnity is given without prejudice to, and does not narrow, the non-excludable carve-outs at Clause 18.1 of the MSA.

8.3 The Client's indemnity at this Clause 8 is subject to the limitations and exclusions of liability at Clause 18 of the MSA (including the per-Service per-Contract Year cap at Clause 18.2 and the exclusions at Clause 18.3 of the MSA). Clause 18.2.2 of the MSA applies.

8.4 Lanmark will give the Client prompt written notice of any third-party claim or regulatory action that may give rise to an indemnity under Clause 8.1, and will not settle or admit liability without the Client's prior written consent (such consent not to be unreasonably withheld or delayed). The Client may take conduct of the defence at the Client's cost where Lanmark gives its prior written approval, such approval not to be unreasonably withheld. Lanmark may refuse approval where, in Lanmark's reasonable opinion, the claim or regulatory action concerns Lanmark's own legal, regulatory, confidentiality or reputational interests, including (without limitation) any matter involving Lanmark's confidential information, testing tooling, testing methodology, other clients of Lanmark, or any direct investigation of Lanmark by a regulator or other authority. Where Lanmark refuses approval, Lanmark will assume conduct of the defence and will keep the Client reasonably informed.

9. Disclaimers and acknowledgement of testing risk

9.1 The Service aims to identify (in the case of VA) and validate (in the case of PT) vulnerabilities in the in-scope environment. The Service is not designed to identify, and cannot guarantee identification of, every vulnerability, weakness or attack vector. In particular, and without limitation, Lanmark and the Third Party Provider do not warrant or guarantee that:

(a) VA or PT will identify every vulnerability in the in-scope environment;

(b) the Client will not suffer a cyber-related loss after a vulnerability has been identified, including from a vulnerability identified in an Assessment Report that has not been remediated;

(c) the in-scope environment will be free of false positive or false negative findings;

(d) VA or PT will be entirely non-disruptive (the Client acknowledges in Clause 7.1.1(e) and in the Authorisation Form that testing necessarily involves tools and techniques that may cause instability).

9.2 The Third Party Provider's tooling, methodology, reports and other deliverables made available in connection with the Service are supplied to the Client under the Third Party Provider Terms. Lanmark does not give any separate warranties (express, implied or statutory) in respect of the Third Party Provider's tooling, methodology, reports or other deliverables, save to the extent that any such warranty cannot be excluded under applicable law. This Clause 9.2 does not exclude any warranty or other obligation that cannot be excluded under applicable law, and does not affect Lanmark's own obligation to plan, schedule and manage the Service in accordance with the MSA and this Schedule.

9.3 Subject to Clause 18 of the MSA, Lanmark is not liable for any disruption, instability, downtime, data loss or other Client loss that arises during or as a result of VA or PT testing carried out in accordance with this Schedule, the Authorisation Form, and any agreed testing window or testing parameters identified in the Authorisation Form. The Client expressly accepts the risk of testing-related disruption in signing the Authorisation Form and is responsible for maintaining backup and recovery arrangements (or, where the In-scope Test Target is not a restorable asset, appropriate alternative safeguards) that mitigate that risk.

9.4 The Service is a point-in-time assessment. An Assessment Report describes the state of the in-scope environment at the time of testing. Vulnerabilities discovered after the test (whether arising from new threats, environmental changes, vendor disclosures or other factors) are outside the scope of the relevant Assessment Report. Lanmark recommends that the Client retains an ongoing cyber security service (such as the Managed Cyber Security Service) for continuous monitoring.

10. Data protection particulars

This Clause 10 supplements Clause 13 (Data protection) of the MSA and sets out the Article 28 processing particulars for the Service. Defined terms in Clause 13 of the MSA apply in this Clause.

