

Terms and Conditions

These are the terms and conditions for the contract between:

- we, us, Citation Cyber Limited (registered in England and Wales with company number 08314901) and with our registered offices at Kings Court, Water Lane, Wilmslow, Cheshire SK9 5AR. and
- you, our customer, for us to provide you with the “Services” which are those set out in the Order Form (as defined below).

These terms apply to the exclusion of any other terms that you may seek to impose or incorporate into the provision of the services, or which are implied by law, trade custom practice or course of dealing.

1. The Contract

(a) Basis of contract

The contract between you and us (the “Contract”) is made up of:

- (i) these terms and conditions (“**Terms and Conditions**” also referred to as “**General Terms**” in the Service Schedules);
- (ii) the Terms of Use which can be found at <https://auth.citation-atlas.co.uk/identity/terms/termsofuse/> (“**Terms of Use**”);
- (iii) the Service Schedules, that apply to different services supplied by us and as agreed in the Order Form;
- (iv) the Order Form setting out the services to be purchased by you under these Terms and Conditions; and
- (v) any other documents referred to in these Terms and Conditions that is stated as forming part of the Contract.

The order of precedence of these documents shall be the order set out above. These Terms and Conditions apply to the Contract. No other terms and conditions will apply. Any samples, drawings, descriptive matter or advertising issued by us the and any descriptions or illustrations contained in our marketing material electronic or otherwise, are issued or published for the sole purpose of giving an approximate idea of the Services described in them. They do not form part of the Contract and are not legally binding.

The Order Form constitutes an offer by you to purchase the Services in accordance with these Terms and Conditions.

(b) Commencement and Duration

The Order shall only be deemed to be accepted on the earlier of (i) both parties signing the Order Form; or (ii) us issuing written acceptance of the Order Form and commencing performance of the Services, at which point and on which date a Contract shall come into existence (**Commencement Date**) and continue for 12, 24, 36 months from the Commencement Date (**Order Term**) unless otherwise specified in the Order Form. At the end of the Order Term, the Contract shall automatically continue for another 12,24, 36 months (Renewal Term) and for all Cyber Essentials and Cyber Essentials Plus contracts, the Order Term shall auto renew from the date of certification unless specified as a ‘one off’ in the Order Form which is not subject to auto renew, unless either party provides at least ‘2 months’ written notice to terminate the Contract, such notice period to end no earlier than the last day of the Order Term or applicable Renewal Term, unless terminated in accordance with any special term contained with an Order Form or in accordance with these Terms and Conditions. If we cannot or do not accept your order for any reason, we will tell you this by email and will not provide any of the Services. If you have already paid for the Services, we will refund the full amount, including any delivery charges, as soon as possible.

2. The services

- (a) We will provide the Services in accordance with the Contract.
- (b) We reserve the right to amend the Services and any Order Form if necessary to comply with any applicable law or regulatory requirement, or if the amendment will not materially affect the nature or quality of the Services, and we will give you reasonable notice in any such event.
- (c) We will use all reasonable endeavours to meet any performance dates specified in an Order Form or Service Schedule, but any such dates shall be estimates only and time shall not be of the essence for performance of the Services
- (d) Unless we agree otherwise in writing, you may only make the Services available to your officers and employees, not to any supplier or other third party.
- (e) We will provide the Services with reasonable care and skill. You and we agree that all terms and conditions implied by law, or otherwise (including those implied under the Sale of Goods Act 1979 and the Supply of Goods and Services Act 1982) are excluded to the fullest extent permitted by law.
- (f) If we agree to supply additional Services not in the existing Order Form, we will enter into an additional Order Form with you, which will also be subject to these Terms and Conditions.
- (g) Any quotations that we may give will only be valid for a period of 20 Business Days (a “**Business Day**” being a day other than a Saturday, Sunday or public holiday in England, when banks in London are open for business) from its date of issue.

3. Customer obligations

- (a) You must do the following:
 - (i) make sure that the information in the Order Form is complete and accurate;
 - (ii) co-operate with us in all matters relating to the Services;
 - (iii) ensure that you and all users accessing the Services comply with these Terms and Conditions, the Terms of Use, and any other licenses or policies relating to the Services (and remain liable for any default by such persons), the Service Schedules and Order Form;
 - (iv) make sure that anyone ordering additional services has the authority to do so;
 - (v) make sure that the content provided as part of the Services is only used internally for your own purposes and is not used for any other purpose, used commercially, or made available to any third party, without our permission in writing;

- (vi) provide us (including anyone working for us in connection with the Services) the access we reasonably need to your premises and other facilities in order to provide the Services;
- (vii) give us any information we may reasonably need to provide the Services, and make sure that the information is accurate. This includes providing information about all incidents which would give rise to you using the Services as soon as possible after these arise;
- (viii) prepare your premises, IT infrastructure, systems and networks for the Services as we reasonably specify;
- (ix) comply with all laws that apply to your activities relating to the Contract;
- (x) obtain and maintain all necessary licenses, consents, and permissions necessary for you and anyone using the Services on your behalf to perform your obligations under the Contract;
- (xi) ensure that your network and systems comply with any specifications we may provide from time to time in order for you to get access the Services;
- (xii) promptly tell us if the number of employees and workers has grown by more than 50% since the start of the Contract, or you want us to provide the Services to other sites. In this situation we have the right to increase the charges to reflect this. This would be on top of any increase we make under clause 4 (e);
- (xiii) be solely responsible for procuring, maintaining and securing your network connections and telecommunications links; and all problems, conditions, delays and all other loss or damage arising from or relating to your network connections or telecommunications links or caused by the internet in order for you to get access the Services;
- (xiv) follow all our advice and recommendations and it is your responsibility for adopting any recommendations within any report we provide you to meet your needs and legal requirements;
- (xv) ensure that the Authorised Users (as defined in the Terms of Use) use the Services and any associated documentation in accordance with the terms of the Contract and you shall be responsible for any Authorised User’s breach of the Contract;
- (xvi) If we cannot meet any of our obligations under the Contract, or we are delayed from meeting them, as a result of something you have or have not done, or you failing to meet any of your obligations, we will not be liable to you for this failure or delay and we can suspend the Services until you put the matter right. Taking this action will not affect any other rights we have under the Contract
- (xvii) Customers are required to utilise all of their bundled penetration testing days and all products and services in packages as part of a managed service by the end of the contract. Failure to do so will result in the forfeiture of any unused days, products, and services. It is the responsibility of the customer to ensure that all days, products and services are utilised within the specified time frame.

