Cyber Compliance and Training 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 Compliance and Training Services Schedule
Document reference	Lanmark Service Schedule: Cyber Compliance and Training
Version	June 2026 Edition
Document date	Effective from 15 June 2026
Status	Published (June 2026 Edition)
Supersedes	No existing single document. Consolidates services previously sold through individual proposals.
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 Compliance and Training 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 three commercial offerings, which the Client may take in any combination as identified in the Order Form:

(a) Phishing Simulation Managed Service combined with Security Awareness Training: a recurring per-user subscription that delivers ongoing simulated phishing campaigns and security awareness content to the Client's Authorised Users. Phishing Simulation and Security Awareness Training are sold and delivered as a single combined offering and cannot be taken separately (Clause 3.1);

(b) Cyber Essentials Certification: a project engagement to prepare for, and obtain, IASME-awarded Cyber Essentials or Cyber Essentials Plus certification through a Third Party Provider platform. Offered in three tiers, Self-Service, Assisted Service and Managed Service, as identified in the Order Form (Clause 3.2);

(c) Microsoft Intune to Cyber Essentials Standards: a project engagement to configure the Client's Microsoft Intune environment to align with the Cyber Essentials technical controls (Clause 3.3).

1.3 The Service is delivered substantially through Third Party Providers. The current Third Party Providers and the role each plays in delivering the Service are identified at Clause 11 (Sub-Processors) and in the live Sub-Processors List published at lanmark.com/terms-of-business.

1.4 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 Submission means the submission of the Client's Cyber Essentials or Cyber Essentials Plus assessment to IASME (through the Third Party Provider's platform) for the awarding of the relevant certification.

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

CE means Cyber Essentials, the United Kingdom Government-backed cyber security certification scheme administered by IASME.

CE Plus means Cyber Essentials Plus, the enhanced certification level under the Cyber Essentials scheme, which includes a technical audit and verification in addition to the self-assessment that underlies CE.

Certification Engagement means a project engagement under Clause 3.2 for the Client to obtain CE or CE Plus certification at the tier identified in the Order Form.

Consultancy Hours means the hours of Lanmark consultancy time included in the Assisted Service tier (two (2) hours) or the Managed Service tier (eight (8) hours) of a Certification Engagement, used to support the Client through preparation, remediation, evidence gathering, submission and (in the case of CE Plus) audit support.

IASME means The IASME Consortium Limited, being the certification body authorised by the National Cyber Security Centre to award Cyber Essentials and Cyber Essentials Plus certifications under the Cyber Essentials scheme, or any successor authorised certification body from time to time.

Intune to CE Engagement means a project engagement under Clause 3.3 to configure the Client's Microsoft Intune environment to align with the Cyber Essentials technical controls.

Phishing Simulation means the recurring simulated phishing campaign service forming part of the offering described at Clause 3.1.

Recommended Remediation means the remediation steps identified by Lanmark or the Third Party Provider in writing during a Certification Engagement as being required for the Client to meet the Cyber Essentials technical controls at the certification tier identified in the Order Form.

Security Awareness Training means the security awareness training content (courses, videos and quizzes) forming part of the offering described at Clause 3.1.

Service means in this Schedule, the Cyber Compliance and Training Service comprising the offerings described in this Schedule (or any combination of them, as identified in the Order Form).

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. The Third Party Providers' platforms operate continuously in accordance with the Third Party Provider Terms.

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

3. Service description

3.1 Phishing Simulation and Security Awareness Training

3.1.1 Phishing Simulation is a recurring managed service that delivers simulated phishing campaigns to the Client's Authorised Users on a regular cadence (twelve (12) campaigns per annum is the standard cadence, delivered monthly, unless the Order Form identifies a different cadence). Simulated campaigns use tailored templates, customisable landing pages and simulated attachments to test the Client's user resilience to phishing techniques. Detailed reporting is provided to the Client through the Third Party Provider's platform and through Lanmark's monthly reporting under Clause 6.4.

3.1.2 Security Awareness Training is delivered in combination with Phishing Simulation as a single commercial offering. Security Awareness Training comprises a library of courses, videos and quizzes covering cyber hygiene, recognition of phishing and social engineering, secure password and credential practice, mobile and remote working security, data handling, and similar topics. Training content is delivered to Authorised Users through the Third Party Provider's platform.

