



# Supplier Terms and Conditions

for the provision of FortisOne GRC by Cyberfortis

G-Cloud15 · Framework Reference RM1557.15

**Complex risk. Clear control.**  
**[fortisonegrc.com](https://fortisonegrc.com)**



## CYBERFORTIS CONSULTING LIMITED

FortisOne GRC by Cyberfortis

---

# Supplier Terms and Conditions

for the provision of FortisOne GRC by Cyberfortis

G-Cloud 15 Framework Agreement, reference RM1557.15

|                            |                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Framework Agreement</b> | G-Cloud 15, framework reference RM1557.15, awarded by the Government Commercial Agency                                                       |
| <b>Lots</b>                | Lot 2b (Cloud Software) and Lot 3 (Cloud Support)                                                                                            |
| <b>Service</b>             | <b>FortisOne GRC by Cyberfortis:</b> a governance, risk and compliance platform, together with implementation, managed and advisory services |
| <b>Supplier</b>            | Cyberfortis Consulting Limited, a company incorporated in England and Wales under company number 16157381                                    |
| <b>Registered office</b>   | <b>Level 30, The Leadenhall Building, 122 Leadenhall Street, London EC3V 4AB</b>                                                             |
| <b>Enquiries</b>           | legal@cyberfortis.co.uk                                                                                                                      |
| <b>Document reference</b>  | FGRC-GC15-STC_v1.0_GB_09-2026                                                                                                                |
| <b>Date of issue</b>       | September 2026                                                                                                                               |
| <b>Governing law</b>       | The law of England and Wales                                                                                                                 |

These Supplier Terms and Conditions are supplementary and subordinate to the Call-Off Contract. Nothing contained in this document shall operate to limit, exclude, qualify or vary any provision of the Framework Agreement or of the Call-Off Contract.

---

## INTRODUCTION

### Guidance for the reader

---

*This section is provided for assistance only. It does not form part of the operative provisions of these Supplier Terms, and creates no right or obligation. See clause S.1.*

#### ***Nature and function of this document***

The contract between the Buyer and the Supplier is the **Call-Off Contract**, formed upon the Buyer placing an Order under the Framework Agreement. These Supplier Terms are supplementary to that contract and subordinate to it. Their function is confined to the following two matters:

- (a) to make provision for those matters which the Framework Agreement and the Call-Off Contract leave to be determined by the Supplier, being in particular service levels, support, security, data residency, sub-processing and exit; and
- (b) to record, in binding terms, the manner in which the Supplier operates the Service, so as to enable the Buyer to discharge its assurance obligations without recourse to a separate questionnaire.

Where these Supplier Terms and the Call-Off Contract are inconsistent, **the Call-Off Contract prevails**, in accordance with clause 2.3. Where these Supplier Terms impose upon the Supplier a standard higher than that required by the Call-Off Contract, **the higher standard binds the Supplier**, in accordance with clause 2.4.

#### ***Structure***

| Division   | Subject matter                                                | Principally addressed to                          |
|------------|---------------------------------------------------------------|---------------------------------------------------|
| Part A     | Contractual framework, order of precedence and scope          | Commercial and legal                              |
| Part B     | Service commitments, support and the obligations of the Buyer | Service owner                                     |
| Part C     | Data, security, artificial intelligence and accessibility     | Data protection officer, SIRO, security assurance |
| Part D     | Charges, intellectual property, liability and insurance       | Commercial and legal                              |
| Part E     | Term, exit, change control and supply chain                   | Contract manager                                  |
| Part F     | General provisions                                            | Legal                                             |
| Annex A    | Service levels, Service Credits and support                   | Service owner                                     |
| Annex B    | Data processing provisions and sub-processors                 | Data protection officer                           |
| Annex C    | Security and assurance statement                              | Security assurance                                |
| Schedule 1 | Obligations of the Buyer                                      | Project lead                                      |

#### **Matters expressly not reserved by the Supplier**

The reader's attention is drawn to clause 2.7, by which the Supplier expressly records that it does not require the Charges to be treated as confidential; does not disclaim responsibility for the continued availability of the Service; reserves no right to terminate for convenience; reserves no right to vary these Supplier Terms unilaterally; imposes no charge for the return of Buyer Data; and does not rely upon any certification held by a third party as though it were a certification of the Supplier.

#### **Certifications: statement as to reliance**

FortisOne GRC is constructed upon the IBM OpenPages architecture, licensed to the Supplier under an IBM Embedded Solution Agreement. IBM holds certifications in respect of that platform. **Those are certifications of IBM and not of the Supplier, and the Supplier does not present them as its own.** The Supplier holds **Cyber Essentials Plus**, valid to August 2027. **The Supplier is not certified to ISO/IEC 27001 and does not claim to be**, although it operates an information security management system designed to that standard, which the Buyer is invited to inspect. Certification to **ISO 9001** is in progress. Paragraph C.1 records precisely which certification is held by which party.

### ***Where the answers are***

Cyberfortis applies a traceability rule: every assertion of compliance should point to a page, an artefact or an accountable owner. The following table directs the most common due-diligence questions to the clause which answers them, so that the Buyer need not issue a separate questionnaire.

| <b>Question commonly asked in assurance</b>                         | <b>Answered at</b> |
|---------------------------------------------------------------------|--------------------|
| Where is our data held, and does it ever leave the United Kingdom?  | 12.1 · 12.2 · B.6  |
| Who can access it, and from where?                                  | 12.4 · 12.5 · C.2  |
| Do you train artificial intelligence models on our data?            | 14.1 – 14.3        |
| What happens if the service is unavailable, and what do we get?     | 5 · A.2 · A.3      |
| How quickly are we told about a breach, and what will you tell us?  | 13.4 · B.4         |
| Who are your sub-processors, and what happens if we object to one?  | 25.4 · B.7         |
| Which certifications do you hold, and which are held by others?     | C.1                |
| May we audit you, and may we test the service ourselves?            | 9.3 · 13.6 · B.3.4 |
| How do we get our data out, in what format, and at what cost?       | 23.3 · 23.4        |
| Will you delete it afterwards, and prove that you have?             | 23.6 · 23.7        |
| Can the Charges rise, and can the contract renew without us acting? | 16.2 – 16.4        |
| Can you walk away from us, or withdraw the service?                 | 22.4 · 22.6        |
| Is the service accessible, and what is not yet conformant?          | 15.1 – 15.4        |
| What insurance do you carry, and for how long?                      | 20.1 · 20.2        |
| Are we required to indemnify you for anything?                      | 28.13              |

### ***Evidence available before award***

The Supplier provides each of the following to a prospective Buyer on request, at no charge, before any Order is placed, so that assurance may be completed in parallel with commercial evaluation rather than after it.

- Cyber Essentials Plus certificate, and evidence of the current certification status of the Platform and infrastructure providers.
- Information security policy set, internal audit summary and current risk register extract.
- Executive summary of the most recent independent penetration test, with remediation status.
- Business continuity and disaster recovery test summary.
- Current sub-processor list, and the data flow and residency description at Annex B.
- Accessibility statement and the most recent independent accessibility audit report.
- Carbon Reduction Plan, and certificates evidencing the insurance required by clause 20.1.
- The information security management system documentation described at paragraph C.1.1, offered for inspection in place of an ISO/IEC 27001 certificate which the Supplier does not hold.
- A specimen monthly service report, so that the Buyer can see in advance exactly what it will receive under paragraph A.6.1.
- A specimen post-incident report of the kind produced under paragraph A.4.4.
- The exit plan template and the data dictionary used for exports under clause 23.3.
- A written response to any assurance question not answered by this document, provided within 5 Working Days.

### **Assurance should not wait for award**

The Supplier's position is that a Buyer should be able to complete its security, data protection and accessibility assurance **before** it commits, using material the Supplier provides at no charge and without a non-disclosure agreement. Nothing in the list above is treated by the Supplier as commercially sensitive.

The corresponding operative provision is at paragraph C.8. *This block is provided for the assistance of the reader and does not form part of the operative provisions.*

---

## SUMMARY

### Schedule of principal commitments

---

*This schedule is provided for reference only and does not form part of the operative provisions. See clause S.1. Each commitment is set out in full in the clause referred to, and the operative wording governs.*

| Subject                 | Commitment of the Supplier                                                                                                               | Clause      |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| Availability            | Not less than <b>99.9%</b> in each calendar month, measured as prescribed by paragraph A.2.4                                             | 5 · A.2     |
| Service Credits         | Applied <b>automatically</b> , up to 30% of the monthly Charge, and expressly <b>not</b> the sole remedy                                 | 5.4 · A.3   |
| Severity 1 response     | <b>30 minutes, 24 hours a day, 365 days a year</b> , including public holidays                                                           | 6.2 · A.4   |
| Data residency          | <b>Exclusively within the United Kingdom</b> , including backups, disaster recovery copies and logs                                      | 12.1        |
| Personnel access        | Restricted to <b>UK-based personnel screened to BPSS</b> ; no access by personnel outside the UK, including those of technology partners | 12.4        |
| Personal Data Breach    | Notified to the Buyer within <b>24 hours</b> of the Supplier becoming aware, with prescribed content                                     | 13.4 · B.4  |
| Buyer Data              | Ownership vests in and remains with the Buyer. <b>The Supplier acquires no right, title or interest in it</b>                            | 10.1 · 10.2 |
| Artificial intelligence | No training upon Buyer Data; no cross-tenant learning; contractual <b>zero retention</b> by model providers                              | 14.1 – 14.3 |
| Sub-processors          | Each <b>named</b> at paragraph B.7; 30 days' notice of change, with rights of objection and termination                                  | 25.4 · B.7  |
| Exit and portability    | Complete Buyer Data in open, documented formats within <b>10 Working Days</b> , at <b>no charge</b>                                      | 23.3        |
| Certified deletion      | Secure deletion, evidenced by <b>written certificate</b> , within 15 Working Days of request                                             | 23.6        |
| Charges                 | Fixed for the initial term; <b>no automatic renewal</b> ; renewal increases capped by reference to CPI                                   | 16.2 – 16.4 |
| Termination             | The Supplier <b>shall not terminate for convenience</b>                                                                                  | 22.4        |
| Change control          | No change degrading security, functionality, performance or accessibility; <b>no unilateral variation</b>                                | 24.2 · 24.5 |
| Insurance               | <b>£7,000,000</b> maintained throughout the Term and for six years thereafter                                                            | 20.1 · 20.2 |
| Accessibility           | Conformance target of <b>WCAG 2.2 Level AA</b> , with published accessibility statement                                                  | 15.1        |
| Transparency            | Full co-operation with FOIA and the transparency requirements; <b>the Charges are not asserted to be exempt</b>                          | 18.2 · 18.4 |
| Limitation              | <b>No contractual limitation period is imposed</b> ; the Limitation Act 1980 applies without abridgement                                 | 19.4        |
| Indemnities             | <b>No provision requires the Buyer to indemnify the Supplier</b>                                                                         | 28.13       |