4. Charges and payment

- (a) The charges for the Services are as calculated in the Order Form (“**Charges**”). For any services not detailed in an Order Form, the Charges shall be calculated on a time and materials basis in accordance with our daily fee rates, as set out in our current price list or otherwise made available by us by the Commencement Date.
- (b) Our daily fee rates for each individual are calculated on the basis of an eight-hour day from 9.00 am to 5.00 pm worked on Business Days. We shall be entitled to charge an overtime rate of 150% of the daily fee rate on a pro-rata basis for each part day or for any time worked by individuals whom we engage on the Services outside these hours, unless otherwise agreed in the Order Form.
- (c) We shall be entitled to charge you for any expenses reasonably incurred by the individuals whom we engage in connection with the Services including travelling expenses, hotel costs, subsistence and any associated expenses, and for the cost of services provided by third parties and required by us for the performance of the Services, and for the cost of any materials;
- (d) The charges for the Services do not include VAT, which you will also have to pay to us, at the rate that applies at the time.
- (e) From the first anniversary of the Commencement Date, we can increase our charges once a year by the greater of:
 - (i) 3%; or
 - (ii) the percentage by which the UK Retail Prices Index has increased by over the previous year.
- (f) For Penetration Testing we will invoice you at the point the test is booked. For all other products we will invoice you upon contract signature, unless otherwise set out in the order form. Where possible we will collect our charges, plus VAT, from your bank account by direct debit.
- (g) If we do not receive any payment due to us under the Contract by the date it is due, we can charge you interest each day on the overdue amount at the rate of 5% per annum above The Bank of England published bank rate at the time, until the overdue amount and interest has been paid off in full. You will be responsible for any loss, liability, damage, costs and expenses (including legal costs) arising in connection with us recovering any unpaid and overdue amounts; You must pay all amounts due under the Contract without taking off any amount (except for any deduction that must be made by law). We may take any amount you owe us off any amount we must pay to you. Taking this action will not affect any other rights we have under the Contract.
- (h) Once the Contract has been formed in accordance with clause 1, the Customer cannot cancel any order for Services, however, the Customer may request any Services to be rescheduled on the following basis:
 - (i) the Customer may reschedule any Services without liability by providing the Supplier receives written notice to reschedule more than 28 calendar days prior to the Agreed Start Date (as set out in the Order Form) for the relevant Service; however, the Customer will be liable for the cost of any travel or accommodation expenses that have already been made by the Supplier and which are non-refundable;

- (ii) the Customer may reschedule any Services from 28 to 21 calendar days prior to the Agreed Start Date by providing written notice at that time, subject to a rescheduling fee, in addition to the agreed Charges, equivalent to 25% of the total Charges for the Service;
- (iii) the Customer may reschedule any Services from 20 to 11 calendar days prior to the Agreed Start Date by providing written notice at that time, subject to a rescheduling fee, in addition to the agreed Charges, equivalent to 50% of the total Charges for the Service;
- (iv) the Customer may not reschedule the Services from 10 calendar days or fewer before the Agreed Start Date of a Service and the full Charges for the Services will still be payable by the Customer even if the Customer does not accept performance of the Services on the Agreed Start Date.
- (i) The Supplier reserves the right to reschedule a Service up to 10 Business Days prior to the Agreed Start Date without liability to the Customer.

5. Intellectual property rights

- (a) All intellectual property rights relating to any data, software, materials, services and/ or other deliverables provided by us or on our behalf under the Contract (for example, templates, guides, handbooks and policies) (“**our Materials**”) belong to us or the relevant third party rights owner. If any intellectual property rights belong to a third party, we have the licences and consents we need to provide the Services to you. You will not own any of the intellectual property rights in any of our Materials or which arise as a result of us providing the Services. (Intellectual property rights are any rights and interest in patents, trademarks, service marks, trade and business names, rights in design, copyright, database rights, know-how, rights to apply for these and any other similar rights which in each case exist at any time anywhere in the world.)
- (b) Subject to payment of the charges in accordance with clause 4, we grant you a non-exclusive, non-transferable right, without the right to grant sublicences, to permit your Authorised Users to use the Services and our Materials during the relevant Subscription Term solely for your internal business operations at the Sites. Defined terms in this clause 5(a) have the meaning given to them in the Terms of Use.
- (c) If we terminate this Contract under clause 9, the above licence will automatically terminate, save in relation to the Deliverables provided that the Customer has complied with clause 9(c). (Deliverables are all documents and materials developed by us or our agents, subcontractors, consultants and employees solely in relation to the Services in any form).
- (d) You can use our Materials only for the purpose of receiving the Services for your own internal business purposes at the Sites (as defined in the Terms of Use). You must keep these safe and not give or show them to any third party or allow any third party to access or use them or use the Services or the deliverables to provide a service to any third party. You shall ensure that no employee or worker keeps any copies of our Materials after ceasing to work for you.
- (e) You will pay to us and hold us harmless against all liabilities, costs, expenses, damages and losses which we suffer as a result of or in connection with any claim made against us because anything which you supply to us in connection with this Contract actually or allegedly infringes a third party’s intellectual property rights. This provision will continue to apply after the Contract has ended.
- (f) We may tell third parties that we provide, or have provided, the Services to you. You agree that we can use your name and logos for this purpose.
- (g) You acknowledge that, where we do not own any of our Materials, your use of rights in such materials is conditional on us obtaining a written licence (or sub-licence) from the relevant licensor or licensors on such terms as are acceptable to us (including in relation to any fees payable) and that will entitle us to license such rights to you.