3.1.3 Phishing Simulation combined with Security Awareness Training is delivered on a per-user recurring monthly subscription basis. The unit of charge is per Authorised User enrolled in the Service. The Order Form identifies the agreed number of Authorised Users at the Service Start Date and the per-user Fee.

3.1.4 The Phishing Simulation in this Schedule is a continuous, programme-style service. It is distinct from the one-off Social Engineering Campaign that may form part of a Penetration Testing engagement under the Cyber Assessments Services Schedule. The two services are not interchangeable: the Phishing Simulation programme aims to change user behaviour over time through repeated tests and training, while a Social Engineering Campaign in PT is a one-off controlled attack simulation forming part of a point-in-time penetration test.

3.2 Cyber Essentials Certification

3.2.1 The Certification Engagement supports the Client through preparation for, and obtaining of, Cyber Essentials or Cyber Essentials Plus certification. Certification is awarded by IASME under the Cyber Essentials scheme rules in force from time to time. Lanmark and the Third Party Provider provide the preparation, gap analysis, remediation guidance, evidence support, Assessment Submission and (for CE Plus) audit support, but the certification award itself is made by IASME.

3.2.2 Each Certification Engagement covers a single certification at one of the levels and tiers below, as identified in the Order Form:

(a) Certification level: CE or CE Plus;

(b) Service tier: Self-Service (preparation guide, precheck, IASME certification fee, no consultancy hours); Assisted Service (Self-Service plus the Cyber Essentials Toolkit and two (2) Consultancy Hours); or Managed Service (Self-Service plus the Cyber Essentials Toolkit and eight (8) Consultancy Hours).

3.2.3 The Cyber Essentials Toolkit comprises template policy documents and supporting content produced by the Third Party Provider and made available to the Client through the Third Party Provider's platform. The Toolkit is included in the Assisted Service and Managed Service tiers.

3.2.4 The Third Party Provider's platform permits the Client to make unlimited Assessment Submissions during the Certification Engagement. This unlimited-resubmission capability is the operational mechanism of the platform's 100% pass guarantee: where the Client implements the Recommended Remediation in full, the Client will achieve certification through one or more Assessment Submissions during the Certification Engagement. Lanmark passes this guarantee through to the Client subject to Clauses 3.2.5 to 3.2.7.

3.2.5 For the purposes of this Clause 3.2, Recommended Remediation is treated as 'implemented in full' only where Lanmark or the Third Party Provider has confirmed in writing, or through the Third Party Provider's platform, that each item of Recommended Remediation has been implemented or has been formally accepted by Lanmark or the Third Party Provider as replaced, excused or not required.

3.2.6 Where the Client does not pass an Assessment Submission (whether or not the Client has implemented the Recommended Remediation in full), the Client may revise the in-scope environment, address the matters identified in the Third Party Provider's platform feedback, and resubmit the Assessment Submission through the Third Party Provider's platform. The Client may do this an unlimited number of times during the Certification Engagement. The Client can submit (and resubmit) directly through the Third Party Provider's platform, which is the operational basis on which the Self-Service tier works without included Lanmark Consultancy Hours.

3.2.7 The Consultancy Hours included in the Assisted Service tier (two (2) hours) and the Managed Service tier (eight (8) hours) are the total Lanmark consultancy commitment for the Certification Engagement. They are intended to support the Client with questions, completion of the assessment questionnaire on the Third Party Provider's platform and general Cyber Essentials guidance, including (where the Client requests it) consultancy support in connection with revision and resubmission. No additional Consultancy Hours arise on a non-pass Assessment Submission. Where the Client requires consultancy time beyond the Consultancy Hours included in the tier, additional hours are chargeable at Lanmark's published rate card. Where the Client has not implemented the Recommended Remediation in full (as defined in Clause 3.2.5), the Client may still use the Third Party Provider's platform to resubmit but the platform's pass guarantee does not apply to a submission that proceeds without full implementation.

