



Crown Commercial Service

G-Cloud 12 Call-Off Contract

This Call-Off Contract for the G-Cloud 12 Framework Agreement (RM1557.12) includes:

Part A: Order Form	2
Schedule 1: Services	12
Schedule 2: Call-Off Contract charges	12
Part B: Terms and conditions	13
Schedule 3: Collaboration agreement.....	32
Schedule 4: Alternative clauses.....	44
Schedule 5: Guarantee.....	49
Schedule 6: Glossary and interpretations	57
Schedule 7: GDPR Information	68

Part A: Order Form

Buyers must use this template order form as the basis for all call-off contracts and must refrain from accepting a supplier's prepopulated version unless it has been carefully checked against template drafting.

Digital Marketplace service ID number	██████████
Call-Off Contract reference	██████
Call-Off Contract title	Wisdom, Kofax and Service Delivery
Call-Off Contract description	As per Schedule 1- Services Daisy CloudBridge Management Enterprise Plus
Start date	11/08/2022
Expiry date	10/08/2024
Call-Off Contract value	<p>██████████ excluding VAT.</p> <p>Subject to any variations and changes in scope the estimated call off contract value including any extension periods (which must be agreed between the Parties), based on the charges in Schedule 2 is ██████████ excluding VAT</p>
Charging method	Services billed monthly in advance and additional usage to be billed monthly in arrears
Purchase order number	TBC

This Order Form is issued under the G-Cloud 12 Framework Agreement (RM1557.12).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Deliverables offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

From the Buyer	The Insolvency Service 3 rd Floor Cannon House 18 Priory Queensway Birmingham B4 6FD
To the Supplier	Daisy Corporate Services Trading Limited 07714737991 Lindred House 20 Lindred Road, Brierfield Nelson Lancashire BB9 5SR 02888250
Together the 'Parties'	

Principal contact details

For the Buyer:

Title: Commercial Business Partner

Name: Frank Joseph

Email: Frank.Joseph@insolvency.gov.uk

Phone: 07966 442909

For the Supplier:

Title: Frameworks Contract Manager

Name: Paddy Sheridan-Ruddy

E-mail: Patrick.sheridan-ruddy@daisyuk.tech

Phone: 07714737991



Call-Off Contract term

Start date	<p>This Call-Off Contract Starts on 11/08/2022 and is valid for 24 months.</p> <p>[The date and number of days or months is subject to clause 1.2 in Part B below.]</p>
Ending (termination)	<p>The notice period for the Supplier needed for Ending the Call-Off Contract is at least [90] Working Days from the date of written notice for undisputed sums (as per clause 18.6).</p> <p>The notice period for the Buyer is a maximum of [30] days from the date of written notice for Ending without cause (as per clause 18.1).</p>
Extension period	<p>This Call-off Contract can be extended by the Buyer for 2 period(s) of up to 12 months each, by giving the Supplier 3 months written notice before its expiry. The extension periods are subject to clauses 1.3 and 1.4 in Part B below.</p> <p>Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.</p>

Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

G-Cloud lot	<p>This Call-Off Contract is for the provision of Services under:</p> <ul style="list-style-type: none"> • Lot 1: Cloud hosting
G-Cloud services required	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:</p> <ul style="list-style-type: none"> • Managed Hosting • Managed Service • Managed Applications • Dedicated Service Delivery Manager
Additional Services	<p>Customer Design Authority</p> <p>The Buyer may require additional licensing and/or enhanced services to support the deployment, as defined by the Suppliers G-Cloud Service offering, service ID [REDACTED] [REDACTED] Any Additional Services shall be subject to agreement between the Parties via the Variation Process (Clause 32).</p>
Location	<p>The Services will be delivered to The Buyer's address:</p> <p>The Insolvency Service</p> <p>3rd Floor</p> <p>Cannon House</p> <p>18 Priory Queensway</p> <p>Birmingham</p> <p>B4 6FD</p>

Quality standards	The quality standards required for this Call-Off Contract are ISO9001:2015
Technical standards:	<p>The technical standards used as a requirement for this Call-Off Contract are ISO27001 Accredited, work to GDPR ICO Standards Article 30, ICO Article 4, 5, 26, 32, 37 and 49 and Recitals 39, 79, 83, 97 and 113.</p> <p> DCS ISO27001 Cert IS 599749.pdf</p>
Service level agreement:	<p>The service level and availability criteria required for this Call-Off Contract are Enterprise Plus support as defined in the Service Description, attached (“Insolvency Service-Wisdom-Kofax-Service Delivery Statement 12-07-2022.docx”)</p> <p> Insolvency Service-Wisdom-Kofa</p>
Onboarding	The onboarding plan for this Call-Off Contract is not applicable as solution is already in situ.
Offboarding	Notwithstanding the Supplier’s obligations under Clause 21 (Exit Plan) below, the offboarding plan for this Call-Off Contract is: Daisy will undertake the collation of the data it holds on behalf of the Buyer and migrate it back to either the Buyer or its new service provider on or by an agreed date (usually the last day of the contract). A final report of the data

being held will be provided by Daisy to the Insolvency Service prior to the migration of data. Should the data to be migrated falls outside our agreed method (usually a data upload or on Hard Drive), then this would be charged back to the Buyer at an agreed cost with any additional costs (both Hardware, Software and Professional Services) being charged back to the Buyer. Once the data has been transferred and acknowledged by the Buyer any remaining data will be permanently deleted and the servers and devices that held that data on behalf of the Buyer will be turned off and decommissioned as part of the Exit Plan