6. Liability

- (a) We do not limit our liability in respect of any liability which by law cannot be limited or excluded (including death or personal injury caused by a party’s negligence).
- (b) We will not be liable to you (whether in contract, tort (including negligence), breach of statutory duty or otherwise (howsoever arising)) for:
 - (i) loss of profits;
 - (ii) loss of sales or business opportunities;
 - (iii) loss of agreements or contracts;
 - (iv) loss of anticipated savings;
 - (v) loss of or damage to goodwill;
 - (vi) loss of use or corruption of software, data or information; or
 - (vii) any indirect or consequential loss or damage.
- (c) Our total aggregate liability to you in connection with the Contract for any loss which arises (whether in contract, tort (including negligence), breach of statutory duty or otherwise (howsoever arising)) in any contract year is limited to 100% of our charges which are paid or due in that contract year, where “contract year” means each consecutive period of one year following the start of the Contract.
- (d) This clause 6 will continue to apply even after the Contract has ended.

7. Confidentiality

- (a) Subject to clause 7(b) and 7(c) you must:
 - (i) use our confidential information only for the purpose of allowing us to provide the Services; and
 - (ii) not reveal our confidential information to anyone else without our written permission.
- (b) You may give our confidential information to your employees, officers, representatives or advisers who need that information for the purposes of exercising your rights or carrying out your obligations under or in connection with the Contract.
- (c) You may provide our confidential information when this is required by law, or by a court or any government or regulatory authority. You may also provide our confidential information when

Terms and Conditions

the information is public knowledge (unless this is a result of unauthorised release of the information) or if you already knew it before we gave it to you.

- (d) We have the same rights and obligations to you in respect of your confidential information as those set out in clauses 7(a), 7(b) and 7(c) above.
- (e) This clause 7 will continue to apply after the Contract has ended.
- (f) For the purpose of this clause confidential information means all information of commercial value, in whatever form or medium, disclosed by the party (or any of its Affiliates) to the other party (or any of its Affiliates), including the Computer Know How, commercial or technical know-how, technology, financial information, information pertaining to business operations or structure, services and strategies, know how, unpublished information relating to intellectual property rights, and information pertaining to suppliers, customers, pricing and marketing and, for clarity, including (in the case of the Supplier's information) information relating to the Supplier software, platforms, applications or any of their constituent parts, or source code.

8. Data protection

- (a) For the purposes of the Contract, depending on the services we provide we may be the data controller, the data processor or a joint data controller.
- (b) Definitions relating to data protection are consistent with the UKGDPR and Data Protection Act 2018.
- (c) Where you are the data controller or joint data controller, you are confirming that you are acting in accordance with the obligations of a data controller as set out in applicable data protection law.
- (d) Where we are acting as a joint data controller with you, we do so to meet the obligations of the Contract.
- (e) Data shared between joint controllers shall be data pertaining to this Contract, our services and may include derived data, such as reporting.
- (f) It is your responsibility to ensure that any appropriate necessary consents are in place.
- (g) We may use anonymised data to tailor and improve our offerings to meet your requirements.
- (h) When we process personal data for the purposes of the Contract as a data processor, we will do the following
 - (i) Comply with all applicable data protection law in the United Kingdom.
 - (ii) Maintain accountability documentation in relations to agreement data
 - (iii) Do so for the purpose of meeting our obligations under the Contract, or where the law permits us to do so.
 - (iv) Act in accordance with your instructions or requests you give us about processing this personal data.
 - (v) Take appropriate organisational and technical measures to protect personal data against unauthorised or unlawful processing, and accidental loss, destruction or damage. Those measures will take account of:
 - (a) The nature of the information and the harm which could arise from such processing, loss, destruction or damage; and
 - (b) The technology available; and
 - (c) The proportionality of taking those measures.
- (i) We will not allow personal data to be transferred out of, or processed outside, the European Economic Area. Unless we have taken such measures as are necessary to ensure the transfer is compliant with all applicable data protection law.
- (j) We will not pass this personal data to any third party unless there is a legal or statutory obligation to do so, or:
 - (i) We have your permission in writing; or
 - (ii) We have entered into a written contract with that third party and they agree to meet obligations that are equivalent to those set out in this clause 8.
- (k) We will only engage sub-processors provided that:
 - (i) We maintain an up-to-date, and accessible, list of categories of sub-processors which we shall update with details of any change in categories of sub-processor at least 14 days prior to any such change. Any changes will be listed on our privacy notice which can be found at <https://www.citation.co.uk/citation-limited-privacy-information/> - consent is deemed to be given (where required) if no objection is received in writing within 14 days of updating this list.
 - (ii) We shall have a written contract in place with any sub-processors we appoint that require it to protect the data to the standard required by applicable data protection law.
- (l) We will provide reasonable and timely assistance to assist you in dealing with data protection related requests relating to the data we hold, including to respond to:
 - (i) Any request from a data subject to exercise any of its rights under applicable data protection law.
 - (ii) Not provide any information to the data subject relating to their rights without your prior written authorization.
 - (iii) Any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the data we hold
- (m) We will cooperate, with any data protection impact assessments required.
- (n) We will inform you of data breaches relating to your data without undue delay. Providing information on the nature of the breach, categories and number of affected individuals, description of likely consequences and measures we have taken to mitigate.
- (o) At the end of the Contract, we will delete personal data provided for the purpose of this Contract where we are the data processor.
- (p) We will make sure that all our personnel who need access to this personal data for the purposes of the Contract keeps to this clause 8 and have received appropriate training.
- (q) We will allow you, and at your expense, after you have given at least 30 days' notice, to enter our premises or any other location where this personal data is processed so you can make sure this

clause 8 is being met.