3.2.8 Where the Client successfully achieves CE or CE Plus certification, the Client is eligible (under the IASME scheme rules) for cyber insurance and related benefits provided by the insurer designated by IASME from time to time. The cyber insurance and any related benefits are a benefit of IASME certification, are provided by the insurer and IASME, and are not a Lanmark service. Clause 12 (Relationship with Third Party Providers) and Clause 9.5 (Cyber insurance disclaimer) apply.

3.3 Microsoft Intune to Cyber Essentials Standards

3.3.1 The Intune to CE Engagement is a project engagement to configure the Client's Microsoft Intune environment to align with the Cyber Essentials technical controls (boundary firewalls and internet gateways, secure configuration, user access control, malware protection, and patch management). The engagement scope, deliverables, milestones and Fees are identified in the Order Form, sized by reference to the Client's environment (number of devices, complexity of existing configuration and integration work required).

3.3.2 The Intune to CE Engagement is typically sold as a separate project from a Certification Engagement. The Client may take the Intune to CE Engagement on its own (for example, to harden the environment in advance of pursuing certification) or alongside a Certification Engagement (where Intune-based configuration is part of the remediation required for the Client to meet the CE technical controls).

3.3.3 The Intune to CE Engagement does not in itself produce Cyber Essentials certification. Certification (where the Client requires it) is obtained through a Certification Engagement under Clause 3.2.

4. In scope and out of scope

4.1 In scope

The Service includes:

(a) the offerings selected by the Client in the Order Form (Phishing Simulation and Security Awareness Training, Certification Engagement at the selected level and tier, Intune to CE Engagement, or any combination);

(b) use of the Third Party Provider's platforms for Phishing Simulation and Security Awareness Training, and for the Certification Engagement, in accordance with the Third Party Provider Terms;

(c) Lanmark Client-side engagement management during Support Hours, including onboarding, monthly reporting (where applicable), Consultancy Hours management (where applicable) and routing of communications between the Client and the Third Party Provider;

(d) 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 work identified during a Certification Engagement that goes beyond the Consultancy Hours included in the relevant tier, and Intune configuration work that goes beyond the scope of the agreed Intune to CE Engagement (Order Form-based separately-quoted work, the Project Services Schedule, or where appropriate the IT Support Services Schedule);

(b) any infrastructure procurement, hardware refresh, software licensing or systems integration work required to meet the Cyber Essentials technical controls (separately quoted as project work);

(c) ongoing Managed Detection and Response, Identity Threat Detection and Response and Managed SIEM (Managed Cyber Security Services Schedule);

(d) Vulnerability Assessment, Penetration Testing and the one-off Social Engineering Campaign that may form part of a Penetration Testing engagement (Cyber Assessments Services Schedule);

(e) general IT support, including endpoint configuration, user administration and tenant administration unrelated to the Service (IT Support Services Schedule);

(f) incident response activity in the event of an actual phishing attack, credential compromise or other Security Incident, including forensic investigation, regulatory breach reporting and recovery (covered by the Managed Cyber Security Services Schedule and the Cyber Assessments Services Schedule, as applicable, or by separately-quoted incident response work);

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

5. Service Levels

5.1 Phishing Simulation and Security Awareness Training

5.1.1 Phishing Simulation campaigns are delivered to the Client's Authorised Users on the cadence identified in the Order Form (twelve per annum by default, monthly). Each campaign is scheduled and delivered by the Third Party Provider's platform in accordance with the Third Party Provider Terms.

5.1.2 Security Awareness Training content is made available to Authorised Users continuously through the Third Party Provider's platform, with new content released by the Third Party Provider in accordance with its content roadmap.

5.1.3 Lanmark provides a monthly summary report covering the previous month's Phishing Simulation results and Security Awareness Training engagement, in accordance with Clause 6.4. The monthly summary report is provided within fifteen (15) Business Days of the end of the relevant calendar month.

5.2 Certification Engagement

5.2.1 The duration of a Certification Engagement depends on the Client's starting compliance position, the certification tier selected and the Client's remediation pace. Lanmark and the Third Party Provider will agree an indicative timeline with the Client at the start of the engagement. The standard expectation is that a Self-Service or Assisted Service CE engagement is completed within twelve (12) weeks of the start of the engagement, and that a Managed Service CE engagement or a CE Plus engagement is completed within twenty (20) weeks; these are targets and not commitments, in recognition that the duration depends materially on Client cooperation and remediation pace.