---

## Contents

---

|                                                                    |  |
|--------------------------------------------------------------------|--|
| <b>PRELIMINARY — BACKGROUND AND STATUS.....7</b>                   |  |
| R Background.....7                                                 |  |
| S Status of the introductory material.....7                        |  |
| <b>PART A — CONTRACTUAL FRAMEWORK.....8</b>                        |  |
| 1 Definitions and interpretation.....8                             |  |
| 2 Status of these Supplier Terms and order of precedence.....9     |  |
| 3 Scope of the Services.....10                                     |  |
| <b>PART B — SERVICE COMMITMENTS.....11</b>                         |  |
| 4 Provision of the Service.....11                                  |  |
| 5 Service levels and Service Credits.....11                        |  |
| 6 Support.....11                                                   |  |
| 7 Business continuity and disaster recovery.....12                 |  |
| 8 Buyer responsibilities.....12                                    |  |
| 9 Acceptable use.....12                                            |  |
| <b>PART C — DATA, SECURITY AND AI.....13</b>                       |  |
| 10 Buyer Data and ownership.....13                                 |  |
| 11 Data protection.....13                                          |  |
| 12 Data residency and location.....13                              |  |
| 13 Security.....14                                                 |  |
| 14 Artificial intelligence and machine learning.....14             |  |
| 15 Accessibility.....15                                            |  |
| <b>PART D — COMMERCIAL TERMS.....16</b>                            |  |
| 16 Charges and payment.....16                                      |  |
| 17 Intellectual property rights.....16                             |  |
| 18 Confidentiality, freedom of information and transparency.....17 |  |
| 19 Liability.....17                                                |  |
| 20 Insurance.....17                                                |  |
| 21 Warranties.....18                                               |  |
| <b>PART E — TERM, CHANGE AND EXIT.....20</b>                       |  |
| 22 Term, suspension and termination.....20                         |  |
| 23 Exit management and data portability.....20                     |  |
| 24 Change control.....21                                           |  |
| 25 Sub-contracting and supply chain.....21                         |  |
| 26 Staff.....22                                                    |  |
| 27 Sustainability and social value.....22                          |  |
| <b>PART F — GENERAL PROVISIONS.....24</b>                          |  |
| 28 General.....24                                                  |  |
| <b>ANNEX A — SERVICE LEVELS AND SUPPORT.....25</b>                 |  |
| A.1 Application.....25                                             |  |
| A.2 Availability.....25                                            |  |
| A.3 Service Credits.....26                                         |  |
| A.4 Support and incident management.....27                         |  |
| A.5 Escalation.....27                                              |  |
| A.6 Service reporting and review.....28                            |  |
| A.7 Worked example of the Availability calculation.....28          |  |
| A.8 Service management calendar.....29                             |  |
| <b>ANNEX B — DATA PROCESSING ANNEX.....30</b>                      |  |
| B.1 Roles.....30                                                   |  |
| B.2 Details of processing.....30                                   |  |
| B.3 Supplier obligations.....30                                    |  |
| B.4 Personal data breach.....30                                    |  |
| B.5 Assistance.....31                                              |  |
| B.6 International transfers.....31                                 |  |
| B.7 Sub-processors.....31                                          |  |
| B.8 Return and deletion.....32                                     |  |
| B.9 Retention schedule.....32                                      |  |
| B.10 Records of processing.....32                                  |  |
| <b>ANNEX C — SECURITY AND ASSURANCE.....33</b>                     |  |
| C.1 Certifications: who holds what.....33                          |  |
| C.2 NCSC Cloud Security Principles.....35                          |  |
| C.3 Division of responsibility.....36                              |  |
| C.4 Security testing.....36                                        |  |
| C.5 Vulnerability remediation.....36                               |  |
| C.6 Security incidents.....37                                      |  |
| C.7 Information classification.....37                              |  |
| C.8 Assurance evidence pack.....37                                 |  |
| <b>SCHEDULE 1 — BUYER OBLIGATIONS.....38</b>                       |  |
| <b>SCHEDULE 2 — DOCUMENT CONTROL.....39</b>                        |  |

## Background and status

---

### R. Background

- (A) The Supplier has been appointed to the Framework Agreement in respect of Lot 2b (Cloud Software) and Lot 3 (Cloud Support).
- (B) The Buyer wishes to procure the Service from the Supplier pursuant to a Call-Off Contract awarded under the Framework Agreement.
- (C) These Supplier Terms set out supplementary provisions applicable to the provision of the Service, and are incorporated into the Call-Off Contract subject to, and in accordance with, clause 2.
- (D) These Supplier Terms are subordinate to the Call-Off Contract in accordance with clause 2.3. Nothing in these Supplier Terms is intended to derogate from, and no provision shall be construed as derogating from, the rights and remedies of the Buyer or the obligations and liabilities of the Supplier arising under the Framework Agreement or the Call-Off Contract.
- (E) These Supplier Terms comprise six Parts (Parts A to F inclusive), three Annexes (Annexes A to C inclusive) and one Schedule (Schedule 1), each of which forms part of these Supplier Terms save where expressly provided otherwise.

### S. Status of the introductory material

- S.1 The sections of this document entitled “Guidance for the reader” and “Schedule of principal commitments” are provided for the assistance of the reader only. **Those sections do not form part of the operative provisions of these Supplier Terms and give rise to no right, obligation or liability on the part of either Party.**
- S.2 In the event of any inconsistency between either of those sections and the operative provisions of these Supplier Terms, **the operative provisions shall prevail.**
- S.3 The recitals set out at clause R are included by way of context and as a record of the Parties’ intention. They do not of themselves create obligations, but may be relied upon as an aid to construction.

## Contractual framework

---

### 1. Definitions and interpretation

- 1.1** Capitalised terms used in these Supplier Terms and not defined below have the meaning given to them in the Call-Off Contract. Where a term is defined both here and in the Call-Off Contract, the Call-Off Contract definition prevails.
- 1.2** In these Supplier Terms, save where the context otherwise requires, the following expressions shall have the following meanings:
- (a) **“AI Feature”** means any functionality within the Service which employs artificial intelligence, machine learning or a large language model to generate, classify, summarise, score or recommend;
  - (b) **“Annexes”** means Annex A, Annex B and Annex C, and **“Schedule 1”** means Schedule 1, each of which forms part of these Supplier Terms;
  - (c) **“Authorised User”** means an individual authorised by the Buyer to access and use the Service;
  - (d) **“Availability”** has the meaning given at paragraph A.2.2;
  - (e) **“Buyer”** means the Contracting Authority which places an Order for the Service under the Framework Agreement;
  - (f) **“Buyer Data”** means all data, records, content and information which the Buyer or any Authorised User uploads to, creates within, or generates by means of the Service, including risk registers, control libraries as configured by the Buyer, policies, assessments, evidence, audit trails, workflow history, incident records, reports and exports;
  - (g) **“Call-Off Contract”** means the contract formed between the Buyer and the Supplier under the Framework Agreement, comprising the General Terms, the Joint Schedules, the Call-Off Schedules and the Order Form;
  - (h) **“Charges”** means the sums payable by the Buyer to the Supplier as set out in the Order Form;
  - (i) **“Data Protection Legislation”** means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003, and all other applicable law relating to the processing of personal data, in each case as amended, extended, consolidated or re-enacted from time to time;
  - (j) **“Framework Agreement”** means the G-Cloud 15 framework agreement, reference RM1557.15;
  - (k) **“Good Industry Practice”** means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness which would reasonably and ordinarily be expected of a skilled and experienced supplier of services substantially similar to the Service;
  - (l) **“Order”** means an order for the Service placed by the Buyer under the Framework Agreement, and **“Order Form”** means the order form executed by the Parties in respect of that Order;
  - (m) **“Party”** means the Buyer or the Supplier, and **“Parties”** means both of them;
  - (n) **“Personal Data Breach”** has the meaning given in Article 4(12) of the UK GDPR;
  - (o) **“Platform”** means the IBM OpenPages technology upon which the Service is constructed, licensed to the Supplier under an IBM Embedded Solution Agreement;
  - (p) **“Platform Event”** means an unavailability of the Service caused solely by a failure of the Platform or of the underlying cloud infrastructure, which the Supplier could not have prevented by the exercise of Good Industry Practice;
  - (q) **“Security Incident”** means any actual or reasonably suspected unauthorised access to, disclosure of, alteration of, loss of or destruction of Buyer Data, or any actual or reasonably suspected compromise of the security of the Service;
  - (r) **“Service”** means FortisOne GRC by Cyberfortis, together with any Implementation Services or Managed and Advisory Services identified in the Order Form;

- (s) **“Service Commencement Date”** means the date specified as such in the Order Form;
- (t) **“Service Credit”** means a credit calculated in accordance with paragraph A.3.1;
- (u) **“Supplier”** means Cyberfortis Consulting Limited, a company incorporated in England and Wales under company number 16157381;
- (v) **“Supplier Terms”** means this document, comprising Parts A to F inclusive, the Annexes and Schedule 1;
- (w) **“Support Hours”** means 08:00 to 18:00 UK time on Working Days, save in respect of Severity 1 incidents, for which support is available 24 hours a day on every day of the year;
- (x) **“Term”** means the period commencing on the Service Commencement Date and expiring in accordance with the Order Form; and
- (y) **“Working Day”** means any day other than a Saturday, Sunday or public holiday in England and Wales.

**1.3** In these Supplier Terms, save where the context otherwise requires:

- (a) words importing the singular include the plural and vice versa, and words importing one gender include every gender;
- (b) a reference to a person includes a natural person, a body corporate, an unincorporated association, a partnership and any governmental or regulatory body, in each case whether or not having separate legal personality;
- (c) a reference to a statute or statutory provision is a reference to it as amended, extended, consolidated or re-enacted from time to time, and includes all subordinate legislation made under it;
- (d) the words “including”, “includes” and “in particular” are to be construed as illustrative and shall not limit the generality of any preceding words;
- (e) a reference to a clause, paragraph, Part, Annex or Schedule is a reference to a clause, paragraph, Part, Annex or Schedule of these Supplier Terms;
- (f) headings are included for convenience only and shall not affect the construction of these Supplier Terms;
- (g) a reference to writing or written includes email transmitted to the addresses specified in the Order Form; and
- (h) any obligation upon a Party not to do an act or thing includes an obligation not to permit or suffer that act or thing to be done.

## **2. Status of these Supplier Terms and order of precedence**

**2.1** These Supplier Terms are the supplier terms referred to in the Order Form. They are supplementary to the Call-Off Contract and are incorporated into it, subject to this clause 2.

**2.2** In the event of any conflict, ambiguity or inconsistency, the following documents take precedence in descending order:

- (a) the General Terms of the Framework Agreement (RM1557.15);
- (b) the Joint Schedules;
- (c) the Call-Off Schedules;
- (d) the Order Form;
- (e) these Supplier Terms, including the Annexes; and
- (f) any other document referred to in these Supplier Terms.

**2.3** **Notwithstanding any other provision of these Supplier Terms, any provision of these Supplier Terms which conflicts with a document ranking above it has no effect to the extent of that conflict**, and the higher-ranking document prevails. No provision of these Supplier Terms is to be read as limiting, excluding,

qualifying or varying any right or remedy of the Buyer, or any obligation, liability or warranty of the Supplier, arising under the Framework Agreement or the Call-Off Contract.

- 2.4 Where these Supplier Terms impose on the Supplier a standard, obligation or commitment that is higher than, or additional to, that required by the Call-Off Contract, the higher standard applies and is binding on the Supplier.** Clause 2.3 operates only to prevent the Supplier from contracting below the framework position; it does not release the Supplier from any commitment made in these Supplier Terms.
- 2.5** If any provision of these Supplier Terms is or becomes invalid, unenforceable or of no effect under clause 2.3, it is severed and the remainder of these Supplier Terms continues in full force.
- 2.6** The Supplier shall not seek to rely upon, nor invite the Buyer to give effect to, any provision of these Supplier Terms which is of no effect by operation of clause 2.3.

***Statement of non-reservation***

- 2.7** For the avoidance of doubt, and without prejudice to the generality of clause 2.3, the Supplier expressly records that it does not by these Supplier Terms:
- (a) require the Buyer to treat the Charges, or the terms of the Call-Off Contract, as confidential;
  - (b) disclaim or qualify its responsibility for the continued availability of the Service;
  - (c) reserve any right to terminate the Call-Off Contract for convenience;
  - (d) reserve any right to vary these Supplier Terms unilaterally, whether by publication, notice or otherwise;
  - (e) impose any charge in respect of the return or export of Buyer Data;
  - (f) seek any indemnity from the Buyer; or
  - (g) rely upon any certification held by a third party as though it were a certification of the Supplier.
- 2.8** The Supplier acknowledges that the Buyer may rely upon the statements set out at clause 2.7, and that each of them is a term of the Call-Off Contract.