Additionally

Upon expiry or termination of this Contract howsoever arising, the Supplier will: allow the Buyer reasonable access to the Supplier's premises upon reasonable notice, to collect any equipment or materials owned by the Buyer; deal with the Buyer's Confidential Information in the possession or control of the Supplier relating to this Contract; and provide reasonable account details relating to the Services, including but not limited to lists of telephone numbers to which the Services relate, account balances, copy invoices and any migration codes required to transfer the Services. Following notice to terminate the Contract being served by either party the Supplier will within a reasonable time: make available an exit manager to assist the Buyer with the organisation and co-ordination of the provision of exit assistance; assist the Buyer with the production of an exit management plan; provide exit assistance in accordance any agreed written exit management plan; and provide reasonable technical information relating to the Services and Products; noting that the Supplier will be entitled to remove it's IP from any configuration and any data considered a security risk; subject in each case to such assistance being chargeable and calculated on a time and materials basis at the Supplier's prevailing standard rates and subject to payment of any relevant third party costs, for example the extension or renewal of any Third Party Software licences. Following notice to terminate this Contract being served by either party pursuant to this clause, the Buyer unless otherwise agreed in writing by the parties, is responsible for extracting, transferring or downloading, as appropriate, any and all data, records and information of the Buyer that the Buyer has direct electronic access to as part of the Services and that the Buyer wishes to retain. The Buyer will confirm in writing to the Supplier without undue delay that all relevant data migration has been completed.

Collaboration agreement	The Insolvency Service has a SIAM provider (Advanced) who are acting on their authority and will be the main BAU contact for Daisy
Limit on Parties' liability	<p>The annual total liability of either Party for all Property Defaults will not exceed 125% of total contract value.</p> <p>The annual total liability for Buyer Data Defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p> <p>The annual total liability for all other Defaults will not exceed the greater of [REDACTED] or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).</p>
Insurance	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> • a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract • professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. [REDACTED] [REDACTED] [REDACTED] [REDACTED] • [REDACTED] [REDACTED] or any higher minimum limit required by Law

Force majeure	A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than 10 consecutive days.
Audit	<p>The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the buyer to carry out audits.</p> <p>The Supplier's records and accounts will be kept until the latest of the following dates:</p> <ul style="list-style-type: none"> • 7 years after the date of Ending or expiry of this Framework Agreement during the timeframes highlighted in clause 7.6, the Supplier will maintain: • commercial records of the Charges and costs (including Subcontractors' costs) and any variations to them, including proposed variations • books of accounts for this Framework Agreement and all Call-Off Contracts • MI Reports • access to its published accounts and trading entity information • proof of its compliance with its obligations under the Data Protection Legislation and the Transparency provisions under this Framework Agreement <p>Subject to any Confidentiality obligations, the Supplier will use reasonable endeavours to:</p> <ul style="list-style-type: none"> • provide audit information without delay • provide all audit information within scope and give auditors access to Supplier Staff <p>The Supplier will allow the representatives of CCS, Buyers receiving Services, the Controller and Auditor General and their staff, any appointed representatives of the National Audit Office, HM Treasury, the Cabinet Office and any successors or assigns of the above access to the records, documents, and account information referred to in clause 7.7 (including at the Supplier's premises), as may be required by them, and</p>

	<p>subject to reasonable and appropriate confidentiality undertakings, to verify and review:</p> <ul style="list-style-type: none"> • the accuracy of Charges (and proposed or actual variations to them under this Framework Agreement) • any books of accounts kept by the Supplier in connection with the provision of the G-Cloud Services for the purposes of auditing the Charges and Management Charges under the Framework Agreement and Call Off Contract only • the integrity, Confidentiality and security of the CCS Personal Data and the Buyer Data held or used by the Supplier • any other aspect of the delivery of the Services including to review compliance with any legislation • the accuracy and completeness of any MI delivered or required by the Framework Agreement • any MI Reports or other records about the Supplier's performance of the Services and to verify that these reflect the Supplier's own internal reports and records • the Buyer's assets, including the Intellectual Property Rights, Equipment, facilities and maintenance, to ensure that the Buyer's assets are secure and that any asset register is up to date
Buyer's responsibilities	<p>The Buyer is responsible for:</p> <ol style="list-style-type: none"> 1. Any directory services changes remain the sole responsibility of the Buyer 2. The data content and its usage relating to the SQL Server 3. To communicate the required downtime to the users of the system ahead of the migration work commencing 4. To provide connectivity into the newly created tenancy for application consumption 5. To work with Daisy to ensure perimeter security is maintained as part of the solution