5.2.2 Consultancy Hours included in the Assisted Service and Managed Service tiers are scheduled with the Client during the engagement. Lanmark will use reasonable endeavours to schedule Consultancy Hours within Support Hours and with reasonable notice to the Client.

5.2.3 Where the Client implements the Recommended Remediation in full, the timing of the Assessment Submission and the issue of the certification are governed by the Third Party Provider's platform and IASME's scheme rules in force from time to time.

5.3 Intune to CE Engagement

5.3.1 The Intune to CE Engagement is delivered against the milestones, deliverables and timeline identified in the Order Form. Where the Order Form does not identify a specific timeline, the engagement is delivered with the duration appropriate to the agreed scope, sized by reference to the Client's environment.

5.4 Third Party Provider, IASME and insurer dependencies

5.4.1 The Service depends on the operation of Third Party Providers' platforms, on the IASME Cyber Essentials scheme rules and operating processes, and (in respect of the cyber insurance benefit at Clause 3.2.8) on the insurer designated by IASME. The applicable operating standards, scheme rules, assessment timelines and operating processes for those

dependencies are as published by the relevant Third Party Provider, IASME or the insurer from time to time. These dependencies are not service elements provided by Lanmark.

5.4.2 Lanmark does not commit to operating standards, scheme rules, assessment timelines or operating processes that are different from, or more onerous than, those published by the relevant Third Party Provider, IASME or the insurer for the activity in question. Where a Third Party Provider fails to meet its operating 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. Where IASME or the designated insurer fails to meet a scheme rule, an operating process or an insurer term, the Client's recourse is in accordance with the IASME scheme rules and the insurer's terms in force from time to time; Lanmark has no obligation or liability in respect of those matters. This Clause 5.4.2 is a Service-specific application of Clause 17.4 of the MSA.

5.5 Service Level measurement and exclusions

5.5.1 Lanmark's records of engagement activity (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 platform activity, training engagement, campaign results, Certification Engagement progress and Assessment Submission outcomes are the authoritative record of Third Party Provider activity.

5.5.2 Time spent waiting for Client action (including delay in providing access, delay in implementing Recommended Remediation, delay in confirming Authorised User lists, delay in scheduling Consultancy Hours, or any other Client-controlled matter) does not count towards any applicable Service Level.

5.5.3 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. The Client's specific position where the Client does not pass an Assessment Submission is set out at Clauses 3.2.4 to 3.2.7 (unlimited-resubmission capability through the Third Party Provider's platform, with the included Consultancy Hours allocation as the total Lanmark consultancy commitment). Otherwise, where Lanmark or a 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 5.5.3 (read with Clauses 3.2.4 to 3.2.7) 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.

6. Operational arrangements

6.1 Onboarding

6.1.1 Onboarding for the Phishing Simulation and Security Awareness Training offering includes initial discussion, design of the Client's first phishing campaign, setup of Authorised Users on the Third Party Provider's platform, and testing and validation. The onboarding Fee is identified in the Order Form.

6.1.2 Onboarding for a Certification Engagement includes initial discussion, access to the Third Party Provider's platform, the precheck to assess compliance gaps against the Cyber Essentials technical controls, and (for Assisted Service and Managed Service tiers) access to the Cyber Essentials Toolkit. The onboarding work is included in the Certification Engagement Fee and is not separately charged.

6.1.3 Onboarding for an Intune to CE Engagement is part of the engagement scope identified in the Order Form.

6.2 Consultancy Hours management

6.2.1 Consultancy Hours are scheduled by agreement between the Client and Lanmark during a Certification Engagement. The Client should request Consultancy Hours through the Service Tooling or through the Client's nominated Lanmark contact for the engagement.

6.2.2 Unused Consultancy Hours expire on completion of the Certification Engagement, whether or not the Client passes the Assessment Submission. Unused Consultancy Hours do not roll over to a subsequent Certification Engagement or to any other Service. Where the Client requires consultancy time beyond the Consultancy Hours included in the tier, additional hours are chargeable at Lanmark's published rate card.