**3. Scope of the Services**

- 3.1** These Supplier Terms are modular. Only those clauses relating to the Services actually identified in the Order Form apply to the Buyer. The Buyer is not required to read or accept terms relating to Services it has not ordered.
- 3.2 Platform Services (Lot 2b — Cloud Software).** Provision of the FortisOne GRC by Cyberfortis platform as a subscription service, including hosting, maintenance, updates, support and the service levels in Annex A.
- 3.3 Implementation Services (Lot 3 — Cloud Support).** Where ordered: discovery, configuration, control library and framework mapping, data migration, integration, testing, training and go-live support, as scoped in the Order Form.
- 3.4 Managed and Advisory Services (Lot 3 — Cloud Support).** Where ordered: ongoing administration of the Buyer's FortisOne environment, and governance, risk and compliance advisory support, as scoped in the Order Form.
- 3.5** The Order Form is the definitive record of what has been ordered, the applicable Charges, the term, and any Service-specific variations. Where the Order Form and these Supplier Terms differ, the Order Form prevails.
- 3.6** Advisory Services are provided as professional support to the Buyer's own governance and decision-making. They do not constitute legal, regulatory, audit or financial advice, and do not transfer to the Supplier any statutory or regulatory obligation of the Buyer.

---

## PART B

### Service commitments

---

#### 4. Provision of the Service

- 4.1 The Supplier shall provide the Service from the Service Commencement Date in accordance with the Call-Off Contract, these Supplier Terms, the Annexes and Good Industry Practice, and shall provide the facilities, personnel, infrastructure, software and other resources necessary to do so.
- 4.2 The Buyer may permit Authorised Users to access the Service up to the entitlement in the Order Form. The Buyer administers its own users and may add, suspend or remove them at any time without reference to the Supplier.
- 4.3 The Supplier shall make available at no additional charge: role-based access control, single sign-on via SAML 2.0 or OpenID Connect, multi-factor authentication, and a complete, exportable user access audit trail.
- 4.4 The Supplier shall provide user documentation, administrator documentation and standard training materials at no additional charge, and shall keep them current.
- 4.5 The Supplier shall provide at least one non-production environment at no additional charge, for the Buyer to test configuration and releases before they reach production.
- 4.6 The Supplier shall not suspend, degrade or withdraw the Service, or any material feature of it, except as expressly permitted by clause 22 or clause 24.

#### 5. Service levels and Service Credits

- 5.1 The Supplier commits to the service levels set out in Annex A. Those service levels are contractual commitments, not targets, aspirations or statements of intent.
- 5.2 The Supplier shall achieve Availability of **at least 99.9% in each calendar month**, measured as set out in paragraph A.2.
- 5.3 Where Availability falls below 99.9% in any month, the Buyer is entitled to Service Credits calculated under paragraph A.3. The Supplier shall apply Service Credits to the next invoice and shall not require the Buyer to make a claim, provide evidence, or meet any minimum threshold.
- 5.4 **Service Credits are not the Buyer's sole or exclusive remedy.** The Buyer's rights and remedies under the Call-Off Contract and at law, including in respect of termination, damages and specific performance, are unaffected by the payment or availability of Service Credits.
- 5.5 The Supplier shall provide a monthly service report at no charge, showing measured Availability, every incident raised with severity and resolution time, planned maintenance undertaken, and any Service Credits due.
- 5.6 If the Supplier fails to meet the Availability commitment in any two months within a rolling six-month period, the Supplier shall, at no charge and within 10 Working Days, produce a rectification plan for the Buyer's approval setting out root cause and remedial action. This is in addition to, and does not limit, the Buyer's rights under the Call-Off Contract.

#### 6. Support

- 6.1 The Supplier shall provide support in accordance with the severity matrix at paragraph A.4.
- 6.2 Severity 1 support is available **24 hours a day, 365 days a year**, including weekends and public holidays, with a response commitment of 30 minutes.
- 6.3 Support is available through the service desk portal and by email at all times, and by telephone for Severity 1 incidents.
- 6.4 Support of the Service is included in the Charges. The Supplier shall not charge separately for incident diagnosis, defect correction, service requests, or advice on the correct use of the Service.

- 6.5 The Supplier shall assign a named service manager as the Buyer's single point of escalation, and shall notify the Buyer before changing that individual.

## 7. Business continuity and disaster recovery

- 7.1 The Supplier maintains a business continuity and disaster recovery plan, tests it at least annually, and shall make the test summary available to the Buyer on request at no charge.
- 7.2 The Supplier commits to a **Recovery Point Objective of 1 hour** and a **Recovery Time Objective of 4 hours** for the Service.
- 7.3 Backups are taken daily, encrypted, retained for 35 days, stored within the United Kingdom, and restore-tested at least quarterly.
- 7.4 The Supplier shall notify the Buyer without undue delay, and in any event within 4 hours, on invoking its disaster recovery plan in a way that affects the Buyer.
- 7.5 The Supplier shall co-operate with the Buyer's own business continuity planning and shall comply with the applicable Call-Off Schedule relating to business continuity and disaster recovery.

## 8. Buyer responsibilities

- 8.1 The Buyer shall perform the obligations set out in Schedule 1. Those obligations are limited to what the Supplier genuinely requires in order to deliver the Service.
- 8.2 Where the Supplier is prevented from performing an obligation as a direct result of the Buyer's failure to perform an obligation in Schedule 1, the Supplier is relieved of that obligation to the extent, and for so long as, the failure continues, **provided that** the Supplier has: (i) notified the Buyer promptly and in writing of the failure and its likely effect; (ii) taken all reasonable steps to mitigate; and (iii) resumed performance promptly once the failure is remedied.
- 8.3 The Supplier shall not rely on clause 8.2 unless it can demonstrate a direct causal link between the Buyer's failure and the Supplier's non-performance. Clause 8.2 is not a general defence to underperformance.

## 9. Acceptable use

- 9.1 The Buyer shall not knowingly use the Service to undertake any activity, or host any content, that is unlawful, fraudulent, malicious or infringing, or that is intended to disrupt or gain unauthorised access to systems, networks or data.
- 9.2 The Buyer shall not reverse engineer the Service, resell direct access to it to a third party, or use it to build a competing product, except to the extent such restriction is prohibited by law.
- 9.3 **The Buyer may conduct security testing, including penetration testing, of its own FortisOne environment** on 10 Working Days' written notice, at no charge and without the Supplier's prior approval. The Supplier shall co-operate with such testing and shall remediate confirmed findings in accordance with paragraph C.5.
- 9.4 Where the Supplier believes the Buyer has breached this clause 9, it shall notify the Buyer, allow a reasonable period to remedy, and engage with the Buyer before taking any action. Suspension is governed by clause 22.5 and is a measure of last resort.

---

## PART C

### Data, security and artificial intelligence

---

#### 10. Buyer Data and ownership

- 10.1 All Buyer Data is and remains the property of the Buyer.** This includes every risk register, control, policy, assessment, item of evidence, audit trail, incident record, workflow history, report and export created in or generated by the Service, together with all Intellectual Property Rights in them.
- 10.2** The Supplier acquires no right, title or interest in Buyer Data. The Buyer grants the Supplier a limited, non-exclusive, non-transferable licence to process Buyer Data solely and exclusively to the extent necessary to provide the Service. That licence terminates on expiry or termination of the Call-Off Contract, subject only to clause 23.
- 10.3 The Supplier shall not use Buyer Data for any purpose other than providing the Service to the Buyer.** In particular, and without limitation, the Supplier shall not use Buyer Data, whether in identifiable, pseudonymised, anonymised or aggregated form, for:
- (a) product research, development or improvement;
  - (b) benchmarking, market analysis, sector reporting or the creation of any dataset or derived product;
  - (c) training, fine-tuning or evaluating any artificial intelligence or machine learning model;
  - (d) marketing, sales, case studies or any form of publicity; or
  - (e) any commercial purpose of the Supplier or of any third party.
- 10.4** The Supplier takes no right to create or exploit anonymised or aggregated datasets derived from Buyer Data. Where the Supplier wishes to do so in future it must ask, and the Buyer is under no obligation to agree. Any such use requires the Buyer's prior written, specific and revocable consent, and the absence of consent shall not affect the Service, the Charges or the Supplier's performance.
- 10.5** Buyer Data is the Buyer's Confidential Information for the purposes of the Call-Off Contract.
- 10.6** The Supplier shall not use the Buyer's name, logo or the existence of the Call-Off Contract in any marketing or publicity without the Buyer's prior written consent, save for the transparency publication required by law or the Framework Agreement.

#### 11. Data protection

- 11.1** For the purposes of the Service, the Buyer is the Controller and the Supplier is the Processor in respect of Personal Data contained within Buyer Data.
- 11.2** Annex B sets out the processing terms required by Article 28 of the UK GDPR. Where the Call-Off Contract includes a data processing schedule, that schedule prevails and Annex B supplements it to the extent of any additional protection it provides to the Buyer.
- 11.3** The Supplier shall comply with the Data Protection Legislation, including the UK GDPR and the Data Protection Act 2018, and shall process Personal Data only on the Buyer's documented instructions.
- 11.4** The Supplier shall provide reasonable assistance at no charge with the Buyer's data protection impact assessments, records of processing, prior consultations with the Information Commissioner, and responses to data subject rights requests.
- 11.5** The Supplier shall notify the Buyer immediately if it considers that an instruction from the Buyer infringes the Data Protection Legislation.

#### 12. Data residency and location

- 12.1 All Buyer Data is stored and processed exclusively within the United Kingdom.** This applies to production data, backups, disaster recovery copies, system and application logs, telemetry, and any Buyer Data contained in support tickets or diagnostic material.

- 12.2 The Supplier shall not transfer Buyer Data outside the United Kingdom. If a transfer ever becomes necessary, the Supplier shall seek the Buyer's prior written consent, and shall not proceed without it. The Buyer may withhold consent without giving reasons and without any effect on the Charges or the Service. Where consent is given, the Supplier shall put in place the UK International Data Transfer Agreement or the UK Addendum, together with a documented transfer risk assessment, before any transfer occurs.
- 12.3 The Supplier shall notify the Buyer at least 30 days before any proposed change to the location of processing, and the Buyer may terminate the affected Service without penalty and without liability for early termination charges if it does not accept the change.
- 12.4 **Access to the production environment is restricted to Supplier personnel located in the United Kingdom who have been security screened to Baseline Personnel Security Standard as a minimum.** No personnel outside the United Kingdom have or shall be granted access to the production environment or to Buyer Data, including personnel of the Supplier's technology partners and sub-processors.
- 12.5 All administrative and privileged access to Buyer Data is logged. The Supplier shall make the access log available to the Buyer on request at no charge, and shall retain it for at least 12 months.

### 13. Security

- 13.1 Annex C sets out the Supplier's security and assurance position, including the mapping of the Service to the National Cyber Security Centre's Cloud Security Principles and the certifications held by each party.
- 13.2 The Supplier shall maintain security measures that comply with Good Industry Practice, the requirements of the applicable Call-Off Schedule relating to security, and the principles of ISO/IEC 27001 and ISO/IEC 27002.
- 13.3 Buyer Data is encrypted at rest using AES-256 or equivalent, and in transit using TLS 1.2 or above.
- 13.4 The Supplier shall notify the Buyer of any Security Incident affecting or reasonably likely to affect the Buyer **within 24 hours** of becoming aware of it, whether or not the incident involves Personal Data, and shall keep the Buyer informed as the incident is investigated and resolved.
- 13.5 The Supplier shall remediate confirmed vulnerabilities within the timescales at paragraph C.5, and shall notify the Buyer where a critical vulnerability affecting the Service cannot be remediated within that period.
- 13.6 The Buyer, and any auditor appointed by the Buyer, may audit the Supplier's compliance with these Supplier Terms on 10 Working Days' notice, at no charge, once per contract year and at any time following a Security Incident. The Supplier shall provide reasonable access to relevant records, personnel and evidence.
- 13.7 The Supplier shall notify the Buyer of any material adverse change to its security posture, certification status or supply chain, within 10 Working Days of becoming aware of it.