Buyer's equipment	The Buyer's equipment to be used with this Call-Off Contract includes none
--------------------------	---

Supplier's information

Subcontractors or partners	<p>The following is a list of the Supplier's Subcontractors or Partners:</p> <p>UNION STREET TECHNOLOGIES LIMITED Milton Gate, 60 Chiswell Street, London, United Kingdom, United Kingdom, EC1Y 4AG</p>
-----------------------------------	--

Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

Payment method	The payment method for this Call-Off Contract is BACS
Payment profile	<p>The payment profile for this Call-Off Contract is that services are billed monthly or annually in advance as per the table shown in Schedule 2 and additional usage to be billed monthly in arrearsOne-off charges will be invoiced on the first invoice following the contract being signed.</p> <p>Invoices are generated on the 1st Each month and payment is due within 30 days.</p> <div><div></div><div></div><div></div></div>

	<p>Assuming a start date in line with the billing period the Service Charges for this contract on the 1st invoice generated will be: [REDACTED] with subsequent invoices up until the anniversary date only billing the services charged Monthly [REDACTED]</p> <p>Should the contract start date fall outside of the billing period then pro-rata charges will be included in order to bring the billing in line. No pro-rata charges will apply for one off or annual charges.</p>
Invoice details	The Supplier will issue electronic invoices monthly The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to	<p>Invoices for payment only shall be sent to payments@insolvency.gov.uk</p> <p>Note that for invoice queries only, you should contact the following: Transactional.Queries@insolvency.gov.uk</p> <p>Postal Invoices shall be sent to:</p> <p>The Insolvency Service</p> <p>Cannon House</p> <p>PO Box 16652</p> <p>B2 2HR</p>
Invoice information required	All invoices must include a valid Purchase Order number
Invoice frequency	Invoice will be sent to the Buyer monthly.
Call-Off Contract value	The total value of this Call-Off Contra [REDACTED]
Call-Off Contract charges	The breakdown of the Charges is As listed in Schedule 2

Additional Buyer terms

Performance of the Service and Deliverables	<p>This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones:</p> <ul style="list-style-type: none"> • Please refer to schedule 1
Guarantee	Not Applicable
Warranties, representations	Not Applicable
Supplemental requirements in addition to the Call-Off terms	Not applicable
Alternative clauses	Not Applicable
Buyer specific amendments to/refinements of the Call-Off Contract terms	<p>All services shall be delivered from the UK unless prior approval has been sought and granted in advance by the Buyer to do otherwise.</p> <p>Any equipment that may be provided by the Buyer to the Supplier during the life of the contract for the delivery of the services shall not be taken outside the UK.</p>



Public Services Network (PSN)	Not Applicable
Personal Data and Data Subjects	Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: Annex 1

1. Formation of contract

- 1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.
- 1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.
- 1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
- 1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

2. Background to the agreement

- 2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.
- 2.2 The Buyer provided an Order Form for Services to the Supplier.

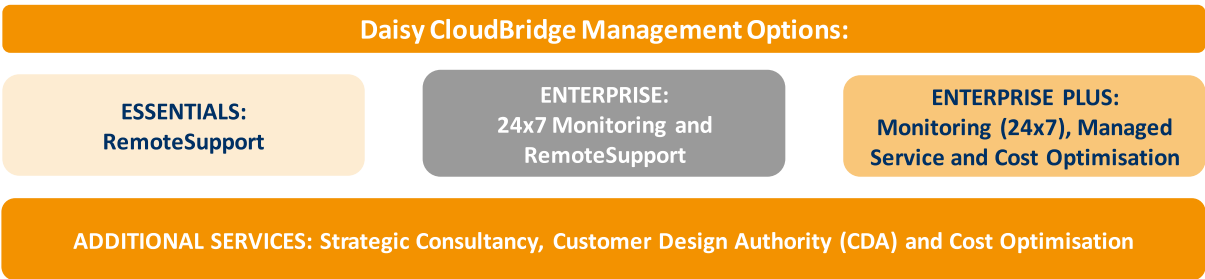
Signed	Supplier	Buyer
Name	[Enter name] Andy Riley	[Enter name] Phil Harding
Title	[Enter title] Sales Director	[Enter title] Senior Commercial Business Partner
Signature		
Date	[Enter date] 11/8/2022	[Enter date] 11/8/2022