6.2.3 Consultancy Hours are intended to support preparation, remediation, evidence gathering, Assessment Submission and (for CE Plus) audit support in connection with the Certification Engagement. They are not intended for use on unrelated work.

6.2.4 For the purposes of Clause 6.2.2, a Certification Engagement is treated as complete on the earliest of:

(a) the issue of certification by IASME under the Cyber Essentials scheme. For the avoidance of doubt, a non-pass outcome on an individual Assessment Submission does not, on its own, complete the Certification Engagement; the Client retains the unlimited-resubmission capability at Clause 3.2.6 unless and until the engagement is otherwise closed under sub-paragraphs (b), (c) or (d) below;

(b) the expiry of the indicative engagement timeline at Clause 5.2.1 (twelve (12) weeks from the start of the engagement for a Self-Service or Assisted Service CE engagement, or twenty (20) weeks from the start of the engagement for a Managed Service CE engagement or a CE Plus engagement at any tier), unless Lanmark agrees in writing to extend that period;

(c) the Client's written notice of withdrawal from the engagement;

(d) the Client's failure to respond to Lanmark, or to engage with the Third Party Provider's platform, for a continuous period of six (6) weeks during the engagement.

6.3 Recommended Remediation

6.3.1 During a Certification Engagement, Lanmark and the Third Party Provider identify Recommended Remediation in writing through the Third Party Provider's platform and (where applicable) through Lanmark's Consultancy Hours. The Client is responsible for implementing the Recommended Remediation in accordance with Clause 7.

6.3.2 Where the Client cannot or does not implement an item of Recommended Remediation, the Client should inform Lanmark in writing so that an alternative approach (or a decision to proceed to Assessment Submission without that item) can be agreed. Where Recommended Remediation is not implemented and is not formally replaced or excused, Clause 3.2.6 applies.

6.4 Reporting

6.4.1 For Phishing Simulation and Security Awareness Training, Lanmark provides the Client with a monthly summary report under Clause 5.1.3, covering campaign results, user engagement with training, repeat-click patterns and recommendations. The Third Party Provider's platform additionally provides detailed reporting that the Client may access directly.

6.4.2 For a Certification Engagement, Lanmark provides progress updates through the Service Tooling and (where applicable) through Consultancy Hours sessions. Formal Assessment Submission outcomes are issued by the Third Party Provider's platform and IASME.

6.4.3 For an Intune to CE Engagement, Lanmark provides progress updates against the milestones identified in the Order Form.

7. Client responsibilities

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

(a) provide accurate and complete information about the Authorised Users to be enrolled in Phishing Simulation and Security Awareness Training, and about the in-scope environment for a Certification Engagement or Intune to CE Engagement;

(b) promptly notify Lanmark of any material change to the Authorised User population, the in-scope environment or the certification scope during the engagement;

(c) permit and facilitate the deployment of, and access to, the Third Party Provider's platforms by the Client's Authorised Users, including the configuration of Microsoft 365 connectors, email allow-lists for simulated phishing campaigns, single sign-on integration and similar onboarding tasks;

(d) encourage Authorised User participation in Security Awareness Training and respond to Phishing Simulation reporting outputs (including, where appropriate, additional training or coaching for users who repeatedly engage with simulated phishing emails);

(e) ensure that Phishing Simulation campaigns are not configured to collect actual Authorised User passwords, credentials, multi-factor authentication codes, payment data or other sensitive Client data, save where Lanmark and the Client have expressly agreed appropriate technical and organisational safeguards in writing in advance of the campaign;

(f) where the Client subscribes to a Certification Engagement, implement the Recommended Remediation in full and within the timescales agreed during the engagement (Clauses 3.2.4 to 3.2.7 apply);

(g) where the Client subscribes to an Intune to CE Engagement, grant Lanmark the access required to the Microsoft 365 tenant, the Intune service and the Client's device estate; and provide accurate inventory and configuration information;

(h) respond promptly to Lanmark requests for information, evidence, approval or scheduling in connection with the Service;

(i) comply with the Third Party Provider Terms to the extent those terms apply to the Client's use of the Service, including any acceptable use rules for the Phishing Simulation platform, the Cyber Essentials platform, and the cyber insurance benefit;

(j) where the Client achieves Cyber Essentials certification and is consequently eligible for the IASME cyber insurance benefit, satisfy any conditions of that insurance directly with IASME and the insurer; the cyber insurance benefit is not a Lanmark service.