9. Ending the contract

- (a) You or we may end the Contract immediately, by giving written notice to the other party, if the other party does any of the following:
 - (i) materially breaches the Contract and, if the matter can be put right, fails to do so within 30 days of receiving written notice to take action;
 - (ii) if a limited company: stops trading, becomes insolvent, enters into administration, receivership, administrative receivership or liquidation, or suffers any similar situation;
 - (iii) if a sole trader or partnership: is declared bankrupt, enters into any debt-repayment arrangement with creditors (those money is owed to), has a receiver appointed over any assets, stops trading, or takes or suffers any similar situation;
 - (iv) if a sole trader or partnership: dies or becomes unable to manage financial affairs, or becomes a patient under any mental-health law.
- (b) Without limiting any other rights we have, we may suspend the Services under the Contract, or any other contract between you and us, if any of the situations in clause 3 (xvi) or clause 9(a) above arise or if you fail to pay any amount due under the Contract by the date that payment is due.
- (c) When the Contract ends for any of the reasons set out in clause 9(a) above, you must immediately pay us all amounts you owe us in connection with the Services. If we have not invoiced you for any service, monthly, quarterly, or annual invoices, we will immediately issue an invoice. You must pay that invoice as soon as you receive it. If you received free services for a period during the Contract we will add the cost of those services (calculated at their monthly rate) to the final invoice. When the Contract ends, all rights and licences you have been granted under the Contract will also end.
- (d) If you and we agree to terminate the Contract (excluding for clarity any termination under clause 9(a) then we will send you a final invoice for 75% of the fees which have not been invoiced in respect of the remainder of the Contract Period at the date that the Contract terminates. The final invoice will include a figure for any free services provided for a period during the Contract (calculated at their monthly rate).
- (e) Any rights and remedies that arose before the Contract ended will continue to apply and will not be affected by the Contract ending. Any terms and conditions that expressly or by implication survive termination of the Contract shall continue in full force an effect.

10. Events beyond your or our control

You will not be liable for failing to meet, or a delay in meeting, your obligations under the Contract if this failure is caused by an event beyond your control and we will not be liable for failing to meet, or a delay in meeting, our obligations under the Contract if this failure is caused by an event beyond our control, which in either case could not have been reasonably anticipated or avoided by the party affected by it.

11. General

- (a) **Entire agreement**
The Contract is the whole agreement between you and us. It replaces all previous agreements, promises, assurances and understandings relating to these services, as outlined in the Order Form. You agree that you have not relied on any statement, promise or assurance not set out in the Contract.
- (b) **Assignment and subcontracting**
You shall not, without our prior written consent, assign, transfer, charge, sub-contract or deal in any other manner with all or any rights or obligations under the Contract. We may at any time assign, transfer, charge, sub-contract or deal in any other manner with any of our rights or obligations under the Contract.
- (c) **Waiver**
If you or we fail to, or delay in, exercising any right or remedy under the Contract or provided by law, this will not prevent you or us from exercising that or any other right in the future. No single or partial exercise of such right or remedy will prevent or restrict any further exercise of that or any other right or remedy.
- (d) **Severance**
If any part of the Contract is or becomes illegal, invalid or cannot be enforced, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision shall be deemed deleted. Any modification or deletion of a provision will not affect the other parts of the Contract, which will continue to apply.
- (e) **Interpretation**
Any words following the terms "including", "include in particular", "For example" or any similar expression are illustrative and do not limit the sense of the words, description, definition, phrase or term preceding those terms.
- (f) **Solicitation**
 - (i) You shall not at any time during the term of the Contract or within 12 months after the last date of supply of any Services:
 - (a) solicit or entice away from us; or
 - (b) employ or attempt to employ any person who is, or has been, employed or engaged by us in the provision of the Services or attempt or authorise such action.
 - (ii) If during the term of the Contract or within 12 months after the last date of supply of any Services, you breach clause 11(f)(i), you shall pay us the greater of:
 - (a) the relevant individual's gross annual salary inclusive of all benefits at the time of their resignation or departure; and
 - (b) the equivalent of 25% of the relevant individual's new annual salary or fee inclusive of all

benefits, such sum being deemed by you and us to be reasonable, commercially justified and proportionate to protect our legitimate interests.

(g) Variation

No variation of the Contract shall be effective unless it is in writing and signed by the parties (or their authorised representatives). The process for varying the Services in an Order should be to issue and accept a replacement Order Form, such Order to constitute a variation in writing.

- (h) Any notice given under or in connection with the Contract must be in writing and be either delivered by hand or sent by first-class post to the other's registered office (if a company) or main place of business (in any other case) or by email (subject to clause (d)) as follows:
 - (i) for email notices to Citation, to the relevant email address given to You by Citation from time to time; and
 - (ii) for email notices to You, to the relevant email address given to Citation by You as part of the initial on-boarding process.
- (i) Any notice will be considered to have been received:
 - (i) if delivered by hand, at the time the notice is left at the correct address;
 - (ii) if sent by email, at the time the email was sent if sent to the correct email address;
 - (iii) if sent by first-class post, at 8:30am on the weekday after posting; and
 - (iv) if sent by a signed-for next-day delivery service, at the time the delivery notice is signed for.
- (j) This clause does not apply to any documents sent or delivered in any legal proceedings, arbitration or dispute resolution.

12. Third-party rights

No one, other than you and we, has any right to enforce all or part of the Contract.

13. Relationship

Nothing in the Contract creates a partnership or joint venture between you and us or authorises either you or us to enter into any commitments for or on behalf of the other.

14. Protection of Business Interests

- (a) In order to protect the confidential information, business relationships and connections of the Supplier to which it has access in performance of the Services, the Customer shall not and shall procure that any subsidiary or holding company of the Customer, and any subsidiary of such a holding company, shall not for the duration of the Contract and for 6 months afterwards:
 - (i) solicit or endeavour to entice away from the Supplier the business or custom of any business which has been a client or prospective client of the Supplier in the preceding 12 months, is referred to in any Confidential Information, and/or has otherwise been introduced by the Supplier to the Customer in relation to the Contract (any and all of the preceding shall be a Restricted Business);
 - (ii) approach a Restricted Business with a view to providing goods or services to them in competition with the business of the Supplier;
 - (iii) engage a Restricted Business, or approach a Restricted Business with the intention of engaging, in relation to the Services or any other activity, sale, purchase, arrangement or otherwise which is similar to the Services, without the prior written consent of the Supplier;
 - (iv) be involved with; carry on, be engaged, concerned or interested in; assist in any way; or otherwise have any business dealings with, any business concern which is in competition with business of the Supplier.

15. Governing law

The Contract and any dispute or claim arising out of or in connection with it will be governed by, and interpreted in line with, the laws of England and Wales.

16. Jurisdiction

You agree that only the courts of England and Wales can settle any dispute or claim arising out of or in connection with the Contract or service, unless we can solve the matter direct with you. Nothing in this clause limits our right to take legal action against you in any other court. Taking action in any other court does not prevent us from taking action under any other laws.

Service Schedules to the Terms and Conditions (General Terms)

All references and defined terms shall have the meaning given in the General Terms unless otherwise specified in these Service Schedules.