Schedule 1: Services

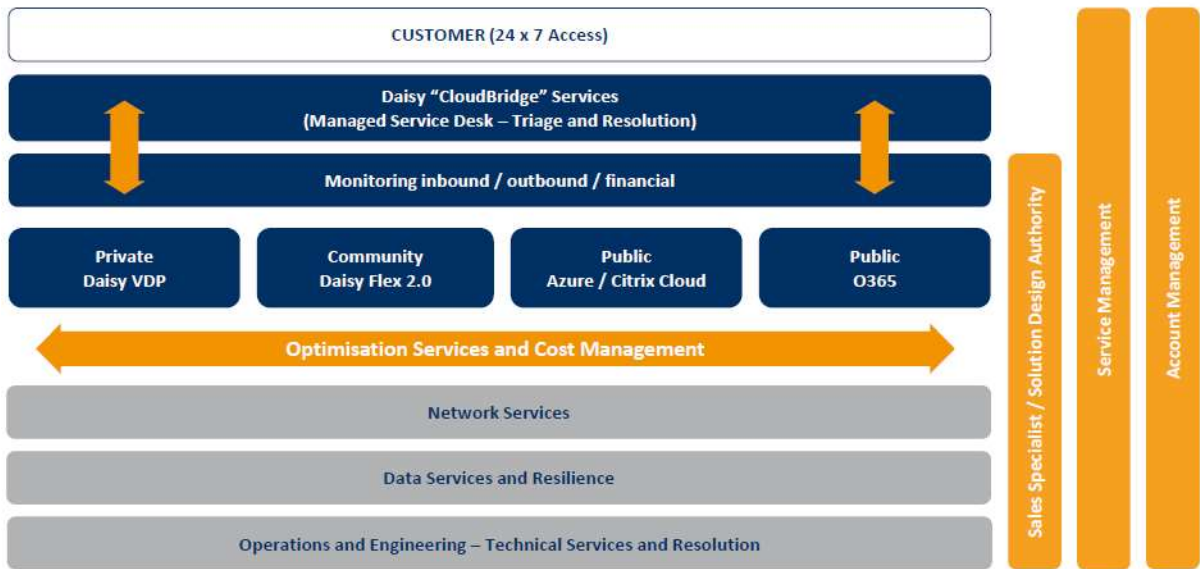
Managed Services Description

Management Enterprise Plus

Daisy will provide both reactive and proactive support and management services for the hosted solution on the ‘Enterprise ‘Plus’ provision.



The services are delivered using Daisy’s standardised support model below which uses consistent tools and processes.



The Management Enterprise Plus offering is a managed service from Daisy, it provides monitoring and support as in Enterprise however full control of the day-to-day operation is passed to Daisy and as such the level of support is not limited by a number of specified hours. Furthermore, Daisy will undertake regular pro-active management of the infrastructure and application layers to improve security and stability.

Daisy’s Manage Services also include access to our service management operational processes, all aligned to ITIL best practice, including;

- **Incident Management**
- **Event Management**
- **Problem Management**
- **Change Management**
- **Request Fulfilment**

These processes are co-ordinated via the Daisy Service Desk and extends across the breadth of Daisy's Technical Management and IT Operations functions.

Monitoring Service

Event Management Summary

Event Management provides response to specific conditions which may not be part of the standard operation of the service and which may cause an interruption to, or a reduction in, the quality of that service if specific actions are not undertaken.

An alert ticket is automatically raised by Daisy's monitoring system as specific thresholds or conditions are met for parameters being monitored. The event is processed by Daisy's monitoring tools and actionable events are allocated a priority and are enriched with additional information according to the parameters set in Daisy monitoring systems. Actionable events are raised as an incident or request ticket, as relevant, in the Daisy IT Service Management toolkit.

Monitoring Overview

From our UK based Daisy Technical Operations Centre, our system monitoring services will be tailored to match precise operational, technical and business requirements. The Technical Operations Centre is staffed 24 hours a day, every day aligned to customer service hours and service levels.

The Daisy monitoring service uses an enterprise class monitoring and management suite, ensuring far greater information can be gathered, analysed and enriched as compared to simple SNMP toolkits.

The monitoring service operates in an agentless mode using a centralised collector, which allows detailed information to be collected (including pre-defined OS services, events, paging, processor queue, etc.) and therefore enhances our ability to monitor the system effectively.

The applications will be monitored (application logs) to ensure the systems are running efficiently.

Monitoring System Tuning and Event Correlation

Through tuning the monitoring system to a Customer environment, we are able to drive consistency to speed up resolution. This also allows tailored communication and troubleshooting approaches in line with Customer’s specific needs. There are a number of integrated systems that Daisy use in the delivery of this service for our customers; these include systems for monitoring and alerting, event correlation & enrichment and the ITSM toolkit.

Our approach to tuning and event correlation adds value by

- reducing ‘alert fatigue’ by suppressing unwanted and noisy alerts, letting people focus on the events that matter
- automating notifications and the creation and prioritisation of tickets, improving efficiency and eliminating human errors and delays
- enriching known events with runbook data, significantly reducing time spent triaging events and diagnosing and resolving incidents, as well as providing consistency and reducing human error.