Article 28 particular	Value for the Cyber Assessments Service
Subject matter of the processing	Provision of the Cyber Assessments Service, comprising VA scanning of the in-scope environment, PT controlled exploitation activity, Social Engineering Campaign delivery, and the production of Assessment Reports.
Duration of the processing	For the duration of each Assessment Cycle (in respect of VA) or each PT engagement (in respect of PT), plus reasonable retention periods for the Assessment Reports and supporting testing records. Lanmark-held records are governed by Lanmark's Data Protection and Retention Policy. Third Party Provider-held records are retained in accordance with the Third Party Provider Terms.
Nature and purpose of the processing	Collection, organisation, structuring, retrieval, consultation, use and (where applicable) deletion of Personal Data for the purpose of cyber vulnerability identification, exploitation testing, social engineering simulation and the production of Assessment Reports.
Types of Personal Data	In-scope Test Target identification data (which may include email addresses, IP addresses, URLs and network identifiers associated with individuals); Authorised User identification data captured during testing (where in scope of a Social Engineering Campaign, this includes the targeted users' names, email addresses, work telephone numbers and behavioural and interaction responses to the simulated attack, including clicked links, submitted forms, opened emails, reported emails and similar interaction data); incidental Personal Data captured in screenshots, logs, traffic captures or report material; nominated Client contact details for the Service.
Categories of data subject	Authorised Users of the Client targeted by testing (in particular Social Engineering Campaign targets); Client employees and contractors whose Personal Data appears incidentally in the in-scope environment; the Client's nominated cyber security contact and signatories of the Authorisation Form.
Documented instructions for processing	Set out in the MSA, this Schedule, the Order Form, the Authorisation Form, the Lanmark service documentation produced during onboarding, and any further written instructions the Client gives Lanmark from time to time. The Third Party Provider Terms inform the processing operations required to deliver the Service through the Third Party Provider's tooling and methodology; the Client's instructions to Lanmark remain governed by the MSA and the Data Protection Legislation.

Cyber assessment activity may incidentally involve special category Personal Data (for example, where the in-scope environment processes health data that becomes visible during testing) and criminal offence data (for example, where testing or a Social Engineering Campaign reveals evidence of attempted or actual unauthorised access to Client systems, suspicious account use, or compromised credentials). The Service is not designed for the routine processing of either category

of data. Where the Client expects either category to feature in the in-scope environment beyond incidental processing, the Client will inform Lanmark before testing so that appropriate technical and organisational measures can be confirmed.

11. Sub-Processors used in delivering this Service

Lanmark uses Sub-Processors to deliver the Service in accordance with Clauses 13.5 to 13.7 of the MSA. The categories of Sub-Processor used in delivering this Service are:

Category	Role in this Service
Third Party Provider	Delivery of standalone VA testing (where the Order Form identifies the Third Party Provider as the VA delivery model) and of all PT engagements. Provision of testing tooling, testing methodology, reporting and supporting infrastructure.
Lanmark VA tooling provider	Where the Order Form identifies in-house Lanmark delivery as the VA delivery model and where the provider of the vulnerability assessment tooling used by Lanmark engineers actually processes Personal Data on Lanmark's behalf in connection with the Service (for example, where the tooling transmits scan data, metadata or reports to the provider's platform). Where the tooling runs locally and no Personal Data leaves Lanmark's environment in connection with the Service, the tooling provider is a supplier of tooling rather than a Sub-Processor and is not included in the Sub-Processors List for this Service.
Service Tooling provider	Provision of the Lanmark service management system used for Client-side engagement, Authorisation Form management, Assessment Report distribution and engagement tracking.

The current Sub-Processor in each category (and in particular the identity of the current Third Party Provider for standalone VA and PT, and the current Lanmark VA tooling provider for in-house delivery), the location of processing for each Sub-Processor, and any applicable international transfer mechanism, are identified in the live Sub-Processors List published at lanmark.com/terms-of-business. The Sub-Processors List is the authoritative source for the identification of current Sub-Processors.

12. Relationship with the Third Party Provider

12.1 Where the Order Form identifies the Third Party Provider delivery model for VA, and in respect of all PT engagements, the testing work is performed by the Third Party Provider. Lanmark plans, schedules and manages the engagement with the Third Party Provider on the Client's behalf, and provides the Client-side engagement management at Clause 5.