### 14. Artificial intelligence and machine learning

This clause 14 shall apply wherever the Service comprises or includes an AI Feature, and shall prevail over any other provision of these Supplier Terms which is inconsistent with it.

- 14.1 **The Supplier shall not use Buyer Data to train, fine-tune, evaluate or otherwise improve any artificial intelligence or machine learning model,** whether the Supplier's own, the Platform's, or that of any third party.
- 14.2 **There is no cross-tenant learning.** No model or model behaviour presented to the Buyer is derived from, informed by, or improved using the data of any other customer, and no Buyer Data shall influence any output presented to any other customer.
- 14.3 Where an AI Feature relies on a third-party model provider, the Supplier shall contract with that provider on **zero-retention** terms, prohibiting the provider from storing Buyer Data beyond the duration of the request, from using it for training or evaluation, and from subjecting it to human review. The Supplier shall name every such provider in Annex B.

- 14.4 AI Features are decision support only.** Output from an AI Feature does not constitute legal, regulatory, audit or professional advice, does not represent the Supplier's assessment of the Buyer's compliance position, and does not replace the Buyer's own judgement, assurance activity or statutory decision-making.
- 14.5** No AI Feature shall make or implement a decision producing legal effects for, or similarly significantly affecting, any individual without meaningful human review by an Authorised User. The Service is configured so that AI-generated content requires human acceptance before it is recorded as an approved record.
- 14.6 Every AI-assisted action is logged, attributable and exportable.** The audit trail records that an AI Feature was used, which user accepted, amended or rejected the output, and when. The Buyer may export this record at any time.
- 14.7 The Buyer may disable any or all AI Features at any time,** in whole or in part, at no charge, by configuration and without notice. Disabling AI Features shall not reduce the core functionality of the Service, affect the Charges, or constitute a breach by the Buyer.
- 14.8** The Supplier shall give the Buyer at least 30 days' written notice before introducing a new AI Feature, changing the model or model provider underlying an existing AI Feature, or materially changing how an AI Feature processes Buyer Data. The Buyer may decline the change, in which case the Supplier shall maintain the existing behaviour or the Buyer may disable the feature under clause 14.7.
- 14.9** The Supplier shall provide, at no charge, the information the Buyer reasonably requires to complete its own AI assurance activity, including any record required under the Algorithmic Transparency Recording Standard and any assessment required by the Buyer's obligations or by government AI guidance applicable to the Buyer.

## **15. Accessibility**

- 15.1** The Supplier's conformance target for the Service is **Web Content Accessibility Guidelines 2.2 Level AA**.
- 15.2** The Supplier publishes and maintains an accessibility statement for the Service, to assist the Buyer in meeting its obligations under the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018.
- 15.3 Where the Service does not fully conform, the Supplier shall say so.** The accessibility statement identifies each known non-conformance, its effect on users, any available workaround, and the date by which the Supplier intends to remedy it.
- 15.4** The Supplier shall provide its most recent independent accessibility audit report to the Buyer on request at no charge.
- 15.5** An accessibility regression introduced by a Supplier release is a defect and shall be corrected under the support process in Annex A at no charge.

---

## PART D

### Commercial terms

---

#### 16. Charges and payment

- 16.1 The Charges are those set out in the Order Form and do not exceed the Framework Prices.
- 16.2 **The Charges are fixed for the initial term.** The Supplier shall not increase the Charges during the initial term for any reason.
- 16.3 Any change to the Charges on renewal requires at least 90 days' written notice and is **capped at the percentage increase in the Consumer Prices Index** over the preceding 12 months. The Buyer may decline the increase, in which case it may allow the Call-Off Contract to expire without penalty.
- 16.4 **There is no automatic renewal.** The Call-Off Contract expires at the end of its term unless the parties expressly agree a renewal in writing. The Buyer is not required to give notice to prevent renewal.
- 16.5 The Supplier shall invoice in accordance with the Order Form. Correctly rendered, undisputed invoices are payable **within 30 days** of receipt, in accordance with the Call-Off Contract and applicable public procurement policy on prompt payment.
- 16.6 Where the Buyer disputes an invoice in good faith it shall pay the undisputed portion by the due date and notify the Supplier of the dispute. **The Supplier shall not suspend, degrade or withhold the Service, or withhold access to Buyer Data, on account of a good-faith payment dispute.**
- 16.7 Interest on late payment of undisputed sums is limited to the statutory rate under the Late Payment of Commercial Debts (Interest) Act 1998. The Supplier shall not charge any additional or contractual late payment fee.
- 16.8 **The Charges are the only amounts payable.** Without limitation, the Supplier shall not charge for: support; software updates, patches or new releases of ordered functionality; non-production environments; standard service and management reporting; data export or exit assistance within clause 23; responses to security questionnaires or assurance requests; or co-operation with audits under clause 13.6.
- 16.9 The Charges are exclusive of VAT, which is payable at the prevailing rate. The Supplier shall accept electronic invoicing in the form the Buyer reasonably requires.

#### 17. Intellectual property rights

- 17.1 Neither party acquires any right, title or interest in the other's Existing IPR except as expressly granted.
- 17.2 The Supplier or its licensors own the FortisOne GRC software, the Platform, the Supplier's configuration layer, its methodologies, and any control libraries and content templates supplied by the Supplier as standard.
- 17.3 The Buyer owns Buyer Data in accordance with clause 10, together with all materials the Buyer provides and all configuration, content and control mappings the Buyer creates within the Service.
- 17.4 Specific IPR created under the Call-Off Contract is dealt with in the applicable Call-Off Schedule. Where the Order Form is silent, **any deliverable prepared exclusively for the Buyer is owned by the Buyer** on payment of the Charges relating to it.
- 17.5 The Supplier grants the Buyer a non-exclusive licence to use the Service and the documentation for its own purposes and those of any other Contracting Authority with which it shares services, for the term. Reports and exports generated by the Buyer may be used, retained and disclosed by the Buyer without restriction and without time limit, including after termination.
- 17.6 The Supplier shall indemnify the Buyer against claims that the Service infringes a third party's Intellectual Property Rights, in accordance with the Call-Off Contract. That indemnity extends to open source components which the Supplier has selected and embedded in the Service.
- 17.7 The Supplier maintains a register of open source components used in the Service, together with their licences, and shall provide it to the Buyer on request at no charge.

- 17.8 **Source code and data escrow is available to the Buyer on request**, on standard terms with a recognised escrow agent, with release events including the Supplier's insolvency or sustained failure to provide the Service.

## 18. Confidentiality, freedom of information and transparency

- 18.1 Each party shall keep the other's Confidential Information confidential and use it only for the purposes of the Call-Off Contract, in accordance with the Call-Off Contract.
- 18.2 **The Supplier acknowledges that the Buyer is subject to the Freedom of Information Act 2000 and the Environmental Information Regulations 2004, and shall not do anything to obstruct or delay the Buyer in meeting those obligations.**
- 18.3 Where the Buyer consults the Supplier on a proposed disclosure, the Supplier shall respond within 5 Working Days. If the Supplier does not respond in that period it is taken to have no objection.
- 18.4 **The Supplier does not assert that the Charges payable under the Call-Off Contract are exempt from disclosure**, and shall not object to their publication.
- 18.5 **The decision whether to disclose information in response to a request is the Buyer's alone.** The Supplier shall not challenge the Buyer's decision, and the Buyer incurs no liability to the Supplier for any disclosure made in good faith.
- 18.6 The Supplier consents to publication of the Call-Off Contract and Order Form under the Government's transparency requirements, subject only to redaction of information properly identified as commercially sensitive in the relevant Joint Schedule.
- 18.7 Nothing in these Supplier Terms restricts the Buyer from sharing information relating to the Service with any other Contracting Authority, the National Audit Office, the Cabinet Office, the Government Commercial Agency, its auditors, or Parliament.

## 19. Liability

- 19.1 Liability is governed by the Call-Off Contract. **These Supplier Terms do not vary, cap, exclude or qualify the liability provisions of the Call-Off Contract in any respect.**
- 19.2 Nothing in these Supplier Terms excludes or limits either party's liability for death or personal injury caused by negligence, for fraud or fraudulent misrepresentation, or for any other liability that cannot lawfully be excluded or limited.
- 19.3 **The Supplier does not seek to exclude or limit its liability** for breach of the Data Protection Legislation, breach of its confidentiality obligations, or breach of clause 10 (Buyer Data), clause 12 (Data residency), clause 13 (Security) or clause 14 (Artificial intelligence), beyond any limitation that applies under the Call-Off Contract.
- 19.4 **No contractual limitation period applies.** The parties' rights to bring a claim are governed by the Limitation Act 1980. Nothing in these Supplier Terms shortens that period.
- 19.5 Service Credits are not the Buyer's sole or exclusive remedy, as set out at clause 5.4. Service Credits paid in respect of a failure may be set off against damages recovered for the same failure, so that there is no double recovery.

## 20. Insurance

- 20.1 The Supplier maintains, with a reputable insurer, insurance of at least: **£1,000,000 professional indemnity; £1,000,000 public liability; and £5,000,000 employers' liability**, meeting or exceeding the minimum levels required by the Framework Agreement for Lots 2b and 3.
- 20.2 The Supplier shall maintain that insurance throughout the term and **for a period of six years after** expiry or termination.
- 20.3 The Supplier shall provide evidence of cover, including certificates and a broker's letter, within 5 Working Days of the Buyer's request, at no charge.

- 20.4 The Supplier shall notify the Buyer in writing within 10 Working Days of any cancellation, lapse, material reduction or material change to its insurance arrangements.** The Supplier does not reserve any right to change its insurance without telling the Buyer.
- 20.5** Where the Order Form requires higher levels of cover, the Supplier shall obtain and maintain them before the Service Commencement Date.

## **21. Warranties**

- 21.1** The Supplier warrants that the Service shall conform in all material respects to the Service Definition and the documentation, and shall be provided with the reasonable skill and care to be expected of a competent supplier of similar services by appropriately qualified and experienced personnel.
- 21.2** The Supplier warrants that it shall use Good Industry Practice to ensure the Service is free from malicious code, and shall scan releases before deployment.
- 21.3** The Supplier warrants that it has full authority to enter into the Call-Off Contract, that its licence to the Platform under the IBM Embedded Solution Agreement is valid and in good standing, and that it is not aware of anything that would prevent it performing its obligations.
- 21.4** Where the Service does not conform to clause 21.1, the Supplier shall correct the non-conformity at no charge and within a reasonable time. This is in addition to, and does not limit or replace, the Buyer's rights and remedies under the Call-Off Contract or at law.
- 21.5** **These Supplier Terms do not exclude any warranty, condition or term implied by statute or common law**, save to the extent the Call-Off Contract expressly permits. In particular, the Supplier does not purport to exclude the implied terms as to satisfactory quality, fitness for purpose or reasonable skill and care.