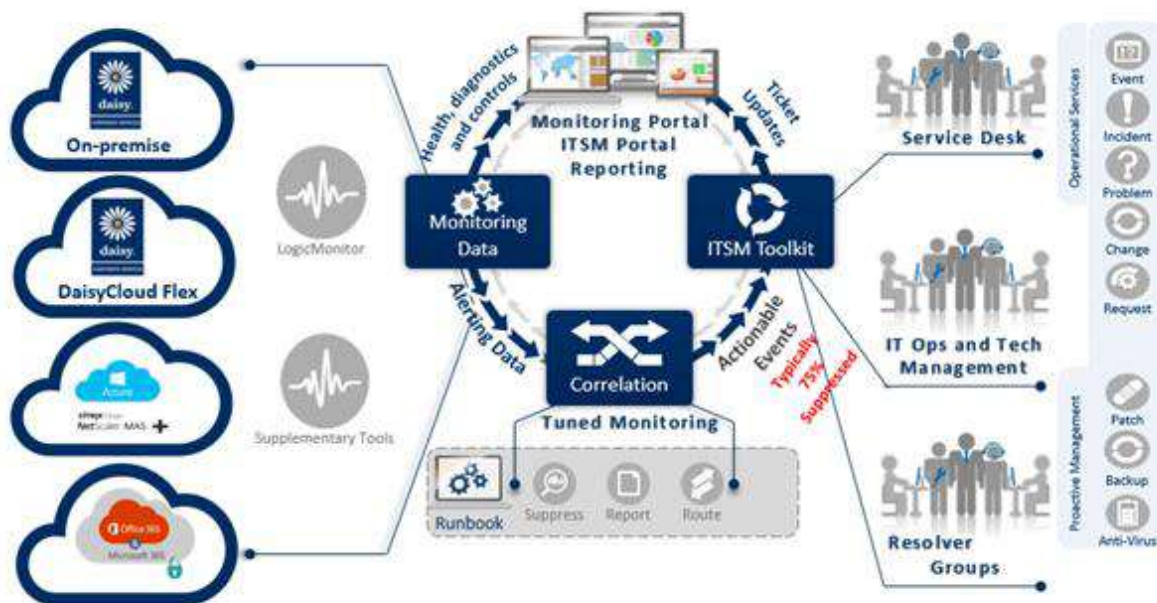
Monitoring Parameters

The scope of the Daisy monitoring service will include the following from level 1 and level 2 monitoring (as listed below), with specific parameters and thresholds defined as part of the low-level design and tuned on an on-going basis. Level 3 monitoring, for the Wisdom and Kofax applications is also included.

Azure	Level 1: <ul style="list-style-type: none">• Azure network services (95% usage)• Azure Storage (% usage) 3 levels – warning/major/critical 75% 90% 98% respectively• Azure VM (90% usage)
Windows Servers	Level 1: <ul style="list-style-type: none">• Device Availability• Disk• Memory• CPU• Memory Stats Alert• Interface Alerts Level 2:

	<ul style="list-style-type: none"> • Level 1 (as above) • Specified Windows Services including: <ul style="list-style-type: none"> ○ Netlogon ○ Client Antivirus ○ IIS Admin ○ World Wide Publishing Service ○ DHCP Client ○ RPC ○ Print Spooler ○ Remote Desktop Services ○ Windows Time
Linux	<p>Level 1:</p> <ul style="list-style-type: none"> • Device Availability • Disk • Memory • CPU • Alerts
<p>Application layer</p> <p><i>(Wisdom and Kofax)</i></p>	<p>Level 3:</p> <ul style="list-style-type: none"> • Windows application log monitoring • Services monitoring • Application log monitoring (Kofax specific) • Service availability (Wisdom specific)

Operational Overview



Note: This model denotes the Daisy managed service solution which will integrate into the wider Insolvency Service SIAM model (if available at time of implementation).

Tickets will be raised in the Insolvency Service's SIAM providers ITSM toolset, Remedy and automatically directed to Daisy's ITSM toolset ServiceNow via API integration. Tickets will be allocated to the appropriate 2nd line resolver groups for resolution. These teams include the Wisdom application support team and the Azure infrastructure support team who provide the managed service.

The Daisy tuned monitoring solution will pick up the event and based on pre-defined criteria will implement one of the following;

- for Information Only alerts, the system will close the alarm condition and may suppress the event. This means that there is a record of the event however no ticket is raised at this point. An example of this might be a CPU spike for 10 seconds above the designated threshold, this may not require immediate investigation so no ticket is required however the event is retained for trending and tracking purposes in case this repeats regularly, in which case a problem record would be created and investigations would be undertaken.
- where an Incident is required to be created, the system will automatically generate a ticket, with a pre-defined priority within our IT Service Management toolkit. For example if a device alarms with status uncontactable the system can generate a P1 Incident within the IT Service Management toolkit, which the technical support team will pick up and work to resolve in line with the service level agreement.
- the system has the capability to pick up pre-defined events and enrich them from the knowledge-base. This can include technical runbook details, troubleshooting steps or customised communication information related to that type of event. When the system creates the ticket within the IT Service Management toolkit, the associated enrichment

information will be provided for the Daisy technical resources, resulting in better efficiency and service quality.

Managed Service

Reactive Technical Support

Daisy will work with the Insolvency Service SIAM provider, however full details of the service from the SIAM and the demarcations will need to be clarified by Insolvency Service.

