Schedule 2
Product details/specifications & Services

2 Program Documentation

2.1 The riskHive ERM tool is a highly configurable Commercial-off-the-shelf (COTS) end-to-end risk management system that quickly and effectively imports, consolidates and maintains your existing risk registers in a secure risk portfolio database. It can be configured to support the import and assimilation of the excel risk registers you currently use, saving time on data migration.

2.2 The ERM system has the following inherent ability:

a) Management and tracking of the following elements with custom views and data:
   i. Multiple configurable risk scenarios: e.g., Inherent, Current, Target and Residual
   ii. Multiple object types: e.g., Risks (Threats), Opportunities, Issues, Assumptions, Uncertainties and Actions

b) Support for different risk assessment methodologies (e.g., for cyber risk or business risk or project risk) by accommodating discrete relevant scoring, metadata and drop-down selection options for specific risk or activity types.

c) Support for recording, assessment and evaluation of existing control activities to evaluate 'current residual' risk and enable dynamic risk management i.e., what is the impact of a control failure on the identified risks, by both graphical and data-based methodologies.

d) Comparison to multiple risk appetites (for difference impact classifications) to determine whether further mitigating actions are required, by heatmap.

e) To monitor and score the progress and effectiveness of identified actions to manage risks and provide a per-user / owner dashboard showing which actions are:
late, unsuccessful, need assistance, not started, not completed, in-progress, etc.

f) To monitor the effectiveness of existing controls (through second line assurance and third line audit testing) by supporting feedback data entry from audit.

g) The system will support any approach to risk management in compliance with recognised frameworks and be able to report on risks and controls in an integrated way.

h) System risk status colours are linked to appetites through heatmap settings and extend through to the graphical risk visualisation tools such as the risk Bow-Tie interfaces, Risk Radars, PID Heatmaps and Gannt-style devices.

2.3 SaaS Services

2.3.1 Software as a Service description applies to commercial terms on which access to the software is provided on an annual fee basis, payable in advance, where the capital license term fee and annual maintenance and support fee are rolled into one common reduced payment designed to spread the cost of ownership equally over annual periods. SaaS provision included hosting for Pilot and Project sized systems on a shared server. Enterprise Unlimited or enhanced security systems must be hosted on a dedicated server.

2.3.2 The licenced ERM solution described in Schedule1 is delivered as a service by means of a fully hosted software application that is accessed over the internet by a web browser device. The service requires an active internet connection and may be accessed using any web browser application including but not limited to:

a) MS Edge Browser,
b) Google Chrome,
c) Mozilla Firefox,
d) Apple Safari

There are no client-side download, ActiveX, native app or browser add-in requirements.

2.4 Availability & Performance

2.4.1 The SaaS Service will be available to the internet 99.5% of 24hours x 365 days per annum with the exception of planned maintenance activities (including patches / upgrades). Planned system outages will be notified and agreed with Customer in advance. Failure of client terminal devices, internet access or any other impediment are excepted, System will be deemed to be compliant when the administrator can login to the application, all related services / daemons start, and the application(s) have external network connectivity. riskHive use the 'uptimerobot' web application to monitor availability in real time and to provide a client-accessible dashboard to evidence records of system uptime.

2.4.2 The hosting has been specified by riskHive and will be performant to the above service levels, the capacity licensed under this Agreement and the performance contained in the Appendix. This capacity and performance are included within the charges contained in Schedule 1 to meet the needs of Customer for the duration of the Agreement. The server and Services will meet the security requirements contained in the Appendix.

2.4.3 The Service Levels shall include that the Saas Service will provide Application with a suitable response time to allow a user to use the Application without degradation in performance that it can reasonably expect. riskHive will perform a network latency test with the user and determine if this is a network issue or an application issue. Action taken would be taken accordingly to restore performance of the Application in accordance with the Service Levels and response if it is found to be an application issue.

2.4.4 In the event of a DR/BCP event (including force majeure) service recovery of the Saas service, riskHive will swap to another virtual machine or another server in our dedicated rack space and restore the latest whole backup of the data and application configuration in accordance with its DR/BCP location and/or plan. The target time for this is 12 hours or less.

2.5 Services

2.5.1 ERM has the ability to email users with relevant information regarding their role within the system. This service is provided as an integral part of the overall ERM service provision.