SCHEDULE A. CONSULTANCY SERVICES: SPECIFIC TERMS

This Services Schedule A sets out the terms and conditions applicable to consultancy Services.

1. Additional Definitions:

- (a) "PCI" means Payment Card Industry;
- (b) "PCI SSC" means Payment Card Industry Standards Security Council;
- (c) "ROC" means the report on compliance created by Supplier as part of the Services.

2. Customer's Duties:

The Customer agrees:

- (a) and acknowledges that consultants are not legally qualified, and, as such, the Customer accepts and acknowledges that, while Supplier and the consultants may give opinions and recommendations based on its industry experience and expertise, the Services and any associated Deliverables do not constitute legal advice, and the Customer is advised to seek such independent legal advice if it feels it necessary to do so.
- (b) that, where Supplier is carrying out PCI related Services for the Customer, Supplier may be obliged to disclose assessment results, including ROCs, to PCI SSC or any then current member of PCI SSC in order to verify the reliability and accuracy of its assessments;
- (c) that, where Supplier is carrying out Audit Services in respect of MasterCard or Visa, Supplier may be obliged to disclose to MasterCard or Visa evidence in support of the audit results;
- (d) nothing in the Deliverables or Services shall be deemed to be confirmation from Supplier that the Customer's operations, methodology, systems, or equipment is fully compliant with all aspects of the Data Protection Legislation and, subject to clause 8.4 in the General Terms, Supplier excludes all liability for any losses, damages, liabilities, claims or otherwise arising in relation to the Customer due to non-compliance with the Data Protection Legislation;
- (e) that other than as set out in Order Form, Supplier will not audit or otherwise test or verify the information provided to it by the Customer or on behalf of the Customer in the course of the Services. Supplier shall be entitled to rely on all information provided to it by the Customer and on the Customer's decisions and approvals in connection with the Services and to assume that all such information provided to Supplier from whatever sources is accurate, complete and not misleading;
- (f) Supplier's role is to provide the Customer with advice and recommendations for its consideration and the Customer remains solely responsible for managing all aspects of its business, for taking all decisions and operating all accounting, internal control or management information systems. This includes applying its independent business judgement to evaluate any advice or recommendations that Supplier provides. The Customer shall decide whether Supplier's advice or recommendations make sense in the context of its business, and whether it wishes to rely on, implement or act on it;
- (g) that unless provided otherwise in the Order Form, Supplier has no responsibility to update any Deliverables for events occurring after the earlier of: (1) the date the Services are completed; and (2) the date the Customer first makes use of the Deliverables;
- (h) that Supplier will not monitor the continuing relevance or suitability of the Deliverables, Services or ROCs for the Customer's purposes.
- (i) Customers are required to utilise all of their bundled penetration testing days and all products and services in packages as part of a managed service by the end of the contract. Failure to do so will result in the forfeiture of any unused days, products, and services. It is the responsibility of the customer to ensure that all days, products and services are utilised within the specified time frame.

3. Customer indemnity

to ensure that, where the Services are taking place on the Customer's premises, the premises are safe. The Customer will indemnify, keep indemnified and hold harmless Supplier in full and on demand from and against all liabilities, direct, indirect and consequential losses, damages, claims, proceedings and legal costs (on an indemnity basis), judgments and costs (including costs of enforcement) and expenses which Supplier (or its Affiliates) incurs or suffers in any way whatsoever arising out of or in connection with any claim or action against Supplier for death and/or personal injury arising out of the Customer's failure to provide safe premises.

SCHEDULE B. PENETRATION TESTING AND VULNERABILITY SCANNING (CYBER HACK) and CYBER ESSENTIALS (CYBER CERT): SPECIFIC TERMS

The Terms in this Schedule B are in addition to the General Terms and apply only to Contracts that cover the provision of Cyber Hack and Cyber Cert Services.

Cyber Hack

1. Penetration testing and vulnerability assessments will be limited to conducting an agreed set of tests on the devices, systems, infrastructure, applications and/or sites that are identified within an Order Form.
2. The Supplier's penetration testing methodology is in line with the guidance of OSSTMM and OWASP and testing is a combination of automated and manual testing, with manual testing designed to exploit any vulnerabilities identified by the automated testing. All tests look for exploitable vulnerabilities within the identified scope. Penetration tests do not include a review of the actual code of any website applications.
3. Test IP Address: The Supplier's testing is carried out on a dedicated penetration testing network, and the Supplier will supply the Customer with the relevant IP address so that the Customer can add it to any IPS/IDS or filtering system to allow testing to be completed. Log files may record ping sweeps and port sweeps from the Supplier's test IP address in addition to other activity that may be suspicious to any SEM or SIEM deployed on the systems and applications under test.
4. The Supplier's testers will take reasonable care not to cause Denial of Service (DOS) conditions or anything that would affect the performance of the systems under test, except where permitted by and agreed with the Customer.

5. The Supplier's testers will take reasonable care not to perform testing that will result in breaking any of the devices they identify nor will they attempt to exploit any vulnerability where it may reasonably be anticipated to cause damage.
6. The Supplier's testers will as soon as possible report any critical risk vulnerability that they might identify to the Customer contact.

Cyber Cert

1. The Customer is required to complete any required testing and submit the completed Cyber Essentials Questionnaire ("CEQ") within 120 days of the Order date covering the purchase of the relevant Cyber Essentials certification service. Unless there are exceptional circumstances, as reasonably determined by the Supplier, any applications not completed within that period will be marked as void; in these circumstances, the Customer agrees that they will not be entitled to any refund or reduction in the Agreed Fee.
2. The Customer is required to ensure that all vulnerability scans have been completed and submitted on the in-scope systems and infrastructure no later than seven calendar days from submitting the Cyber Essentials questionnaire to the Supplier. Failure to do so will result in a "fail" outcome and a new application will be required to reinstate the certification process before a positive outcome can be assessed.
3. The testing methodology for Cyber Essentials and Cyber Essentials Plus will be in accordance with the requirements set out by IASME Consortium.
4. The Supplier will inform the Customer where further tests are required due to a "fail" outcome of the assessment, or in the event that the questionnaire does not meet the scope. These tests will be subject to agreement with the Customer and will be billed separately.
5. The Supplier's testers are all qualified to the level that IASME deems appropriate for carrying out assessments.
6. Unless otherwise agreed, the Supplier reserves the right to list the Customer's company name on its website upon achieving certification.
- 7.