Where the Client does not meet a responsibility under this Clause 7, and that failure causes or materially contributes to a delay in the Service, a failure of the Service, a failure to achieve certification, a Client loss arising in connection with the Service or a third-party claim, Lanmark and the Third Party Providers 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 Authorised Users targeted by Phishing Simulation), 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) the Client's breach of any obligation under this Schedule, the MSA or the Third Party Provider Terms;

(b) the Client's failure to enrol or de-enrol Authorised Users in Phishing Simulation accurately, or the Client's targeting of Authorised Users in a manner not authorised by the Client's own internal policies;

(c) the Client's provision of inaccurate, incomplete or misleading information about the Authorised User population, the in-scope environment or the certification scope;

(d) the Client's failure to implement Recommended Remediation that the Client has expressly agreed to implement, where that failure causes harm to a third party;

(e) the Client's reliance on, use of, or failure to comply with the terms of the IASME cyber insurance benefit, the IASME scheme rules or the insurer's terms, where a third-party claim or regulatory action against Lanmark arises in connection with that reliance, use or failure to comply.

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, the Third Party Providers' methodology or platforms, 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 no guarantee of security or compliance

9.1 Phishing Simulation and Security Awareness Training aim to reduce, but do not eliminate, the Client's exposure to phishing-based cyber attacks. Lanmark and the Third Party Provider do not warrant or guarantee that Phishing Simulation will: (a) prevent any actual phishing attack against the Client; (b) result in zero user click-through on real phishing emails; or (c) achieve any particular reduction in Client phishing risk metrics over time. Reducing phishing risk depends on user engagement with training, Client culture and broader cyber controls maintained by the Client.

9.2 Security Awareness Training content is supplied by the Third Party Provider in accordance with its content roadmap. Lanmark does not give any separate warranties (express, implied or statutory) in respect of the Third Party Provider's training content, the currency of any specific training module or the suitability of the training for any particular regulatory requirement, 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 configure and manage the Service in accordance with the MSA and this Schedule.

9.3 The Third Party Providers' platforms, content, methodology, assessor function and certification work 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 Providers' platforms, content, methodology, assessors or other deliverables, save to the extent that any such warranty cannot be excluded under applicable law. This Clause 9.3 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, configure and manage the Service in accordance with the MSA and this Schedule.

9.4 Cyber Essentials certification, where achieved, confirms that the Client has met the requirements of the Cyber Essentials scheme as assessed by IASME. It does not guarantee that the Client will not experience a cyber incident, that the Client's systems are free from vulnerabilities, that the Client meets every regulatory or contractual security requirement, or that the Client's broader cyber resilience posture is sufficient for the Client's specific risk profile. Cyber Essentials is one element of a broader cyber resilience posture that the Client should maintain (including ongoing monitoring, incident response capability, backup arrangements and cyber insurance).

9.5 The cyber insurance benefit available to organisations that achieve Cyber Essentials certification is provided by IASME and the insurer designated by IASME under the Cyber Essentials scheme rules. It is not a Lanmark service. Lanmark does not warrant the availability, cover, exclusions or claims handling of the cyber insurance, gives no advice in respect of it, and is not liable in respect of any matter arising under the cyber insurance. The Client should review the cyber insurance terms directly with IASME or the designated insurer to confirm cover, eligibility and conditions.

9.6 Subject to Clause 18 of the MSA, Lanmark is not liable for any actual phishing attack, credential compromise, Security Incident, regulatory action, certification failure or other Client loss that occurs while the Service is in operation, to the extent that the Service has operated in accordance with this Schedule and the Third Party Provider Terms. The Service is one

element of the Client's broader cyber resilience posture; it does not transfer the Client's residual cyber risk to Lanmark.