### ***Inclusions summary***

*The following table summarises clause 16.8 and the clauses referred to in it. It is provided for reference and does not vary the operative provisions.*

| <b>Item</b>                                                          | <b>Position</b>                                         | <b>Clause</b> |
|----------------------------------------------------------------------|---------------------------------------------------------|---------------|
| Platform subscription, hosting and underlying infrastructure         | Included in the Charges                                 | 16.8          |
| Support at every severity, including 24/7/365 cover for Severity 1   | Included in the Charges                                 | 6.4 · A.4.5   |
| Software updates, patches and new releases of ordered functionality  | Included in the Charges                                 | 16.8          |
| At least one non-production environment                              | Included in the Charges                                 | 4.5           |
| Single sign-on, multi-factor authentication and access audit trail   | Included in the Charges                                 | 4.3           |
| Monthly service reporting and quarterly service review               | Included in the Charges                                 | A.6           |
| Responses to security questionnaires and assurance requests          | Included in the Charges                                 | 16.8          |
| Co-operation with audits, and the Buyer's own security testing       | Included in the Charges                                 | 9.3 · 13.6    |
| Data protection impact assessment and data subject rights assistance | Included in the Charges                                 | 11.4 · B.5    |
| Accessibility audit report and penetration test executive summary    | Included in the Charges                                 | 15.4 · C.4    |
| Data export, and up to 20 person-days of exit assistance             | Included in the Charges                                 | 23.3 · 23.8   |
| Implementation Services                                              | <b>Chargeable</b> — only where stated in the Order Form | 3.3           |
| Managed and Advisory Services                                        | <b>Chargeable</b> — only where stated in the Order Form | 3.4           |
| Additional modules or user entitlements                              | <b>Chargeable</b> — only where stated in the Order Form | 4.2           |
| Exit assistance beyond 20 person-days                                | <b>Chargeable</b> — at the rates in the Order Form      | 23.8          |

---

## PART E

### Term, change and exit

---

#### 22. Term, suspension and termination

- 22.1 The term is as set out in the Order Form, subject to the maximum permitted by the Framework Agreement.
- 22.2 **The Call-Off Contract does not renew automatically.** It expires at the end of its term unless the parties expressly agree otherwise in writing. The Buyer need take no action to prevent renewal.
- 22.3 The Buyer's rights to terminate, in whole or in part, are those set out in the Call-Off Contract and are not limited or qualified by these Supplier Terms.
- 22.4 **The Supplier shall not terminate the Call-Off Contract for convenience.** The Supplier may terminate only where: (a) the Buyer is in material breach and has failed to remedy it within 30 days of written notice; (b) undisputed sums remain unpaid more than 60 days after the due date and after two written reminders; or (c) the Buyer is insolvent, to the extent termination is permitted by the Call-Off Contract.
- 22.5 The Supplier may suspend the Service only where necessary to address a material and imminent security risk, to prevent unlawful use causing imminent harm, or to comply with a binding legal requirement. Any suspension shall be no wider and no longer than strictly necessary. The Supplier shall give notice before suspending where it is safe to do so, and immediately afterwards where it is not, shall keep the Buyer informed, and shall restore the Service as soon as the cause is resolved. **The Supplier shall not suspend the Service for non-payment of disputed sums.**
- 22.6 The Supplier shall not withdraw the Service during the term. If the Supplier decides to withdraw the Service at the end of a term, it shall give at least **12 months' written notice**, shall continue to provide the Service for the remainder of the term, and shall provide migration assistance under clause 23 at no charge.
- 22.7 On expiry or termination the Supplier shall refund, pro rata, any Charges paid in advance for Services not provided. **The Supplier shall not levy breakage costs, unrecovered costs, or any other early termination charge** where the Buyer terminates for the Supplier's default or in exercise of a right under the Call-Off Contract.

#### 23. Exit management and data portability

- 23.1 The Supplier shall comply with the exit management provisions of the Call-Off Contract. This clause 23 supplements them.
- 23.2 **The Supplier shall provide an exit plan to the Buyer on request at any time during the term, at no charge, and shall keep it current.** The Buyer does not have to serve a termination notice in order to obtain one.
- 23.3 On the Buyer's request at any time, and in any event on expiry or termination, the Supplier shall provide the **complete** Buyer Data — including all records, configuration, attachments, workflow history and audit trails — in open, documented, machine-readable formats (CSV, JSON or XML for structured data, and native format for attached documents), together with a data dictionary describing the structure, **within 10 Working Days and at no charge.**
- 23.4 The Buyer may also export its own data through self-service functionality at any time during the term, without notice to or assistance from the Supplier.
- 23.5 The Supplier shall retain Buyer Data for 30 days after expiry or termination so that the Buyer can verify the completeness of the export, and shall then securely delete it.
- 23.6 The Supplier shall securely delete all Buyer Data from all systems, including backups, in accordance with Good Industry Practice, and shall provide a **written certificate of deletion signed by an authorised officer within 15 Working Days** of the Buyer's request.
- 23.7 Where the Supplier is required by law to retain any Buyer Data, it shall tell the Buyer what is retained, on what legal basis, and for how long. Retained data remains subject to the confidentiality, security and residency

obligations in these Supplier Terms and shall be deleted as soon as the requirement ends. **The Supplier does not reserve any right to retain copies of Buyer Data for its own records.**

**23.8** The Supplier shall provide up to **20 person-days** of exit and migration assistance at no charge, including reasonable co-operation with any replacement supplier. Assistance beyond that is charged at the rates in the Order Form.

**23.9** **The Supplier shall not make the return of Buyer Data conditional on payment of any sum, disputed or otherwise, or on the resolution of any dispute.**

## **24. Change control**

**24.1** Changes to the Call-Off Contract are made using the variation procedure in the Call-Off Contract.

**24.2** The Supplier may make changes to the Service in the ordinary course, **provided that no change shall degrade the security, functionality, performance, accessibility or data protection characteristics of the Service.** Changes shall be made to add features, improve or clarify existing commitments, correct defects, or maintain alignment with current security standards or applicable law.

**24.3** The Supplier shall give at least **30 days' written notice** of any change that materially affects the Buyer's use of the Service, its integrations, or its assurance position. Where a change has a material adverse effect, the Buyer may terminate the affected Service without penalty on notice given within 60 days of becoming aware of the effect.

**24.4** The Supplier may make emergency changes required to address a security vulnerability without prior notice, and shall inform the Buyer within 24 hours of doing so.

**24.5** **These Supplier Terms cannot be varied unilaterally.** No change to these Supplier Terms takes effect in relation to an existing Call-Off Contract unless agreed in writing by both parties. **Publication of a revised version of these Supplier Terms, or of any policy, standard or document referred to in them, has no effect on an existing Call-Off Contract.**

**24.6** **No term of this agreement is incorporated by reference to a website.** All of the Supplier's terms are contained in this document and its Annexes. Where a URL appears, it is for information only and does not form part of the contract.

## **25. Sub-contracting and supply chain**

**25.1** The Supplier remains fully responsible to the Buyer for the acts and omissions of its sub-contractors and sub-processors as if they were its own.

**25.2** **The Service is built on the IBM OpenPages platform, licensed to the Supplier under an IBM Embedded Solution Agreement. The Supplier contracts with the Buyer as prime contractor and is solely responsible to the Buyer for the Service.** The Buyer has no contractual relationship with IBM, is not required to accept or be bound by any IBM terms, and no IBM term limits the Supplier's obligations to the Buyer under the Call-Off Contract or these Supplier Terms.

**25.3** Key sub-contractors and all sub-processors are named at paragraph B.7. The Supplier shall comply with the Call-Off Contract provisions relating to key sub-contractors.

**25.4** The Supplier shall give at least 30 days' written notice before appointing, replacing or removing a sub-processor. The Buyer may object on reasonable grounds, and if the objection cannot be resolved the Buyer may terminate the affected Service without penalty and without liability for early termination charges.

**25.5** The Supplier shall impose on every sub-contractor and sub-processor obligations no less protective than those in these Supplier Terms, including as to data protection, security, UK data residency, personnel location and the artificial intelligence commitments in clause 14.

**25.6** The Supplier complies with the Modern Slavery Act 2015, pays its own supply chain within 30 days, and requires Cyber Essentials certification from any sub-contractor with access to Buyer Data.

## 26. Staff

- 26.1 The staff transfer provisions of the Call-Off Contract apply. The parties do not anticipate that the Transfer of Undertakings (Protection of Employment) Regulations 2006 shall apply on commencement of the Platform Services.
- 26.2 On expiry or termination, the Supplier shall provide the employee liability information required by the Call-Off Contract and co-operate fully with the Buyer and any replacement supplier. **The Supplier does not seek an indemnity from the Buyer in respect of TUPE.**
- 26.3 All Supplier personnel with access to Buyer Data are screened to Baseline Personnel Security Standard as a minimum, and to any higher standard required by the Order Form, before access is granted.
- 26.4 The Supplier complies with its obligations in respect of right to work, and with the off-payroll working rules where they apply.
- 26.5 The Supplier shall procure that the personnel of any subcontractor or sub-processor with access to Buyer Data are screened to a standard no lower than that required of the Supplier's own personnel under clause 26.3, and shall evidence that screening to the Buyer on request.

## 27. Sustainability and social value

- 27.1 The Supplier publishes a Carbon Reduction Plan meeting the requirements of applicable government procurement policy, and shall provide it to the Buyer on request.
- 27.2 The Supplier is committed to achieving net zero by **2030** and reports annually on progress.
- 27.3 The Supplier shall deliver and report on any social value commitments recorded in the Order Form.
- 27.4 The Supplier shall provide, on request and at no charge, information on the energy and carbon intensity attributable to the Buyer's use of the Service, to support the Buyer's own reporting.
- 27.5 The Supplier applies sustainable operating practices to the delivery of the Service, including the right-sizing of compute and storage, the scheduled suspension of non-production environments outside working hours, the retirement of unused resources, and a preference for the lowest-carbon United Kingdom region consistent with the residency commitment at clause 12.1.
- 27.6 The Supplier shall report annually to the Buyer, at no charge, on the measures taken under clause 27.5 and on their measured effect.
- 27.7 The Supplier shall comply with the applicable Call-Off Schedule relating to sustainability, and shall provide the information the Buyer reasonably requires in order to discharge its own environmental reporting obligations, including under the Greening Government Commitments where those apply to the Buyer.

### **Exit sequence**

*The following table summarises the operation of clauses 22 and 23. It is provided for reference and does not vary the operative provisions.*

| Stage                   | When                                   | What the Supplier does                                                                                    | Clause |
|-------------------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------|--------|
| Exit plan               | At any time on request during the Term | Provides and maintains a current exit plan, at no charge, without any termination notice being required   | 23.2   |
| Notice served           | Day 0                                  | Confirms the exit plan and nominates an exit lead                                                         | 23.1   |
| Data export             | Within 10 Working Days of request      | Provides the complete Buyer Data in CSV, JSON or XML with attachments and a data dictionary, at no charge | 23.3   |
| Self-service export     | At any time                            | Available to the Buyer without notice to or assistance from the Supplier                                  | 23.4   |
| Migration support       | Throughout the exit period             | Up to 20 person-days at no charge, including co-operation with any replacement supplier                   | 23.8   |
| Service ends            | Expiry or termination date             | Access ceases; prepaid Charges for services not provided are refunded pro rata                            | 22.7   |
| Verification window     | 30 days after the end date             | Buyer Data is retained so that the Buyer may verify the completeness of the export                        | 23.5   |
| Secure deletion         | After the verification window          | All Buyer Data is securely deleted from all systems, including backups                                    | 23.6   |
| Certificate of deletion | Within 15 Working Days of request      | Written certificate signed by an authorised officer                                                       | 23.6   |

#### **No condition may be attached to the return of Buyer Data**

The Supplier shall not make the return of Buyer Data conditional upon payment of any sum, disputed or otherwise, or upon the resolution of any dispute, and shall not levy any charge for the standard export described at clause 23.3. See clauses 23.9 and 16.6.