Terms applicable to both Cyber Hack and Cyber Cert

1. Limitations on the testing, such as a requirement for out-of-hours testing or weekend testing, or restrictions such as testing only during office hours should be stipulated at the time of submitting an Order and may be subject to additional Charges. Unless included in the Order Form the Supplier shall not be required to comply with such limitations when performing the Services.
2. Logs are kept of the actions taken during a test and, in line with the Supplier's data retention procedure, these are retained, along with all other Customer files, for six years and are then destroyed. Customer files will be encrypted, classified as restricted to the testing consultant and to senior management of Citation Cyber, stored on a restricted network drive, and will be backed up in their encrypted form to the Supplier's mirrored, secure off-site backup environment. Within the overall context of the Citation Cyber ISO27001 certification, these controls directly protect the Customer's data from disclosure, damage and information leakage.
3. The Supplier will not:
 - (a) disclose test results or related information to third parties without the Customer's prior permission, unless otherwise required by law;
 - (b) allow anyone, other than on a need-to-know basis, access to the Customer's test information;
 - (c) exchange information in relation to the tests and test results other than by using encrypted email.
4. The Supplier will only identify vulnerabilities that are already known at the date on which any tests are carried out, and which are capable of being exposed by the range of testing tools deployed by the Supplier. The Customer accepts that it is in the nature of technical security testing that there may be flaws that will be uncovered in the future or by the use of alternative tools and attack methodologies, none of which could normally be identified at the time of testing, and therefore the Supplier excludes all liability relating to any such flaws not identified during testing, other than unidentifiable flaws and related matters. That while the results of this test will provide a reasonably accurate view of the current security level of the tested computer system(s), The Supplier cannot be held responsible if the Penetration Test or Cyber Essentials Test fails to discover certain security or configuration issues on the target computer system(s).
5. The Customer agrees:
 - (a) to provide authorisation in writing, and where applicable obtain consent from its ISP and any third party suppliers of the system, for the Services to be carried out and, when and in the manner requested by the Supplier, to provide written evidence of such consent and to notify relevant employees that the services are to be carried out and that they may be monitored;
 - (b) that it shall properly and fully back-up all data and copies of all computer programs and data which are held immediately prior to commencement of the services, and which may be affected by the provision of the services and, where appropriate, regularly make back-ups during the performance of the services, to enable straightforward recovery and/or reinstatement of any and all data and/or computer programs lost or damaged (whether in whole or part) through performance of the services;
 - (c) that, whilst The Supplier will conduct all services in line with accepted best practice and use reasonable endeavours to avoid disruption of the Customer's network, the tools and techniques used may cause disruption to the Customer's systems, software and/or possible loss of or corruption to data and/or software, and the Customer agrees to provide such redundant systems as are prudent in the circumstances, and further ensure all relevant data and systems are backed up to the fullest extent;
 - (d) to notify The Supplier in writing in advance or as soon as possible after becoming aware if there are any periods during which the services are due to be or are being performed when The Supplier should not perform the services or should cease performing the services due to critical business processes (such as batch runs) or if any part of the system or any attached systems, data or software is business critical so that The Supplier can, if needs be and with the Customer's consent, modify its testing approach;
 - (e) The Customer will respond in a normal fashion when it detects the tests in its firewall logs, alert systems, etc. as it would do in case of a real security penetration; in order not to distort the results of the test. However,

the Customer agrees not to notify legal or public authorities of this penetration;

- (f) to use any software and/or hardware which the Supplier uses or makes available to the Customer as part of the Services, only for lawful purposes, solely to the extent necessary to receive the benefit of the Services and in accordance with any applicable licence terms and The Supplier's instructions provided from time to time;
 - (g) to ensure there is sufficient bandwidth to enable The Supplier to perform the services.
6. The Supplier shall accept no liability for damages, whether past, present or future, caused to the Customer by any automated or non-automated attacks on the Customer's internet-facing infrastructure or its applications, irrespective of whether or not the Supplier's security testing activity carried out under the Contract did, did not, or could have but did not, identify any vulnerability exploited or which might in future be exploited by any such attack.
 7. The Supplier will identify vulnerabilities that its testing has exposed; wherever possible, it will identify by reference to commonly available and published information the appropriate patches and fixes that are recommended to deal with the identified vulnerability but it will be entirely the Customer's responsibility to formally identify and deploy an appropriate solution to the vulnerabilities identified by the Supplier's security testing.
 8. **Customer Indemnity:** Customer shall assume all liability and shall indemnify, keep indemnified and hold harmless the Supplier, its officers, employees, agents, contractors and sub-contractors in full and on demand from and against any and all third party claims (including, but not limited to, claims for alleged or actual infringement of Intellectual Property Rights), losses, damages, demands, costs, expenses, charges (including, but not limited to, court and legal Charges) and liabilities (in each case whether direct, indirect or consequential) of whatever nature, arising in relation to the provision of these testing Services, save to the extent that any such losses, damages, demands, costs, expenses, charges or liabilities are incurred as a direct result of The Supplier's breach of the terms of this Schedule B.

SCHEDULE C. IN-HOUSE TRAINING: SPECIFIC TERMS

1. The Terms in this Schedule C are in addition to the General Terms and apply only to Contracts that cover the provision of in-house training services.
2. The Customer agrees to provide:
 - (a) a venue that is appropriate for the number of people attending;
 - (b) a PowerPoint projector and screen;
 - (c) two flip charts with pens; and
 - (d) tea, coffee and lunch for the delegates and the Supplier's trainer.
3. Apply once the Supplier has accepted an Order from the Customer for delivery of a training course.
4. Places on in-house training courses cannot be sold on to other organisations, unless this has been specifically agreed by the Supplier in advance in writing.
5. The Supplier reserves the right to deliver any training services at distance and remotely using an appropriate online video conferencing or web communications platform, to be designated by the Supplier at that time.