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 Compliance and Training Service
Subject matter of the processing	Provision of the Cyber Compliance and Training Service, comprising the delivery of simulated phishing campaigns and security awareness content to Authorised Users, the assessment of Authorised User engagement and performance, the preparation for and obtaining of Cyber Essentials and Cyber Essentials Plus certification, and the configuration of the Client's Microsoft Intune environment to align with the Cyber Essentials technical controls.
Duration of the processing	For the duration of each Service offering (recurring for Phishing Simulation and Security Awareness Training; the duration of the engagement for a Certification Engagement or an Intune to CE Engagement), plus reasonable retention periods for results, reports and certification records. Lanmark-held records are governed by Lanmark's Data Protection and Retention Policy. The Third Party Providers' platforms retain records (including campaign results, training engagement records, assessment submissions and certification records) in accordance with the Third Party Provider Terms. IASME retains certification records in accordance with the IASME scheme rules.
Nature and purpose of the processing	Collection, organisation, structuring, retrieval, consultation, use and (where applicable) deletion of Personal Data for the purpose of delivering phishing simulation, security awareness training, cyber compliance preparation, certification submission, technical configuration and reporting.
Types of Personal Data	Authorised User identification data (name, role, email address, work telephone, sign-in identifiers); Phishing Simulation interaction data (clicked links, submitted forms, opened emails, reported emails, completion of training modules, quiz scores, training progress); Certification Engagement evidence data (information about the Client's IT environment, policy documents, configuration screenshots, evidence submissions); Microsoft Intune configuration data captured during an Intune to CE Engagement; nominated Client contact details for the Service.
Categories of data subject	Authorised Users of the Client; Client employees and contractors enrolled in Phishing Simulation and Security Awareness Training; the Client's nominated security or compliance contact and signatories of assessment submissions.
Documented instructions for processing	Set out in the MSA, this Schedule, the Order 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 Providers' platforms; the Client's instructions to Lanmark remain governed by the MSA and the Data Protection Legislation.

Phishing Simulation campaigns are not configured to collect actual Authorised User passwords, credentials, multi-factor authentication codes, payment data or other sensitive Client data, save where Lanmark and the Client have expressly agreed appropriate technical and organisational safeguards in writing in advance (Clause 7(e) applies). Simulated landing pages and forms are designed to capture engagement metadata (whether the user clicked, submitted, opened or reported) and not real credentials.

Phishing Simulation and Security Awareness Training do not typically involve special category or criminal offence Personal Data. The Service is not designed for the routine processing of either category. Where a Certification Engagement or an Intune to CE Engagement incidentally surfaces Personal Data of these categories (for example, where the Client's evidence material contains incidental information about health, criminal record checks or similar matters), the Client will inform Lanmark before testing or evidence submission 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
Phishing Simulation and Training platform provider	Provision of the platform that delivers simulated phishing campaigns, security awareness training content, training engagement tracking, campaign reporting and Authorised User enrolment.
Cyber Essentials platform and assessor provider	Provision of the white-labelled platform used to deliver Certification Engagements, the precheck functionality, the Cyber Essentials Toolkit, the Assessment Submission mechanism and (for CE Plus) the technical audit. The platform provider's assessors are authorised to recommend the award of certification through IASME under the Cyber Essentials scheme rules in force from time to time.
Service Tooling provider	Provision of the Lanmark service management system used for Client-side engagement, Consultancy Hours management and Lanmark reporting.

The current Sub-Processor in each category is 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, the location of processing and any applicable international transfer mechanism.

IASME and Microsoft

IASME is the certification body that awards Cyber Essentials and Cyber Essentials Plus certifications under the Cyber Essentials scheme. IASME is not a Lanmark Sub-Processor for this Service. IASME's role in respect of the Client's certification submission and the cyber insurance benefit is governed by the IASME scheme rules in force from time to time and by the insurer's terms (as applicable).

Microsoft Corporation is not a Lanmark Sub-Processor for this Service. Where an Intune to CE Engagement is in scope, the Service uses the Client's existing Microsoft 365 tenant and Microsoft Intune subscription. Microsoft's role in respect of the Client's tenant and Intune subscription is governed by the Microsoft terms applicable to the Client's tenant directly.

12. Relationship with Third Party Providers and IASME

12.1 The substantive elements of the Service are delivered through Third Party Providers' platforms and (in the case of Cyber Essentials certification) through IASME. Lanmark configures, manages and presents the Service to the Client, but does not itself deliver the underlying platform, training content, assessment activity or certification award.