In addition to providing proactive support and incident resolution for automated alerts generated by the monitoring solution, the Daisy Managed Service also provides the ability for approved Insolvency service SIAM contacts to raise incidents via the SIAM Remedy ITSM toolset. The ticket will flow from Remedy to Daisy's ServiceNow ITSM toolset via an API toolset integration which the Daisy Service Desk will manage in line with contractual service levels

P1 incidents will be responded to on a 24x7 basis with lower priority incidents being addressed during normal working hours (specific application support response times are detailed in section 4.2.10.1). The incidents will be triaged in the first instance by the Insolvency SIAM provider and the ticket will be allocated to a second line resolver group within the Daisy Technical Operations function once logged.

The second line analyst will engage directly with the system(s) using the provisioned remote access management tools where appropriate to resolve the relevant services (see indicative examples below):

Infrastructure layer

- **Operating System faults**
- **Anti-Virus quarantine events**
- **Backup failures**
- **Managed Remote Desktop services faults**
- **Microsoft Azure and Office 365 escalations to Microsoft**
- **Microsoft Azure Site Recovery configuration issues**

Application layer

- **Permission issues**
- **Document recovery**
- **Retention problem resolution**
- **Offline cascade problems**

- **Kofax batches not releasing**
- **Kofax VRS configuration and issue resolution**
- **Kofax dll issues¹**
- **Problems from inactive services**

Where required, an incident will also be escalated to the Daisy third line support team within the Daisy Technical Operations function and onward to any internal subject matter experts or vendor as necessary in order to provide a resolution.

During the engagement, dynamic updates will be made on our IT Service Management toolkit ensuring all parties are aware of the progress of the ticket.

Problem Management

The goal of Incident Support and the underlying Daisy incident management process is to bring a failed service live again as soon as possible by attempting a fix or a workaround. Where an incident or number of incidents warrant root cause analysis to determine a permanent fix or to reduce the risk of a repeat failure, Daisy will provide problem management and manage problem tickets from Remedy via the ITSM toolset integration with Daisy's ServiceNow. Problem management is provided for the scope of Daisy contracted services only and the output of the process may result in a recommendation to the customer rather than a fix.

A problem record can be raised from a variety of scenarios related to Incidents.

- **following a major incident to ensure a major incident does not re-occur and that major incident actions are tracked**
- **where several incidents are connected or linked or where an incident has reoccurred (reoccurring incident).**
- **by the Daisy Service Desk or Technical Operations teams who have identified a potential problem (problem candidate).**
- **automated detection of an infrastructure or application fault using management toolkits.**
- **notification from a vendor that a problem exists.**

The problem originator will link the original/related incident(s), CIs or business lines and known workarounds.

All relevant details will be taken from the incident record(s) and a problem record created. A summary is added to the problem record of the issue and what actions are required. Any relevant CI's, incidents and changes are linked to the problem record.

The Daisy Technical Management function shall then undertake activities to investigate the problem with a view to establish the root cause.

Where the root cause has been established and a resolution has been identified to the problem, a known error record is created and linked to the problem record. The Customer will then be presented with the recommended next steps to mitigate future occurrence of the root cause which, in some cases, may require additional charges to be accepted. Where the charges are accepted (or indeed no charges apply and the change is authorised to proceed), Daisy shall implement the resolution accordingly.

Change Management

The goal of change management is to control the lifecycle of all changes by understanding, predicting and minimising the risk of making changes.

In order to maintain effective control over change in the environment Daisy uses a change management process needs that ensure all changes follow a risk-controlled approach with an agreed assessment and approval taking place with the business and technical stakeholders.

The Daisy change manager runs weekly change advisory boards (CABs) where required changes are reviewed ensuring that the documented procedure is appropriate and that an effective roll-back plan is included in case the change should fail. Emergency CABs (eCABs) are also be held as necessary to implement emergency changes in order to prevent or rectify a major incident.

Changes are categorised as emergency, standard and normal.

Daisy will participate on weekly InsS CABs, these should be restricted to one hour perweek. Should additional meeting be necessary a CR will be required.

Wisdom Maintenance: Daisy will be responsible for all changes within the system configuration, this does not include items that can be modified via the Standard Wisdom application interface, which maintained by InsS, all items on the 'Wisdom Settings' page will be maintained by Daisy, InsS will NOT have access to the 'Wisdom Settings' Page.

Kofax Maintenance: Daisy will be responsible for all changes within the system configuration, this includes items that can be modified via the administration application (Admin), InsS will NOT have access to the administration module.

- **Emergency change is used only when necessary to solve a major incident or prevent a major incident from occurring. Emergency changes are assessed to ensure that the impact and risk of performing the change is not greater than the impact and risk of not performing it. eCAB is used to control the emergency change process.**
- **Standard change is for pre-authorised low risk, relatively common and follows a procedure or work instruction. A catalogue of such changes is defined in transition based on the customers solution and technologies and is then updated during the life of the service.**
- **Normal change is for all other changes and is sub-categorised into minor, significant or major based on the level of risk related to the change.**

Standard Change Catalogue

A standard change catalogue will be defined as part of the service transition to align to the specific service for the customer. As an example, the below are typical standard changes within the Daisy catalogue:

- **Reboot a Device**
- **Add/Remove a Device on Server Monitoring**
- **Add or Remove an Antivirus Client**
- **Increase or decrease of vCPU allocation**
- **Increase or decrease of vRAM allocation**
- **Add New IP Address to Existing VM**
- **Install/Renew an SSL Certificate**
- **Change the State of a Server Service**

Chargeable Changes / Project Work

As with any service offering, there are circumstances where a request for change or an implementation request from the customer falls outside the inclusive change catalogue or service.