Force Majeure

1. The Supplier reserves the right to postpone and reschedule a training course or service at any time and with no liability to the Customer, if due to a force majeure event and in accordance with clause 12.1 of the General Terms.

Additional Delegates

2. The training course will be agreed at the time of booking for a maximum number of delegates. If the Customer wishes to exceed this number, this must be agreed in advance and in writing with the Supplier, and additional Charges/course costs may have to be paid in advance of the course taking place.
3. If additional, unscheduled delegates attend on the day, the Supplier does not guarantee that they will be able to attend and reserves the right to refuse access to the training. If the Supplier chooses to allow the delegate to attend, the Supplier will levy an additional charge of 120% of the agreed course charge per additional delegate.

Delegate Background

1. The Customer is responsible for ensuring that the backgrounds of its delegates is suitable for the training course they are attending. The Supplier will not be liable for any refund if delegates decide that the course material is inappropriate for them or if they are unable to participate fully for any reason.
2. The Customer will ensure that all delegates have additional time set aside in relation to any pre-course reading material that may be provided in relation to the course they are attending, depending on its topic and duration.

Course Materials

1. Course materials may not be used, copied, reproduced, stored in a retrieval system, distributed or transmitted in whole or in part or in any form or by any means, whether electronically, mechanically, or otherwise, or translated into any language, without the Supplier's prior written permission.

Service Schedules to the Terms and conditions (General Terms)

SCHEDULE D. CITATION CYBER HUB SERVICES

1. Interpretation

1.1 The definitions and rules of interpretation in this clause apply in this Schedule E.

Authorised Users: those employees, agents and independent contractors of the Customer who are authorised by the Customer to use the Services and the Documentation, as further described in the Order Form.

Customer Data: the data inputted by the Customer, Authorised Users, or the Supplier on the Customer's behalf for the purpose of using the Services or facilitating the Customer's use of the Services.

Documentation: the document made available to the Customer by the Supplier online via Cyber learn or such other web address notified by the Supplier to the Customer from time to time which sets out a description of the Services and the user instructions for the Services.

Effective Date: the date of the Order.

Citation Cyber Hub: The hub located at <http://opp.mitigatehub.com/>, operated and provided by the Supplier, in which the Services are provided.

Citation Cyber Hub Licence: The end user licence governing the access to and use of Citation Cyber Hub and the Services in Cyber learn, which applies to all Authorised Users.

Phishing Portal Services means the provision of Supplier's web-based facility included in Citation Cyber Hub through which the Customer uses a phishing attack simulation tool to send emails simulating a phishing attack to its employees and view certain data in respect of such simulated attack;

"Phishing Portal" refers to the Simulated Phishing feature on Citation Cyber Hub;

Services: the Cyber learn subscription services and Software, agreed to be provided by the Supplier to the Customer in the Order Form, and in accordance with this Schedule D and accessed via Citation Cyber Hub, consisting of any or all of: Cyber learn – E learning; Phishing Portal Services (Schedule D); Cyber comply – Compliance / policy management; Cyber hack – Penetration Test reports, schedule and vulnerability scanning; Cyber cert – Cyber essentials online questionnaire; Cyber intel – breach notification & threat intelligence tool; Cyber sure – Insurance documents upload; and as may be more particularly described in the Order Form.

Software: the online software applications provided by the Supplier as part of the Services.

Support Services Policy: the Supplier's policy for providing support in relation to the Services as made available at Citation Cyber Hub which are available on a ticket basis.

User Subscriptions: the user subscriptions purchased by the Customer which entitle Authorised Users to access and use the Services and the Documentation in accordance with this agreement.

Virus: any thing or device (including any software, code, file or programme) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any programme or data, including the reliability of any programme or data (whether by re-arranging, altering or erasing the programme or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.

Vulnerability: a weakness in the computational logic (for example, code) found in software and hardware components that when exploited, results in a negative impact to the confidentiality, integrity, or availability, and the term Vulnerabilities shall be construed accordingly.

2. User subscriptions

- 2.1 Subject to the Customer purchasing the User Subscriptions in accordance with clause 3.2, the restrictions set out in this clause 2 and the other terms and conditions of this agreement, the Supplier hereby grants to the Customer a non-exclusive, non-transferable right, without the right to grant sublicenses, to permit the Authorised Users to use the Services and the Documentation during the Order Term solely for the Customer's internal business operations.
- 2.2 In relation to the Authorised Users, the Customer undertakes that:
 - (a) the maximum number of Authorised Users that it authorises to access and use the Services shall not exceed the number set out in the Order Form or has otherwise purchased from time to time;
 - (b) it will not allow or suffer any User Subscription to be used by more than one individual Authorised User at a time;
 - (c) each Authorised User shall keep a secure password for his use of the Services, and that each Authorised User shall keep his password confidential;
 - (d) it shall permit, on reasonable notice, the Supplier or the Supplier's designated auditor to audit the Services in order to establish the number, name and password of each Authorised User and otherwise audit compliance with this Schedule D.
 - (e) if any of the audits referred to in clause 2.2(d) reveal that the Customer has underpaid Charges to the Supplier, then without prejudice to the Supplier's other rights, the Customer shall pay to the Supplier an amount equal to such underpayment as calculated in accordance with the prices set out in the Order Form within 10 Business Days of the date of the relevant audit;
- 2.3 The Customer shall not access, store, distribute or transmit any material during the course of its use of the Services that is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive; facilitates illegal activity; depicts sexually explicit images; promotes unlawful violence; is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or is otherwise illegal or causes damage or injury to any person or property
- 2.4 The Customer shall not:
 - (a) except as may be allowed by any applicable law which is incapable of exclusion by agreement between the parties and except to the extent expressly permitted under the Contract:
 - (i) attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Software and/or Documentation (as applicable) in any form or media or by any means; or

- (ii) attempt to de-compile, reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Software; or
 - (b) access all or any part of the Services and Documentation in order to build a product or service which competes with the Services and/or the Documentation; or
 - (c) use the Services and/or Documentation to provide services to third parties; or
 - (d) license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Services and/or Documentation available to any third party except the Authorised Users, or
 - (e) attempt to obtain, or assist third parties in obtaining, access to the Services and/or Documentation, other than as provided under this clause 2; or
 - (f) introduce or permit the introduction of, any Virus or Vulnerability into the Supplier's network and information systems.
- 2.5 The Customer shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Services and/or the Documentation and, in the event of any such unauthorised access or use, promptly notify the Supplier.
- 2.6 The rights provided under this clause 2 are granted to the Customer only, and shall not be considered granted to any subsidiary or holding company of the Customer unless specified in the Order Form.
- 2.7 The Supplier reserves the right to suspend the Services and/or User Subscription(s) if it reasonably believes there is a breach of the requirements of this clause 2.