---

## PART F

### General provisions

---

#### 28. General

- 28.1 Notices.** Notices must be in writing and sent to the addresses in the Order Form. Email is valid service for all notices other than notices of termination or of a dispute, which must also be sent by post.
- 28.2 Assignment.** The Supplier may not assign, novate or otherwise transfer the Call-Off Contract or any part of it without the Buyer's prior written consent. The Buyer may assign or novate to any Contracting Authority in accordance with the Call-Off Contract.
- 28.3 Entire agreement.** The Call-Off Contract, including these Supplier Terms, is the entire agreement between the parties in relation to the Service. This clause does not exclude liability for fraudulent misrepresentation.
- 28.4 No waiver.** A failure or delay in exercising a right is not a waiver of it.
- 28.5 Third party rights.** A person who is not a party has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term, except as the Call-Off Contract expressly provides.
- 28.6 Disputes.** Disputes are resolved in accordance with the dispute resolution procedure in the Call-Off Contract. The parties shall first attempt resolution by escalation between senior representatives. **These Supplier Terms do not require arbitration, do not require any dispute to be heard outside England and Wales, and do not impose any pre-condition on the Buyer's access to the courts.**
- 28.7 Governing law and jurisdiction.** These Supplier Terms and any dispute arising out of them are governed by the law of England and Wales, and the courts of England and Wales have exclusive jurisdiction.
- 28.8 Compliance with law.** The Supplier complies with all applicable law, including the Bribery Act 2010, the Modern Slavery Act 2015, the Equality Act 2010, the Data Protection Act 2018 and the Procurement Act 2023, and maintains policies and training to support that compliance.
- 28.9 Conflicts of interest.** The Supplier shall notify the Buyer promptly of any actual or potential conflict of interest and shall not proceed with affected work until the Buyer is content.
- 28.10 Independent contractor.** The Supplier is an independent contractor. Nothing in these Supplier Terms creates a partnership, joint venture, agency or employment relationship.
- 28.11 Survival.** Clauses which by their nature are intended to survive expiry or termination do so, including clauses 10, 12, 13, 14, 17, 18, 19, 20 and 23.
- 28.12 Execution.** These Supplier Terms may be accepted electronically and take effect on the Buyer placing an Order.
- 28.13 No indemnity from the Buyer.** For the avoidance of doubt, **no provision of these Supplier Terms requires or purports to require the Buyer to indemnify the Supplier, or any other person, in respect of anything.**
- 28.14 Enquiries and amendment.** Any enquiry in respect of these Supplier Terms may be addressed to the Supplier at legal@cyberfortis.co.uk, and the Supplier shall respond within 5 Working Days. Where the Buyer is unable to accept any provision of these Supplier Terms, the Supplier shall consider in good faith the amendment or disapplication of that provision by means of the Order Form.

## Service levels, Service Credits and support

### A.1. Application

**A.1.1** This Annex applies to the Platform Services. It sets out binding commitments, not targets. Where the Order Form specifies different or additional service levels, the Order Form prevails.

### A.2. Availability

**A.2.1 The Supplier shall achieve Availability of at least 99.9% in each calendar month.**

**A.2.2** Availability is calculated as:

$$\text{Availability \%} = (T - E - D) \div (T - E) \times 100$$

where **T** is the total minutes in the calendar month, **E** is Excluded Minutes, and **D** is Downtime Minutes.

**A.2.3 Downtime** means any period during which the Service is unavailable to Authorised Users, or during which a core function of the Service cannot be used for its intended purpose and no workaround is available.

**A.2.4 Measurement.** Availability is measured by independent external monitoring, at intervals of no more than 60 seconds, from at least three separate United Kingdom locations, against a synthetic transaction that exercises authentication and the retrieval of a record — not a simple network reachability check. The Supplier shall make the measurement data available to the Buyer on request at no charge.

**A.2.5 Excluded Minutes** are, and are only:

- (a) planned maintenance carried out in accordance with paragraph A.2.6;
- (b) unavailability caused directly by the Buyer's act or omission, or by the Buyer's own network or equipment;
- (c) a Force Majeure Event as defined in the Call-Off Contract; and
- (d) a Platform Event, subject to paragraph A.2.8.

**A.2.6 Planned maintenance** shall not exceed **8 hours in any calendar month**, shall be notified at least **5 Working Days** in advance, and shall be carried out outside 07:00 to 20:00 UK time on Working Days. Emergency maintenance required to address a security vulnerability may be carried out at any time, shall be notified as soon as practicable, and shall not exceed 4 hours in any calendar month.

**A.2.7** Time outside these limits is not Excluded and counts as Downtime.

### *The Platform Event carve-out, and the limits on it*

**A.2.8** FortisOne GRC is built on the IBM OpenPages Platform. A Platform Event — unavailability caused solely by the Platform or underlying cloud infrastructure, which the Supplier could not have prevented by exercising Good Industry Practice — is excluded from the Service Credit calculation. **That exclusion is subject to all of the following, each of which is a binding commitment:**

- (a) the Supplier shall report every Platform Event to the Buyer in the monthly service report, with duration and root cause, **whether or not it affects Service Credits**;
- (b) the Supplier shall pursue all remedies available to it under the IBM Embedded Solution Agreement and **shall pass through to the Buyer, in full, any service credit or compensation it recovers** attributable to the Buyer's Service;
- (c) the Supplier shall not classify an event as a Platform Event without providing evidence of root cause if the Buyer asks for it;
- (d) **if Platform Events cause measured availability to fall below 99.0% in any month, or occur in three consecutive months, the Buyer may terminate the affected Service without penalty**, without liability for early termination charges, and with a pro rata refund of prepaid Charges; and

- (e) the exclusion does not apply where the Supplier failed to implement a resilience, failover or configuration measure that was available to it.

**A.2.9** Paragraph A.2.8 shall be construed so as to give effect to the ability of the Buyer to verify the existence and cause of any Platform Event and, where the thresholds at paragraph A.2.8(d) are met, to terminate in consequence of it. The exclusion at paragraph A.2.5(d) shall not be construed so as to defeat that ability.

### **A.3. Service Credits**

**A.3.1** Where Availability in a calendar month is below 99.9%, the Buyer is entitled to a Service Credit calculated as a percentage of the Charges for that month for the affected Service:

| <b>Availability achieved in the month</b> | <b>Service Credit</b>     |
|-------------------------------------------|---------------------------|
| 99.9% or above                            | None                      |
| 99.00% to below 99.90%                    | 5% of the monthly Charge  |
| 98.00% to below 99.00%                    | 10% of the monthly Charge |
| 95.00% to below 98.00%                    | 20% of the monthly Charge |
| Below 95.00%                              | 30% of the monthly Charge |

**A.3.2 Service Credits are applied automatically.** The Supplier shall calculate them, state them in the monthly service report, and credit them against the next invoice. The Buyer is not required to claim, to submit evidence, or to meet any minimum threshold or de minimis.

**A.3.3** Where the Call-Off Contract ends before a Service Credit is applied, the Supplier shall pay it to the Buyer as a refund within 30 days.

**A.3.4 Service Credits are not the Buyer's sole or exclusive remedy,** and do not limit the Buyer's rights under the Call-Off Contract or at law. Service Credits paid for a failure may be set off against damages recovered for the same failure.

**A.3.5** Failure to meet the Availability commitment in two months within any rolling six-month period is a material breach for the purposes of the Call-Off Contract.

## A.4. Support and incident management

**A.4.1** The Supplier shall provide support in accordance with the following matrix. Times to respond and resolve run from the Supplier's receipt of the incident.

| Severity     | Definition                                                                                                                                                    | Hours         | Respond        | Update               | Workaround     | Resolve                  |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|----------------|----------------------|----------------|--------------------------|
| 1 — Critical | Service wholly unavailable; or data integrity or security compromised; or a core function unusable with no workaround, affecting all or most Authorised Users | 24 / 7 / 365  | 30 min         | Hourly               | 4 hours        | 8 hours                  |
| 2 — High     | A major function is significantly impaired or unavailable, affecting many users, with no straightforward workaround                                           | Support Hours | 2 hours        | Daily                | 1 Working Day  | 5 Working Days           |
| 3 — Medium   | A function is impaired for a limited number of users, and a workaround is available                                                                           | Support Hours | 8 hours        | Every 3 Working Days | 5 Working Days | Next scheduled release   |
| 4 — Low      | Minor or cosmetic issue, question, or service request with no material operational impact                                                                     | Support Hours | 2 Working Days | Weekly               | n/a            | As agreed with the Buyer |

**A.4.2 The Buyer sets the initial severity.** The Supplier may propose a reclassification with reasons, but where the Buyer has assigned Severity 1 the Supplier shall respond at Severity 1 while any disagreement is resolved.

**A.4.3** Support is available through the service desk portal and by electronic mail at all times, and by telephone for Severity 1 incidents on the number published in the service desk portal and notified to the Buyer in writing on or before the Service Commencement Date. The Supplier shall notify the Buyer in writing of any change to that number.

**A.4.4** For every Severity 1 incident the Supplier shall provide a written post-incident report, including root cause and preventive action, **within 10 Working Days at no charge.**

**A.4.5** Support is included in the Charges. The Supplier does not charge for incident diagnosis, defect correction, service requests or advice on correct use of the Service.

## A.5. Escalation

| Level | Contact                                     | Escalate after (Severity 1) | Escalate after (other) |
|-------|---------------------------------------------|-----------------------------|------------------------|
| 1     | Service desk                                | On raising                  | On raising             |
| 2     | Service Manager — John D.                   | 2 hours                     | 1 Working Day          |
| 3     | Head of Service Delivery — Gulzar Khan      | 4 hours                     | 3 Working Days         |
| 4     | Global Managing Director — Kateryna Sporysh | 8 hours                     | 5 Working Days         |

**A.5.1** The Buyer may escalate at any time without waiting for these periods to elapse.

## A.6. Service reporting and review

- A.6.1** Within 5 Working Days of the end of each month the Supplier shall provide, at no charge, a service report covering: measured Availability and the calculation; every incident with severity, duration and resolution; Service Credits due; planned and emergency maintenance undertaken; Platform Events; security incidents and vulnerability remediation status; and forthcoming changes.
- A.6.2** The Supplier shall hold a service review with the Buyer at least quarterly, at no charge.
- A.6.3** The Supplier shall review service levels annually with the Buyer and **shall not propose any reduction to the commitments in this Annex** during the term.

## A.7. Worked example of the Availability calculation

The following worked example illustrates the calculation prescribed at paragraph A.2.2. It is illustrative only and does not vary the commitment at paragraph A.2.1.

| Step                                                                 | Basis                                        | Value             |
|----------------------------------------------------------------------|----------------------------------------------|-------------------|
| Total minutes in the calendar month (T)                              | 30-day month $\times 24 \times 60$           | 43,200            |
| Planned maintenance, notified in accordance with paragraph A.2.6 (E) | Within the 8-hour monthly limit              | 240               |
| Measured Downtime (D)                                                | One Severity 1 incident, externally measured | 55                |
| Measurable minutes (T – E)                                           | $43,200 - 240$                               | 42,960            |
| Availability                                                         | $(42,960 - 55) \div 42,960 \times 100$       | <b>99.872%</b>    |
| Band applicable under paragraph A.3.1                                | 99.00% to below 99.90%                       | —                 |
| Service Credit due                                                   | Percentage of the monthly Charge             | <b>5%</b>         |
| How it is applied                                                    | Automatically, against the next invoice      | No claim required |

- A.7.1** In the example above the Supplier would additionally record the incident, its duration, its root cause and the resulting Service Credit in the monthly service report required by paragraph A.6.1, and would provide a written post-incident report under paragraph A.4.4.
- A.7.2** Had the 55 minutes of Downtime been attributable solely to a Platform Event, no Service Credit would arise, but the event would still be reported under paragraph A.2.8(a) and would count towards the termination thresholds at paragraph A.2.8(d).