12.2 The Service is therefore subject to:

(a) the Third Party Provider Terms, including the Third Party Provider's published methodology, processing terms and data protection particulars;

(b) the operational availability of the Third Party Provider's tooling, testing personnel and infrastructure;

(c) the Third Party Provider's methodology, feature set and operating model from time to time.

12.3 Clause 17 of the MSA (Third Party Providers) applies to the Service. In particular, and without limitation, Clause 17.4 of the MSA confirms that Lanmark is not liable for any act or omission of the Third Party Provider, including any failure of the Third Party Provider's testing or reporting to meet a published standard or to perform as described in the Third Party Provider's documentation.

12.4 Where VA is delivered in-house by Lanmark engineers using Lanmark's vulnerability assessment tooling, Clause 12.1 to 12.3 do not apply to the in-house element of the engagement. Lanmark's delivery of in-house VA is governed by the MSA and this Schedule.

13. Service-specific commercial terms

13.1 The Fees for the Service are set out in the Order Form. VA Fees are charged on an annual subscription basis, per Assessment Cycle. PT Fees are charged on a one-off engagement basis.

13.2 The Order Form identifies the test categories selected by the Client (Clauses 3.1.2 and 3.2.2), the default scope limits applicable to each category (for example, up to 10 IP addresses, up to 100 IP addresses, up to 5 web application URLs), and any agreed expansion beyond the default scope limits.

13.3 Where the Client requests testing of additional In-scope Test Targets beyond the default scope limits, additional Fees apply as set out in the Order Form or, where not set out in the Order Form, at Lanmark's published rate card at the time the additional testing is performed.

13.4 The onboarding Fee at Clause 6.2 is one-off and is payable on the first engagement. The Client does not pay a further onboarding Fee on subsequent renewals of the VA subscription or subsequent PT engagements, save where the engagement requires materially new onboarding work.

14. Explicit overrides of the Master Services Agreement

Clause 1.3 of the MSA provides that a Service Schedule prevails over the MSA only in respect of specific service detail and only where the Service Schedule explicitly states an override. The following provisions of this Schedule are explicit overrides of the MSA for the Cyber Assessments Service:

(a) Clauses 5.3.1 and 5.4.3 of this Schedule set the Service-specific Service Level position: where the Third Party Provider delivers the testing and fails to meet its operational standards, Lanmark's obligation and liability is limited to using reasonable endeavours to pass through or assist the Client with remedies available under the Third Party Provider Terms; the Service Levels are service management targets and do not give rise to service credits or fee reductions; the Client's remedy for any Lanmark engagement-level failure is service review and escalation. This is a Service-specific application of Clauses 17.4 and 18.4 of the MSA and prevails over any inconsistent position the MSA might otherwise be read to allow for this Service;

(b) Clause 8 of this Schedule sets out a Service-specific indemnity from the Client to Lanmark, limited to third-party claims (including regulatory action) and Lanmark's reasonable costs and expenses incurred in responding to such claims or action, with triggers specific to cyber assessment risk (breach of the Authorisation Form warranties, failure to obtain hosting provider authorisation, failure to take or verify backups, inaccurate information about In-scope Test Targets, and breach of Schedule, MSA, Authorisation Form or Third Party Provider Terms). The indemnity at Clause 8 is subject to the limitations and exclusions of liability at Clause 18 of the MSA, including the non-excludable carve-outs at Clause 18.1;

(c) Clause 9 of this Schedule sets out Service-specific disclaimers, including that VA and PT cannot guarantee identification of every vulnerability, that testing necessarily involves tools and techniques that may cause instability, and that Lanmark is not liable for disruption arising during or as a result of testing carried out in accordance with this Schedule and the Authorisation Form. These disclaimers do not affect Lanmark's own obligation to plan, schedule and manage the Service in accordance with the MSA and this Schedule, and are Service-specific applications of Clauses 17.4 and 18 of the MSA.

Save as set out above, this Schedule does not override the MSA. Any provision of this Schedule that conflicts with the MSA without expressly stating an override under this Clause 14 is to be read consistently with the MSA in accordance with Clause 1.3 of the MSA.