3. Additional user subscriptions

- 3.1 Subject to clause 3.1 and clause 3.2, the Customer may, from time to time during any Order Term, purchase additional User Subscriptions in excess of the number set out in Order Form by following the request process in Citation Cyber Hub. If the request and order is accepted, the Supplier shall activate the additional User Subscriptions as soon as reasonably possible.
- 3.2 The relevant Charges for additional User Subscriptions shall be confirmed at point of order in Citation Cyber Hub. Customer shall pay to the Supplier the relevant Charges either at the point of Order by debit card, by direct debit if established, or by BACS on receipt of an invoice, all as confirmed at the time of Order by the Supplier. If such additional User Subscriptions are purchased part way through the Order Term or any Renewal Term (as applicable), such Charges may be applied pro-rata from the date of activation by the Supplier for the remainder of the Order Term or then current Renewal Term, as applicable and determined by the Supplier. On confirmation of the Order, the additional User Subscriptions shall form part of the Contract under the relevant Order Form covering Citation Cyber Hub Services.

4. Services

- 4.1 The Supplier shall use commercially reasonable endeavours to make the Services available on an uptime basis of the Citation Cyber Hub of 99.5%, based on 24 hours a day, seven days a week, except for:
 - (a) planned maintenance carried out during the maintenance window of 7 pm to 7 am UK time; and
 - (b) unscheduled maintenance performed outside Business Hours, provided the Supplier has used reasonable endeavours to give the Customer at least 6 Normal Business Hours' notice in advance.
- 4.2 The Supplier will, as part of the Services and at no additional cost to the Customer provide the Customer with the Supplier's standard customer support services during Business Hours in accordance with the Supplier's Support Services Policy in effect at the time that the Services are provided. The Supplier may amend the Support Services Policy in its sole and absolute discretion from time to time.
- 4.3 If specified in the Order Form the Supplier will, and to which the Customer hereby consents and licenses the Supplier to:
 - (a) provide a single session of training for one or more administrators nominated by the Customer (the "Training") to enable the Customer to administer the Services in Citation Cyber Hub;
 - (b) provide basic customisation of the Services using the customer's corporate branding;
 - (c) basic customisation of the Services and Documentation, limited to company logos and references, and links to appropriate customer policies.

5. Customer data

- 5.1 The Customer shall own all right, title and interest in and to all of the Customer Data that is not personal data and shall have sole responsibility for the legality, reliability, integrity, accuracy and quality of all such Customer Data.
- 5.2 The Supplier will make backups, once per day, of all Customer Data in Citation Cyber Hub. The Supplier will retain these backups for no longer than 60 days. The Supplier will provide an electronic copy of the backup to the Customer upon written (email) request by an officer of the Customer organisation. There may be an additional charge if the Customer asks the Supplier to do this more than once per year. The Supplier does not keep regular snapshots of progress through courses by individual Authorised Users, and the Supplier will not necessarily keep backups of all reports that the Customer might create for itself.
- 5.3 In the event of any loss or damage to Customer Data, the Customer's sole and exclusive remedy against the Supplier shall be for the Supplier to use reasonable commercial endeavours to restore the lost or damaged Customer Data from the latest back-up of such Customer Data maintained by the Supplier in accordance with the archiving procedure described in clause 5.3. The Supplier shall not be responsible for any loss, destruction, alteration or disclosure of Customer Data caused by any third party (except those third parties sub-contracted by the Supplier to perform services related to Customer Data maintenance and back-up for which it shall remain fully liable.
- 5.4 Both parties will comply with all applicable requirements of the Data Protection Legislation. Appendix A to the General Terms which will apply in the event the Supplier processes any personal data on the Customer's behalf when performing the Services.

6. Supplier's obligations

- 6.1 The Supplier:
 - (a) does not warrant that:

- (i) the Customer's use of the Services will be uninterrupted or error-free; or
 - (ii) the Software or the Services will be free from Vulnerabilities.

- 6.2 is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Customer acknowledges that the Services and Documentation may be subject to limitations, delays and other problems inherent in the use of such communications facilities.

7. Customer's obligations

- 7.1 The Customer shall:
 - (a) ensure that the Authorised Users use the Services and the Documentation in accordance with is Schedule D and Citation Cyber Hub Licence, and shall be responsible for any Authorised User's breach of the same;
 - (b) ensure that its network and systems comply with the relevant specifications provided by the Supplier from time to time;
 - (c) be, to the extent permitted by law and except as otherwise expressly provided in this agreement, solely responsible for procuring, maintaining and securing its network connections and telecommunications links from its systems to the Supplier's data; and centres, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Customer's network connections or telecommunications links or caused by the internet.
- 7.2 The Customer shall, in relation to the receipt of Portal Phishing Services:
 - (a) ensure at least one employee shall act as liaison between the Customer and Supplier and shall respond promptly to queries and requests for information;
 - (b) not exceed any maximum usage levels set out in the Order Form or otherwise agreed in writing between Customer and Supplier from time to time;
 - (c) input only the work email addresses of Customer's own employees into the Phishing Portal and to ensure that all addresses are accurate.

8. Customer indemnity:

Customer shall assume all liability and shall indemnify, keep indemnified and hold harmless the Supplier, its officers, employees, agents, contractors and sub-contractors in full and on demand from and against any and all third party claims (including, but not limited to, claims for alleged or actual infringement of Intellectual Property Rights), losses, damages, demands, costs, expenses, charges (including, but not limited to, court and legal Charges) and liabilities (in each case whether direct, indirect or consequential) of whatever nature, arising in relation to the provision of these testing Services, save to the extent that any such losses, damages, demands, costs, expenses, charges or liabilities are incurred as a direct result of The Supplier's breach of the terms of this Schedule D.