12.2 Where Lanmark presents a Third Party Provider's platform, content, methodology, assessor function or certification workflow to the Client under Lanmark's brand (a white-labelled arrangement), Lanmark's obligations under this Schedule are limited to Lanmark's own configuration, management and engagement responsibilities. The underlying platform, content, methodology, assessor function and certification workflow remain the Third Party Provider's. Clause 17 of the MSA applies.

12.3 Where the Service depends on the operation of a Third Party Provider's platform or on IASME's scheme rules, Lanmark's obligations under this Schedule are subject to that Third Party Provider's or IASME's operation in accordance with the Third Party Provider Terms or the IASME scheme rules. Lanmark is not liable for any act or omission of a Third Party Provider or of IASME, including any failure of the platform to operate as expected, any change in the IASME scheme rules, or any change in the cyber insurance terms or the conduct of the insurer.

12.4 The Client may request a copy or current reference for the Third Party Provider Terms applicable to the Service and the current IASME scheme rules from Lanmark.

13. Service-specific commercial terms

13.1 The Fees for the Service are set out in the Order Form. The unit of charge for each offering is as follows:

(a) Phishing Simulation and Security Awareness Training: per Authorised User per month, on a recurring subscription basis;

(b) Certification Engagement: per engagement, by reference to the certification level (CE or CE Plus) and the service tier (Self-Service, Assisted Service or Managed Service) identified in the Order Form;

(c) Intune to CE Engagement: per engagement, sized to the Client's environment as identified in the Order Form.

13.2 Onboarding Fees (where applicable) are identified in the Order Form. For Phishing Simulation and Security Awareness Training, an onboarding Fee may apply at the start of the first subscription period and is not normally repeated on renewal, save where the engagement requires materially new onboarding work.

13.3 Consultancy time required beyond the Consultancy Hours included in a Certification Engagement tier is chargeable at Lanmark's published rate card at the time the work is performed.

13.4 The IASME certification fee is included in each Certification Engagement tier as set out in the Order Form. IASME certification fees are passed through from IASME and are not Lanmark Fees. Where IASME changes its certification fees, Lanmark may pass through the change in accordance with Clause 7.10 of the MSA (Third Party Provider pass-through).

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 Compliance and Training Service:

(a) Clauses 5.4.1, 5.4.2 and 5.5.3 of this Schedule set the Service-specific Service Level position. The Service depends on Third Party Providers' platforms, on the IASME Cyber Essentials scheme rules and operating processes, and on the insurer designated by IASME (for the cyber insurance benefit). Lanmark passes through, and does not commit to operating standards more onerous than, those published by the Third Party Providers, IASME or the insurer; Lanmark's obligation and liability for Third Party Provider failures is limited to using reasonable endeavours to pass through or assist the Client with remedies under the Third Party Provider Terms; the Service Levels do not give rise to service credits. The Client's specific position where the Client does not pass an Assessment Submission is set out at Clauses 3.2.4 to 3.2.7: the Third Party Provider's platform permits unlimited Assessment Submissions during the Certification Engagement, and the included Consultancy Hours allocation for the engagement tier is the total Lanmark consultancy commitment. This is a Service-specific application of Clauses 17.4 and 18.4 of the MSA;

(b) Clause 8 of this Schedule sets out a Service-specific indemnity from the Client to Lanmark, limited to third-party claims and regulatory action against Lanmark, and to Lanmark's reasonable costs and expenses incurred in responding, with triggers tied to Client-controlled risk in this Service (including third-party claims arising from the Client's reliance on, use of, or failure to comply with the IASME cyber insurance benefit, scheme rules or insurer 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 Phishing Simulation and Security Awareness Training reduce but do not eliminate phishing risk, that Lanmark gives no separate warranties for the Third Party Provider's training content or platforms (while preserving Lanmark's own configuration and management obligations), that Cyber Essentials certification is not a guarantee of security, that the IASME cyber insurance benefit is a third-party benefit and not a Lanmark service, and that Lanmark is not liable for cyber-related loss occurring while the Service operates in accordance with this Schedule and the Third Party Provider Terms. These disclaimers do not affect Lanmark's own obligation to plan, configure 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.