## A.8. Service management calendar

The following activities are performed at the stated frequency at no charge to the Buyer.

| Activity                                                                                  | Frequency                                                   | Performed by       | Paragraph |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------|--------------------|-----------|
| Service report: availability, incidents, Service Credits, maintenance and Platform Events | Monthly, within 5 Working Days of month end                 | Supplier           | A.6.1     |
| Service review meeting                                                                    | Quarterly                                                   | Supplier and Buyer | A.6.2     |
| Backup restore test                                                                       | Quarterly                                                   | Supplier           | 7.3       |
| Privileged access review, evidenced to the Buyer on request                               | Quarterly                                                   | Supplier           | C.2       |
| Business continuity and disaster recovery test, with summary provided                     | Annually                                                    | Supplier           | 7.1       |
| Independent penetration test by a CREST-accredited supplier                               | Annually                                                    | Supplier           | C.4.1     |
| Review of the service levels in this Annex                                                | Annually                                                    | Supplier and Buyer | A.6.3     |
| Buyer audit of compliance with these Supplier Terms                                       | Once per contract year, and following any Security Incident | Buyer              | 13.6      |
| Confirmation of the sub-processor list                                                    | On request, and 30 days before any change                   | Supplier           | B.7       |

- A.8.1** The Supplier shall give the Buyer not less than 10 Working Days' notice of any activity in this calendar which requires the Buyer's participation, and shall propose alternative dates where the Buyer is unable to attend.
- A.8.2** Where an activity is not completed within its stated frequency, the Supplier shall record that fact, the reason for it and the revised date in the next monthly service report under paragraph A.6.1.
- A.8.3** The outputs of each activity in this calendar form part of the assurance evidence available to the Buyer under paragraph C.8.

---

## ANNEX B

### Data processing annex

---

This Annex sets out the provisions required by Article 28(3) of the UK GDPR in respect of the processing of Personal Data by the Supplier on behalf of the Buyer. Where the Call-Off Contract contains a data processing schedule, that schedule shall prevail, and this Annex shall supplement it to the extent that it confers additional protection upon the Buyer.

#### B.1. Roles

**B.1.1** The Buyer is the Controller. The Supplier is the Processor. The Supplier does not determine the purposes or means of processing Buyer Data and shall not act as a Controller in respect of it.

#### B.2. Details of processing

|                                   | Detail                                                                                                                                                                                                                         |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Subject matter</b>             | Provision of the FortisOne GRC governance, risk and compliance service, and any Implementation or Managed and Advisory Services ordered                                                                                        |
| <b>Duration</b>                   | The term of the Call-Off Contract, plus the 30-day verification period at clause 23.5                                                                                                                                          |
| <b>Nature and purpose</b>         | Hosting, storage, structuring, retrieval, display, backup, transmission and deletion of Buyer Data, solely to deliver the Service                                                                                              |
| <b>Types of Personal Data</b>     | Names, job titles, business contact details, organisational unit and system identifiers of Authorised Users; and any Personal Data the Buyer chooses to include within risk, control, incident, assessment or evidence records |
| <b>Categories of Data Subject</b> | The Buyer's employees, workers, contractors and officers; and any individual referenced in records the Buyer uploads                                                                                                           |
| <b>Special category data</b>      | Not required by the Service. The Buyer should not upload special category or criminal offence data unless expressly agreed in the Order Form and a DPIA has been completed                                                     |

#### B.3. Supplier obligations

- B.3.1** The Supplier shall process Personal Data only on the Buyer's documented instructions, which are these Supplier Terms and the Order Form, unless required otherwise by law — in which case it shall inform the Buyer first, unless the law prohibits it.
- B.3.2** The Supplier shall ensure that persons authorised to process Personal Data are subject to binding confidentiality obligations and have received data protection training.
- B.3.3** The Supplier shall implement the technical and organisational measures set out in Annex C.
- B.3.4** The Supplier shall make available all information necessary to demonstrate compliance with Article 28, and shall submit to audits under clause 13.6. **The Supplier does not restrict the Buyer's audit rights to a meeting or a written response.**

#### B.4. Personal data breach

- B.4.1** **The Supplier shall notify the Buyer within 24 hours of becoming aware of a Personal Data Breach affecting Buyer Data.** Notification is not conditional on the Buyer asking, on the Supplier completing its investigation, or on the breach being confirmed as reportable.
- B.4.2** The notification shall describe, so far as known at the time: the nature of the breach; the categories and approximate number of Data Subjects and records affected; the likely consequences; the measures taken or

proposed; and a named contact. The Supplier shall provide updates as the investigation progresses and a full written report within 10 Working Days.

- B.4.3** The Supplier shall assist the Buyer, at no charge, with any notification to the Information Commissioner or to Data Subjects, and shall not make any such notification itself without the Buyer's prior written agreement.

## **B.5. Assistance**

- B.5.1** The Supplier shall assist the Buyer, at no charge and within 5 Working Days of request, with: responding to Data Subject rights requests; data protection impact assessments; prior consultation with the Information Commissioner; and the Buyer's records of processing.
- B.5.2** Where the Supplier receives a request directly from a Data Subject, it shall not respond substantively but shall refer the request to the Buyer within 2 Working Days.

## **B.6. International transfers**

- B.6.1** **There are no international transfers.** All processing takes place within the United Kingdom, in accordance with clause 12. If a transfer ever becomes necessary the process at clause 12.2 applies.

## **B.7. Sub-processors**

- B.7.1** The Buyer gives general written authorisation for the Supplier to appoint the sub-processors listed below. The Supplier shall notify the Buyer at least 30 days before appointing, replacing or removing any sub-processor, and the Buyer may object under clause 25.4.

| <b>Sub-processor</b>                              | <b>Purpose</b>                                                                                     | <b>Location</b>                                 | <b>Access to Buyer Data</b>                                                                                                                               |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IBM United Kingdom Limited</b>                 | Supply and maintenance of the IBM OpenPages platform software under an Embedded Solution Agreement | United Kingdom                                  | No access to the production environment or to Buyer Data. Software supply and Level 3 code defect support only, provided on anonymised reproduction cases |
| <b>Amazon Web Services EMEA SARL</b>              | Hosting of the production, backup and disaster recovery environments                               | United Kingdom only — London region (eu-west-2) | Encrypted data at rest under keys controlled by the Supplier. No AWS personnel access to plaintext Buyer Data                                             |
| <b>Amazon Web Services EMEA SARL (Amazon SES)</b> | System notifications and alerts to Authorised Users                                                | United Kingdom — London region (eu-west-2)      | Name and business email address of Authorised Users only                                                                                                  |
| <b>IBM United Kingdom Limited (watsonx)</b>       | Model inference for AI Features, where enabled by the Buyer                                        | United Kingdom                                  | Zero retention. Prompt content only, for the duration of the request. No training, no storage, no human review                                            |

- B.7.2** The Supplier shall impose on each sub-processor, by written contract, obligations no less protective than those in this Annex, and remains fully liable to the Buyer for each sub-processor's performance.
- B.7.3** A current list of sub-processors is maintained and provided to the Buyer on request. **The list is not maintained by reference to a website and cannot be changed without notice under clause 25.4.**

## B.8. Return and deletion

**B.8.1** Return and deletion of Personal Data is governed by clause 23, including the certificate of deletion at clause 23.6 and the position on retained copies at clause 23.7.

## B.9. Retention schedule

The following retention periods apply. All retention is within the United Kingdom in accordance with clause 12.1.

| Category of data                                              | Retention period                                                                                                     | Clause      |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|-------------|
| Buyer Data held in the production environment                 | The Term                                                                                                             | 12.1        |
| Backups of Buyer Data                                         | 35 days on a rolling basis, then overwritten                                                                         | 7.3         |
| Buyer Data following expiry or termination                    | 30 days for verification, then securely deleted                                                                      | 23.5 · 23.6 |
| System and application logs, including privileged access logs | Not less than 12 months                                                                                              | 12.5        |
| Audit trail of user, configuration and AI-assisted actions    | Not less than 12 months, exportable by the Buyer at any time                                                         | 14.6        |
| Support tickets and diagnostic material containing Buyer Data | 24 months, then deleted                                                                                              | 12.1        |
| Business contact details of Authorised Users                  | The Term, then deleted with the Buyer Data                                                                           | B.2         |
| Any data retained under a legal obligation                    | Only for so long as the obligation subsists, then deleted; the Buyer is told what is retained, why, and for how long | 23.7        |

## B.10. Records of processing

**B.10.1** The Supplier maintains a record of all categories of processing carried out on behalf of the Buyer, in accordance with Article 30(2) of the UK GDPR, and shall provide that record to the Buyer on request at no charge.

**B.10.2** The record includes the identity and contact details of the Supplier and of each sub-processor, the categories of processing, the location of processing, the applicable retention periods, and a general description of the technical and organisational measures set out at Annex C.

**B.10.3** The Supplier shall notify the Buyer of any material change to that record within 10 Working Days of the change taking effect.

**B.10.4** The Supplier shall appoint and maintain a point of contact for data protection matters, and shall notify the Buyer of the identity of that person and of any change to it.

## Security and assurance statement

This Annex records the security and assurance position of the Supplier, to the intent that the Buyer may discharge its assurance obligations without recourse to a separate questionnaire. **Each statement contained in this Annex is a term of the Call-Off Contract and is warranted by the Supplier to be accurate as at the date of issue.** Evidence in support of each statement shall be provided to the Buyer upon request and at no charge.

### C.1. Certifications: who holds what

#### The most important paragraph in this Annex

FortisOne GRC is built on the IBM OpenPages platform. IBM holds certifications for that platform. **Those are IBM's certifications. They are not certifications of the Supplier, and the Supplier does not present them as its own.** The table below states which party holds each certification and its current status. Where the Supplier relies on the Platform's assurance, it says so.

| Certification                       | Held by                        | Scope                                                     | Status                                                                                                                |
|-------------------------------------|--------------------------------|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Cyber Essentials Plus               | Cyberfortis Consulting Limited | Cyberfortis corporate IT and service delivery environment | <b>Held</b> — valid to August 2027. Certificate provided to the Buyer on request                                      |
| ISO/IEC 27001                       | —                              | —                                                         | <b>Not held.</b> The Supplier is not certified and does not claim to be. See paragraph C.1.1                          |
| ISO 9001                            | Cyberfortis Consulting Limited | Quality management system                                 | <b>In progress</b> — certification not yet awarded                                                                    |
| ISO/IEC 20000-1                     | —                              | —                                                         | <b>Not held.</b> The Supplier does not claim it                                                                       |
| SOC 2 Type II                       | —                              | —                                                         | Not held. The Supplier does not claim it                                                                              |
| ISO/IEC 27001, 27017, 27018         | IBM                            | IBM OpenPages platform                                    | Held by IBM. Evidence of IBM's current certification available on request. <b>Not a certification of the Supplier</b> |
| Cloud infrastructure certifications | Amazon Web Services            | AWS London region (eu-west-2)                             | Held by AWS. <b>Not a certification of the Supplier</b>                                                               |

**C.1.1 The Supplier is not certified to ISO/IEC 27001 and makes no claim to be certified.** It operates an information security management system designed to the requirements of that standard, comprising a documented policy set reviewed annually, a maintained risk register, an internal audit programme, a named security lead reporting to the board, and a documented incident management process. **The Buyer may inspect that evidence under clause 13.6 and is invited to do so, in place of reliance upon a certificate.**

**C.1.2** The Supplier shall notify the Buyer within 10 Working Days if any certification recorded in this table is awarded, lapses, is suspended or is withdrawn, and shall provide an updated version of this Annex.

**C.1.3** The Supplier shall not represent, in any tender, proposal or marketing material, that it holds a certification which is recorded in this table as not held.