2.5.2 riskHive and its clients enjoy a mutually beneficial relationship where Customer may request feature and functionality changes to the riskHive product and riskHive caries out these services as part of its product road map development plan within the costs of the services and fees contained in Schedule 2. It is estimated an additional ERM customisation work of between 10-30 days per year may be carried out FoC for the Customer in addition to the support and maintenance activities.

2.5.3 RiskHive at its own discretion may provide SME services FoC in support of the successful implementation of the ERM solution.

2.5.4 In the case that the above conditions cannot be met and where riskHive is genuinely unable to carry out the work 'gratis' it may agree with the Customer a separate statement of work to develop such functionality.

2.6 Data Management Services

2.6.1 "**Customer Data**" means all data, information, text, drawings, statistics, analysis, forms, data base entries, flow charts and other materials embodied in any form (physical or electronic) relating to the Customer or any member of the customer's group (and/or their respective contractors, customers, partners or joint ventures) generates, collects, processes, stores or transmits in connection with the Services, this Agreement and each statement of work;

2.6.2 riskHive shall ensure that a backup copy of the Customer Data is made at least once in any [twenty-four (24) hour period] and that such copy is recorded on media from which the Customer Data can be easily read, retrieved and re loaded and it shall comply with the requirements contained in Schedule 4: Data Management.

2.6.3 If at any time any incident occurs which may adversely affect the Services, the Customer Data or the Customer's reputation, then riskHive shall notify the Customer and provide the Customer with details of the remedial action it proposes to take, including details of how riskHive will ensure such event does not occur in respect of, and/or there is no impact on, the Customer Data.

Schedule 3
Support & Maintenance
Updates & Upgrades

Definitions:

- **Support**:
  After-sales service provided by riskHive in solving software conflicts and usability problems and also supplying updates and patches for bugs and security vulnerabilities in the program.
- **Maintenance**:
  the modification of the software product after delivery to correct faults, to improve performance or other attributes as may be required that are not related to system functional development.
- **Upgrades & Updates**:
  Customer shall be entitled to the new product version upgrades and updates as contained in the riskHive product roadmap as contained in the Appendix to this Agreement. The Customer and riskHive may develop new features and functionality to improve the riskHive product that is included as part of the Services under this Agreement. riskHive will maintain the current and one version previous of the software. The previous version will be maintained for 6 months after the release of the latest version.

3.0 Support / Maintenance Request Handling details

1.1 Two levels of support are provided as standard for the solution support:

3.1.1 Front line support:

24/7 Instant online access to System User, System Administration Manual and Videos. This feature allows users to access an online knowledge base. This can be instrumental in reducing the number of requests that appear at first-line support and allowing the user to move on quickly.

3.1.2 Second-line user support

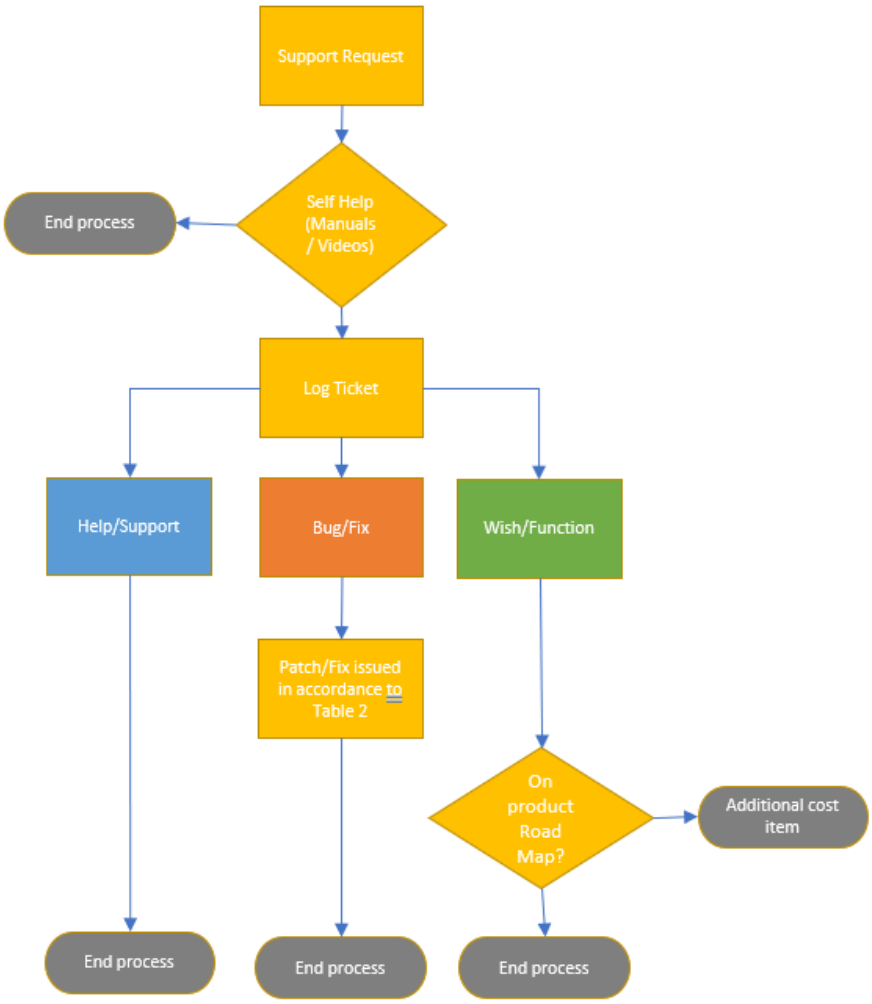
a) This is provided during business hours by experienced members of the riskHive technical team, which may be any one of the following, as appropriate for the nature of the support query:

I. a dedicated support person,
II. an implementation consultant,
III. a technical coach or
IV. an application developer.

3.2 Second line support shall be provided on UK working days between 0900 and 1730 in English with response times as per Table 1.

Table 1 – Response Times	Table 2 – Software issue patches and fixes
50% of tickets being responded to immediately (within 60 minutes)	Critical / Security related issue – 5 working days or less
80% of tickets being responded to quickly (within 4 hours)	Significant functional issue – 10 working days or less
95% of tickets being responded to within 8 hours	Noticeable functional issue – 30 working days or less
99.5of tickets being responded to within 24 hours	

3.3 Support Request Process



- Front line support is accessible via the 24/7 online User and Administration Manuals and 'How to Videos'.
- If the online knowledge base does not hold the answers expected the user should email support@riskhive.com
- Once an email is received, riskHive will raise a ticket in Azure DevOps, responding according to the times outlined in Table 1.
- Once the request has been actioned, the ticket will be closed.

Patch/Fixes

- Where patches/fixes are determined, these will be actioned in accordance to Table 2.

Wish/Function

- Where a wish or function ticket type is raised, this will be considered if a Change Request is required.
- The type of request may result in a change to the current system, a change programmed into our Road Map or not accepted.

3.6 System / Data Backups

Secure regular automated system backup and separate regular automated system configuration and data backup capability are standard features. Daily backups of system configuration and data are made at a configured time and stored locally on the server and may be sent by secure FTP to a remote server of the client's specification. The ERM solution supports full restore of system configuration and data from any version-compatible backup in <5 minutes from start of process.

3.7 Additional Services Rate Card

Customer may request riskHive to provide additional services over and above those contracted for in this agreement may be required. In such cases the following rate card shall apply and be invoked by means of separate contract extension. No additional work that is subject to this rate card shall be carried out without written authorization or a valid purchase order from Customer. No work shall be accrued without the express permission and authorization of Customer procurement by means of a properly numbered Purchase Order and no unauthorized invoice shall be issued against unauthorized work.

Service Type	Notes	Service Fee	Unit
Set-up and config support	New system set-up nominally comprises 3 days' configuration support and 2 days' ad min / user training		One-off
DBA Support Service	Outsource ERM database administration and management with direct system admin function support (6 days / month)		Monthly
SME Support Service	Active Expert risk register and portfolio review and advisory services on-demand by SME (24 hrs/pcm)		Monthly
General Risk Consulting	System or risk consulting not related to application-user support issues		Day-rate
Additional training	System (user, administrator) and Subject (Risk management, risk analysis, etc). Minimum 5 delegates		Per-user per course
Customise / Develop App	Development or customisation of ERM application or stub-feature. Includes design and PM support		Per day

Schedule 4

4.0 Data Management

4.1 riskHive acknowledges and agrees that the in relation to Customer Data:

a) it is the property of the Customer, and the Customer reserves all Intellectual Property Rights which may, at any time, subsist in the Customer Data.

b) riskHive shall only store, copy or use the Customer Data to the extent necessary to perform its obligations under this Agreement and each statement of work and shall not disclose it to any third party without the prior written approval of the Customer;

c) if at any time riskHive suspects or believes that the Customer Data has or may become lost or corrupted in any way for any reason then riskHive shall immediately notify the Customer and inform the Customer of what remedial action it proposes to take.

d) ensure that the Customer Data is kept segregated and secure and not capable of being accessed by a third party (other than the riskHive's sub-contractors and personnel properly authorised to access such data in order to support the performance of the Services);

e) merge or combine the Customer Data with other data or remove any of the Customers' proprietary notices.