An example of this type of chargeable work might be the introduction of a new service for the customer (move from Exchange to Office 365 for example) where significant design effort or consideration on other services needs to be addressed.

Where Daisy consider the request to fall outside the inclusive service, then it would be highlighted by the Service Manager to agree a way forward with the customer.

Where it is likely that this type of change might be a regular occurrence, then Daisy are able to provide a solution for pre-paid technical and project work as small works packages.

All Service Management processes will integrate with our SIAM SM processes. Daisy will use our SIAM leads toolset to facilitate Incident, Request, Problem and Change Management.

Proactive Services

1.1.1.1.1 Windows Server Security Vulnerability Updates (patches)

Server patching is crucial for maintaining the integrity of a server and for providing the latest stable versions of software installed.

Daisy will provide a patch management service to implement system security vulnerability updates on Managed Windows servers, in a controlled, automated manner without causing impact to service.

1.1.1.1.1.1 Software & Types of Patches

In order to ensure a consistent set of patches are applied, Daisy will configure the automated patching tool to update customer servers for:

Product	Default Approval Status
Microsoft Windows Server (all current versions*)	Approved

* “All current versions” refers to all versions of the specified software deemed as supportable by the vendor i.e. not end of life products. Excludes Windows clusters.

The patch classifications in scope are:

Microsoft Classification	Default Approval Status
Security Update – Monthly Security-Only Update	Approved

Further details are available in Daisy’s patching documentation, available upon request.

1.1.1.1.1.2 Patch Schedules

Daisy will patch customer servers based upon agreed schedules. A schedule consists of server groups, dates and patch windows.

Once agreed between Daisy and the customer these schedules will be used to create a templated change request form and will be saved in the customer specific Operations Manual. Any changes to this schedule or any of its sub-components will be subject to Daisy’s change management process.

The Daisy templated change request form will be used for each patch window with only the date changing each time.

Each schedule will be designed to cover all relevant servers in the estate, server groups will be used to separate key components of the server estate in order to ensure where possible no loss of service is introduced by patching.

During each patch window, no other changes will be permitted on any servers in the affected server groups by either Daisy or the customer.

1.1.1.1.3 Patching Process

Daisy's server patching process consists of three stages:

Preparation - This stage ensures that all schedules are agreed in advance and recorded in a templated change request form stored in the customer specific Operations Manual. After the first run of patching for each customer, the planning stage is largely static as the schedules are designed to be repeatable at agreed intervals via the use of the templated change request forms. Any changes to schedules or their sub-components are subject to Daisy's change management process.

Patching - During this stage the agreed patches will be applied to the servers using Daisy's automated patching tool. No remediation of failed patch installations will take place during the Patching stage; these shall be managed and resolved as incidents.

Reporting - Following the Patching Stage, Daisy will provide the customer with reports to show the status of the patching for the period.

1.1.1.1.2 Wisdom Server Updates (patches)

Daisy will provide a patch management service to implement Wisdom updates in a controlled manner, these may cause impact to service and will be agreed prior to being installed.

1.1.1.1.2.1 Wisdom Patches

In order to ensure a consistent set of patches are applied, Daisy will update application servers for:

Wisdom Product	Default Approval Status
Point Release	Approved
Major Release	Approved

1.1.1.1.2.2 Patch dates

Daisy will provide Wisdom release details as and when a patch is released.

Daisy will follow the agreed patching process to deliver the patch.

During each patch window, no other changes will be permitted on any servers in the affected server groups by either Daisy or the customer.

1.1.1.1.2.3 Patching Process

Daisy's server patching process consists of three stages:

Preparation - This stage ensures that The Insolvency Service understands the changes which are included in the patch. The schedule for the installation of the patch will be agreed in advance.

Pre-Production Patching - During this stage the agreed patches will be applied to the Wisdom pre-production server. The patch must be tested by The Insolvency Service and signed off prior to the patch being applied to the production environment.

Production Patching - During this stage the agreed patches will be applied to the Wisdom production server. The patch must be tested and signed off by The Insolvency Service.

1.1.1.1.3 Kofax Server Updates (patches)

1.1.1.1.3.1 Wisdom Patches

In order to ensure a consistent set of patches are applied, Daisy will update application servers for:

Kofax Product	Default Approval Status
Point Release	Approved
Major Release	Approved

Daisy will provide a patch management service to implement Kofax updates in a controlled manner, these may cause impact to service and will be agreed prior to being installed.

1.1.1.1.3.2 Patch Schedules

Daisy will provide Kofax release details as and when a patch is released.

Daisy will follow the agreed patching process to deliver the patch.

During each patch window, no other changes will be permitted on any servers in the affected server groups by either Daisy or the customer.