## C.2. NCSC Cloud Security Principles

The Service is assessed against the National Cyber Security Centre's 14 Cloud Security Principles as follows.

| Principle                                 | How the Service meets it                                                                                                                                                                                                                               |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1. Data in transit protection</b>      | TLS 1.2 minimum, TLS 1.3 preferred, for all external and internal service-to-service traffic. HSTS enforced. Certificates managed and monitored for expiry. No unencrypted protocol is available                                                       |
| <b>2. Asset protection and resilience</b> | All Buyer Data held in the United Kingdom (clause 12). AES-256 encryption at rest. Daily encrypted backups retained 35 days, restore-tested quarterly. RPO 1 hour, RTO 4 hours. Secure media sanitisation on disposal                                  |
| <b>3. Separation between users</b>        | Logical separation of tenants enforced at application and data layers. Cross-tenant access is not technically possible through the application. Separation is tested as part of the annual penetration test                                            |
| <b>4. Governance framework</b>            | Named security lead accountable to the board. Documented policy set reviewed at least annually. Security risks recorded on a maintained risk register with owners and treatment plans                                                                  |
| <b>5. Operational security</b>            | Vulnerability scanning of infrastructure and application; protective monitoring with alerting; formal configuration and change management; documented incident management process tested annually                                                      |
| <b>6. Personnel security</b>              | All personnel with access to Buyer Data screened to BPSS as a minimum, with identity, right to work, employment history and unspent criminal record checks. Higher clearance where the Order Form requires. Access removed on the day a leaver departs |
| <b>7. Secure development</b>              | Secure development lifecycle with peer code review, static and dynamic application security testing, and dependency and container scanning in the build pipeline. Security defects triaged under paragraph C.5                                         |
| <b>8. Supply chain security</b>           | All sub-processors named at paragraph B.7. Contractual flow-down of security, residency and data protection obligations. Cyber Essentials required of any sub-contractor with access to Buyer Data                                                     |
| <b>9. Secure user management</b>          | Role-based access control administered by the Buyer. Least privilege enforced. Privileged access reviewed quarterly and evidenced to the Buyer on request                                                                                              |
| <b>10. Identity and authentication</b>    | SAML 2.0 and OpenID Connect single sign-on. Multi-factor authentication available to all users and mandatory for administrative and privileged accounts                                                                                                |
| <b>11. External interface protection</b>  | Web application firewall, rate limiting and bot protection at the edge. Authenticated and authorised APIs. No administrative interface is exposed to the public internet                                                                               |
| <b>12. Secure service administration</b>  | Administration only from managed devices over authenticated, MFA-protected channels. Just-in-time privileged access with approval. Privileged sessions logged. UK personnel only (clause 12.4)                                                         |
| <b>13. Audit information for users</b>    | Complete, immutable and exportable audit trail of user, configuration, data and AI-assisted actions, retained for at least 12 months and available to the Buyer at any time without charge                                                             |
| <b>14. Secure use of the service</b>      | Administrator and user documentation, secure configuration guidance, and onboarding support provided at no charge, so the Buyer can operate the Service securely                                                                                       |

### C.3. Division of responsibility

Assurance depends upon knowing who is accountable for what. The following table divides responsibility between the Buyer, the Supplier and the Platform and infrastructure providers. **Where responsibility is shared, the Supplier remains accountable to the Buyer in accordance with clause 25.1**, and the Buyer has no contractual relationship with any provider named in the final column.

| Control domain                                                   | Buyer                         | Cyberfortis                       | Platform and infrastructure |
|------------------------------------------------------------------|-------------------------------|-----------------------------------|-----------------------------|
| Physical and environmental security of data centres              | —                             | Oversight and assurance           | Accountable                 |
| Infrastructure patching and hardening                            | —                             | Accountable                       | Performs                    |
| Platform software maintenance and code defect correction         | —                             | Accountable                       | Performs                    |
| Application configuration supplied as standard                   | —                             | Accountable                       | —                           |
| Configuration, control mappings and content created by the Buyer | Accountable                   | Provides the capability           | —                           |
| Identity, roles and user administration                          | Accountable                   | Provides the capability           | —                           |
| Multi-factor authentication                                      | Accountable for its own users | Mandatory for privileged accounts | —                           |
| Data classification and lawful basis for processing              | Accountable                   | —                                 | —                           |
| Accuracy and quality of Buyer Data                               | Accountable                   | —                                 | —                           |
| Encryption at rest and in transit                                | —                             | Accountable                       | Performs                    |
| Backup, restore and disaster recovery                            | —                             | Accountable                       | Performs                    |
| Protective monitoring and security incident response             | Reports suspected compromise  | Accountable                       | Supports                    |
| Vulnerability identification and remediation                     | —                             | Accountable                       | Performs for the Platform   |
| Continuity of the Buyer's own operations and processes           | Accountable                   | Supports                          | —                           |
| Exit, data export and portability                                | Requests and verifies         | Accountable                       | —                           |

### C.4. Security testing

**C.4.1** The Supplier commissions an independent penetration test of the Service at least annually, carried out by a CREST-accredited or equivalent supplier, and shall provide the executive summary and remediation status to the Buyer on request at no charge.

**C.4.2** The Buyer may carry out its own security testing under clause 9.3, on notice, at no charge and without needing the Supplier's approval.

### C.5. Vulnerability remediation

| Severity (CVSS v3.1)   | Remediated within      |
|------------------------|------------------------|
| Critical — 9.0 to 10.0 | <b>7 calendar days</b> |

| Severity (CVSS v3.1) | Remediated within       |
|----------------------|-------------------------|
| High — 7.0 to 8.9    | <b>14 calendar days</b> |
| Medium — 4.0 to 6.9  | 30 calendar days        |
| Low — below 4.0      | 90 calendar days        |

**C.5.1** Periods run from confirmation of the vulnerability. Where a critical or high vulnerability affecting the Service cannot be remediated within the period, the Supplier shall notify the Buyer, explain why, and set out compensating controls and a remediation date.

#### **C.6. Security incidents**

**C.6.1** Security Incidents are notified to the Buyer within 24 hours under clause 13.4, whether or not Personal Data is involved, with a written post-incident report within 10 Working Days.

#### **C.7. Information classification**

**C.7.1** The Service is designed and operated to handle information classified at **OFFICIAL**, including information carrying the OFFICIAL-SENSITIVE handling caveat where the Order Form so provides and the Buyer's risk assessment supports it.

**C.7.2** The Service is **not** approved for information classified above OFFICIAL. The Supplier shall tell the Buyer if it believes the Buyer is using the Service outside its approved classification.

#### **C.8. Assurance evidence pack**

**C.8.1** The following are available to the Buyer on request at no charge, before or after contract award: Cyber Essentials Plus certificate; ISMS policy set and internal audit summary; penetration test executive summary; business continuity test summary; sub-processor list; access control and privileged access procedure; secure development policy; incident management procedure; accessibility statement and audit report; Carbon Reduction Plan; and evidence of insurance.

---

## SCHEDULE 1

### Buyer obligations

---

This Schedule sets out the obligations of the Buyer. It is limited to those matters which the Supplier reasonably requires in order to provide the Service. The Supplier's entitlement to relief in consequence of any failure by the Buyer to perform an obligation set out in this Schedule is governed by, and constrained by, clauses 8.2 and 8.3.

#### **S1.1. People and decisions**

- S1.1.1** The Buyer shall nominate a contract manager and a service owner, and shall notify the Supplier of any change to either.
- S1.1.2** Where Implementation Services have been ordered, the Buyer shall provide decisions, approvals and access to appropriate personnel within the timescales agreed in the project plan.

#### **S1.2. Users**

- S1.2.1** The Buyer shall administer Authorised User accounts, including the prompt removal of users who no longer require access.
- S1.2.2** The Buyer shall take reasonable steps to procure that Authorised Users comply with clause 9 (Acceptable use).

#### **S1.3. Data**

- S1.3.1** The Buyer shall be responsible for the accuracy, quality and lawfulness of the data which it uploads to the Service, and for the existence of a lawful basis for any Personal Data contained within it.
- S1.3.2** The Buyer shall not upload information classified above OFFICIAL, nor any special category or criminal offence data, save as agreed under paragraph B.2.

#### **S1.4. Technical environment**

- S1.4.1** The Buyer shall maintain its own network connectivity, devices and browsers within the supported versions published by the Supplier, which the Supplier shall keep current and reasonable.

#### **S1.5. Security**

- S1.5.1** The Buyer shall protect account credentials, shall enable multi-factor authentication for privileged accounts, and shall notify the Supplier promptly of any suspected compromise of an account.

#### **S1.6. Payment**

- S1.6.1** The Buyer shall pay correctly rendered, undisputed invoices in accordance with clause 16.

#### **S1.7. Completeness of this Schedule**

- S1.7.1** The obligations set out in this Schedule 1 constitute the entirety of the obligations of the Buyer under these Supplier Terms.
- S1.7.2** **The Supplier shall not assert, and shall not be entitled to rely upon, any obligation on the part of the Buyer which is not expressly set out in this Schedule 1 or in the Call-Off Contract.**

---

## SCHEDULE 2

### Document control

---

#### S2.1. Version history

| Version | Date of issue  | Status | Summary of change                                                                                      | Issued by                      |
|---------|----------------|--------|--------------------------------------------------------------------------------------------------------|--------------------------------|
| 1.0     | September 2026 | Issued | First issue of the Supplier Terms for the G-Cloud 15 Framework Agreement (RM1557.15), Lot 2b and Lot 3 | Cyberfortis Consulting Limited |

**S2.1.1** The version of these Supplier Terms applicable to a Call-Off Contract is the version identified in the Order Form. A later version has no effect upon that Call-Off Contract except by agreement in accordance with clause 24.5.

#### S2.2. Review and maintenance

**S2.2.1** These Supplier Terms are reviewed by the Supplier not less than annually, and in any event upon any material change to the Framework Agreement, to the Service, to the supply chain, or to applicable law.

**S2.2.2** Where a review results in a change which improves the position of the Buyer, the Supplier shall offer that change to the Buyer at no charge.

**S2.2.3** The Supplier shall notify the Buyer of the issue of a revised version within 20 Working Days, together with a summary of what has changed.

#### S2.3. Status of this document

**S2.3.1** **This document is published for the purposes of the G-Cloud 15 Framework Agreement and is not confidential.** The Supplier does not restrict its circulation, reproduction or publication, whether by the Buyer, by the Government Commercial Agency, or by any other person.

**S2.3.2** No provision of this document is asserted to be exempt from disclosure under the Freedom of Information Act 2000. See clauses 18.2 to 18.6.

#### S2.4. Enquiries

**S2.4.1** Enquiries concerning these Supplier Terms may be addressed to the Supplier at [legal@cyberfortis.co.uk](mailto:legal@cyberfortis.co.uk). The Supplier shall respond within 5 Working Days in accordance with clause 28.14.

#### **Before placing an Order**

Where the Buyer is unable to accept any provision of these Supplier Terms, the Supplier shall consider in good faith the amendment or disapplication of that provision by means of the Order Form. The Supplier would rather amend a term than lose the opportunity to serve the Buyer.

## **CYBERFORTIS CONSULTING LIMITED**

FortisOne GRC by Cyberfortis

---

### Supplier Terms and Conditions

Document reference FGRC-GC15-STC\_v1.0\_GB\_09-2026

G-Cloud 15 Framework Agreement, reference RM1557.15, Lot 2b and Lot 3

Issued September 2026

Cyberfortis Consulting Limited is a company incorporated in England and Wales under company number 16157381.

Registered office: **Level 30, The Leadenhall Building, 122 Leadenhall Street, London EC3V 4AB**

Enquiries: [legal@cyberfortis.co.uk](mailto:legal@cyberfortis.co.uk) · [cyberfortis.co.uk](https://cyberfortis.co.uk)

*This document is published for the purposes of the G-Cloud 15 Framework Agreement and is not confidential. Its circulation, reproduction and publication are not restricted. See paragraph S2.3.*