4.2 If riskHive has failed to comply with a with this section and any its obligations to Customer Data (in Schedule 4), the Customer may, on reasonable notice, attend the Supplier's (or that of its contractors) premises to supervise with the Supplier's staff who will retrieve such applicable the Customer Data on the Customer's behalf from the Supplier's premises, equipment, system, hardware, software or other facilities. In carrying this out, the Supplier shall provide such assistance as the Customer reasonably requires enabling the Customer to exercise this right.

Schedule 5

5 Data Protection/Processing

This Data Processing Addendum (DPA) is made between riskHive Software Solutions Ltd ("Provider") and ("Customer") and applies to the Processing of Personal Data by Provider on behalf of Customer (Customer Personal Data) in order to provide the Services under this Agreement.

5.0 Personal Data Processing

5.1 Roles of the Parties. The parties acknowledge and agree that regarding the Processing of Personal Data, Customer is the Controller, Provider is the Processor and that Provider will engage Sub-processors pursuant to the requirements set forth in this agreement.

5.2 Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

5.3 Provider's Processing of Personal Data. Provider shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes:

a) processing in accordance with this agreement and applicable supplements;

b) processing initiated by Users in their use of the Services;

c) and processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

5.4 Details of the Processing.

a) The subject-matter of Processing of Personal Data by Provider is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 4 (Details of the Processing) to this DPA.

5.5 Subprocessors Authorization.

a) Customer authorizes Provider to engage subcontractors ("Subprocessors") to process Customer Personal Data. A list of the current Subprocessors is set out in the appropriate exhibit to this agreement.

5.6 Notification of Changes.

a) Provider shall notify Customer in advance of any changes to the list of Subprocessors as set out in that exhibit.

5.7 Customer Objection.

a) Within 30 days after Provider's notification of the intended change, Customer can object to the addition of a Subprocessor on the basis that such addition would cause Customer to violate applicable legal requirements. Customer's objection must be in writing and include any specific reasons for its objection and options to mitigate. If Customer does not object within such period, the Subprocessor may be commissioned to Process Customer Personal Data.

5.8 Right to Terminate.

a) If Customer legitimately objects to the addition of a Subprocessor and Provider cannot reasonably accommodate Customer's objection, Provider shall notify Customer. Customer may, in that case, terminate the affected Services by giving Provider written notice within one month of Provider's notice. Provider shall refund a prorated portion of any pre-paid charges for the period after that termination date.

5.9 Subprocessor Obligations.

a) Provider shall impose substantially similar data protection obligations as set out in this agreement on any approved Subprocessor before the Subprocessor begins processing any Customer Personal Data.

5.10 Personnel Processing Data

a) Confidentiality. Data Processor shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities. Data Processor shall ensure that such confidentiality obligations survive the termination of the Data Processor of the personnel processing data.

5.11 Limitation of Access.

a) Data Processor shall ensure that Data Processor's access to Personal Data is limited to personnel performing Services in accordance with the agreement.

5.12 Data Protection Officer.

a) Data Processor will appoint a data protection officer. The appointed person may be reached at info@riskhive.com

5.13 Data Security.

a) Data Processor shall maintain administrative, physical and technical safeguards designed for the protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data. Data Processor will not materially decrease the overall security of the Services during a subscription term.

5.14 Technical and Organizational Measures

a) Security Measures. Data Processor has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Data, including the measures specified in this Section to the extent applicable to Data Processor's Processing of Personal Data. These measures are intended to protect Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure or access, and against all other unlawful forms of Processing. Additional measures, and information concerning such measures, including the specific security measures and practices for the particular Cloud Services ordered by Customer, may be specified in the Agreement.

5.15 Physical Access Control.

a) Data Processor employs measures designed to prevent unauthorized persons from gaining access to data processing systems in which Personal Data is Processed, such as the use of security personnel, secured buildings and data centre premises.

5.16 System Access Control.

a) The following may, among other controls, be applied depending upon the particular Cloud Services ordered: authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes, and logging of access on several levels. For Cloud Services hosted at Data Processor: (i) logins to Cloud Services Environments by Data Processor employees and Third Party

b) Subprocessors are logged; (ii) logical access to the data centres is restricted and protected by firewall/VLAN; and (iii) intrusion detection systems, centralized logging and alerting, and firewalls are used.

c) Data Access Control. Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted, and application access rights are established and enforced.

5.17 Transmission Control.

a) Except as otherwise specified for the Cloud Services (including within the Data Processor Cloud Order or the applicable

service specifications referenced in the Agreement), transmissions of data outside the Cloud Service environment are encrypted.

5.18 Input Control.

a) The Personal Data source is under the control of the Customer, and Personal Data integration into the system, is managed by secured file transfer (i.e., via web services or entered into the application) from the Customer.

5.19 Data Backup.

a) For Cloud Services hosted at Data Processor: back-ups are taken on a regular basis; backups are secured using a combination of technical and physical controls, depending on the particular Services,

5.20 Data Segregation.

a) Personal Data from different Data Processor customers' environments is logically segregated on Data Processors systems.

5.21 Confidentiality.

a) All Data Processor employees and Third Party Subprocessors that may have access to Personal Data are subject to appropriate confidentiality arrangements.

b) Data Subject Rights and Requests

c) Obligation to Notify. Provider will, to the extent permitted by law, inform Customer of requests from Data Subjects exercising their Data Subject rights (e.g., rectification, deletion and blocking of data) addressed directly to Provider regarding Client Personal Data.

d) Responses to Data Subjects. Customer shall be responsible for responding to such requests from Data Subjects. Provider will reasonably assist Client in responding such Data Subject requests.

e) Indemnification by Customer. If a Data Subject brings a claim directly against Provider for a violation of their Data Subject rights, Customer will indemnify Provider for any cost, charge, damages, expenses or loss arising from such a claim to the extent that Provider has notified Customer about the claim and given Customer the opportunity to cooperate with Provider in the defence and settlement of the claim.

f) Claims by Customer, Subject to the terms of the Agreement, Customer may claim from Provider amounts paid to a Data Subject for a violation of their Data Subject rights caused by Provider's breach of its obligations under GDPR Data Breach. In the event of any unauthorized access or theft of Customer data, Provider shall promptly notify Customer and do all such acts and things as Customer considers reasonably necessary to remedy or mitigate the effects of the data breach. The parties shall coordinate and cooperate in good faith on developing the content of any related public statements or any required notices.

Definitions

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity.

"Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Authorized Affiliate" means any of Customer's Affiliate (s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Provider but has not signed its own order and is not a "Customer" as defined under the Agreement.

"Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

"Data Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
"Data Protection Law" means applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement.

"Data Subject" means an identified or identifiable natural person.
'I EEA" means the European Economic Area, namely the European Union Member States along with Iceland, Lichtenstein and Norway.

"European Subprocessor" means a Subprocessor that is physically processing Personal Data in the EEA or Switzerland.

"Personal Data" means any information relating to a Data Subject. For the purposes of this DPA, it includes only personal data entered by Customer or its Authorized Users into or derived from their use of the Cloud Service. It also includes personal data supplied to or accessed by the Provider or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Security Breach" means a confirmed (1) accidental or unlawful destruction, loss, alteration, or disclosure of Customer Personal Data or Confidential Data, or (2) similar incident involving Personal Data for which a Data Processor is required under applicable law to provide notice to the Data Controller.

"Standard Contractual Clauses" also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof released by the Commission (which will automatically apply). The current Standard Contractual Clauses are located at http://ec.europa.eu/justice/data-protection/internationaltransfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc.

"Subprocessor" means an Affiliate of the Provider and third parties engaged by the Provider of its Affiliates to process personal data.
"Third Country Subprocessor" means any Subprocessor incorporated outside the EEA and outside any country for which the European Commission has published an adequacy decision as published at http://ec.europa.eu/justice/data protection/international-transfers/adequacy/index en.htm.

List of Subprocessors:

1) Role: Hosting partner
   Organisation: Microsoft Azure UK. Microsoft Campus, Thames Valley Park, Reading, RG6 1WG
   Website: https://www.microsoft.com/en-gb/
   Certifications: ISO 9001; 20001; 27001; 27017; 27018; 27701; CSA STAR; SOC 1-2-3; WCAG