1.1.1.1.3.3 Patching Process

Daisy's server patching process consists of three stages:

Preparation - This stage ensures that The Insolvency Service understands the changes which are included in the patch. The schedule for the installation of the patch will be agreed in advance.

Pre-Production Patching - During this stage the agreed patches will be applied to the Kofax pre-production server. The patch must be tested by The Insolvency Service and signed off prior to the patch being applied to the production environment.

Production Patching - During this stage the agreed patches will be applied to the Kofax production server. The patch must be tested and signed off by The Insolvency Service.

Anti-Virus Update Monitoring and Management

The Anti-Virus (AV) threat prevention service is one of the cornerstones to the security of the customer's systems. In order to support your evolving business requirements, we will ensure that your systems have up-to-date protection against malware, viruses, spyware and other security risks.

As part of the AV service, Daisy will:

undertake On-Access, On-Demand and/or Scheduled scanning checks of the server to seek to detect and clean malware and to help protect files from viruses found in the virus definitions

help block viruses found in the virus definitions on detection

manage and apply updates to the virus definitions

perform configuration of AV software in accordance with good industry practice and AV software vendor guidelines

where infection is found, take appropriate and reasonable measures to recover the operating system as far as reasonably possible to its last known good configuration including any Daisy managed or supported applications.

Backup Management

Daisy will ensure that the InsS data backup is completed and secure in line with the SLA. Daisy will notify InsS should any breaches happen and the associated risks.

Daisy's proactive approach monitors for positive confirmation and backup failures in order to respond to these alerts and investigate as appropriate.

As part of the Backup Management Service, Daisy will:

- implement a backup schedule in agreement with the customer
- monitoring of backup progress
- review backup reports
- re-perform any failed backups within the same window, subject to backup schedule allowing
- investigate any failures in accordance with the incident management service. In the event of a repeated failed backup, Daisy will initiate problem management
- implement backup management changes

Management Information and Reporting

Daisy's reporting provides visibility into complex infrastructure, offering granular performance monitoring and actionable data and insights.

Through a read-only logon to our monitoring, Daisy's service managers will have access to real-time dashboards, customisable for the Customers' monitored infrastructure allowing them to share important information with Customers' as part of the service review process.

This dashboard will be complimented by monthly reports, covering;

- **Service Level Performance**
- **Patch management performance and compliance**
- **AV performance and compliance**
- **Backup management performance, successes and failures**

1.1.1.2 DBA tasks provided by Daisy

As part of the managed service Daisy will provide the following:

- **Install & configure to a standard or accepted base configuration.**
- **Perform proactively and reactive Database Management Tasks**
- **System patching within same SQL version on request.**
- **Database creation to customer application specification.**
- **Monitor the Microsoft SQL Server™ service plus Microsoft SQL Server™ agent service and ensure the service are running.**
- **Monitor additionally specified Microsoft SQL Server™ related services only that are listed as required and ensure the service is running.**
 - **Microsoft SQL Server™ browser service**
 - **Microsoft SQL Server™ integration services service (SSIS)**
 - **Microsoft SQL Server™ Analysis Services Service (SSAS)**
 - **Microsoft SQL Server™ Reporting services service (SSRS)**
- **Monitor storage of Microsoft SQL Server™ databases and logs as well as pre specified folders containing Microsoft SQL Server™ error logs and Microsoft SQL Server™ agent job logs.**
- **Alerting the customer when predefined thresholds have been breached with regard to storage usage. Daisy will raise a change request for the customer to agree to add storage to give 30% free space with the customer being charged at agreed rates for additional storage.**
- **Planning and configuration of backup and recovery, subject to the resources being available and covered contractually**

- **Monitor and record basic performance metrics for use in trouble shooting and performance monitoring.**
- **Monitor and respond to any alerts produced by the monitoring system.**
- **Events and alerts received by Daisy monitoring but classified as outside supported criteria such as SQL Server Agent job failures, SSIS Package failures etc.**
- **Execute scripts supplied by customer (or 3rd party authorised by the customer) as long as the results do not modify the system to out of acceptance criteria and completely at the customer's risk.**
- **Ensuring compliance with database system vendor license agreements where licencing is controlled by Daisy.**
- **DB Performance monitoring and tuning can be done on customer request in the event of severe or sudden performance degradation to a system with any work being carried out with full customer co-operation to fix and find the cause of such issues.**
 - **Where recommendations made by Daisy are not implemented at the request of InsS this element in support is invalidated.**
- **Management of a maintenance plan for the Wisdom databases to ensure regular re-indexing is completed in accordance with the recommended best practice**

1.1.1.3 Ad-hoc / On Demand Tasks

- **Performance monitoring and tuning can be done proactively (in agreement with the customer or as written recommendations). Where strong recommendations are made by Daisy and not implemented by the customer this element in support is invalidated.**

1.1.2 Out of Scope unless otherwise agreed

With the exception of the Wisdom and Kofax managed service, the following SQL services will be out of scope.

- **Any task or process that would result in the manipulation/loss of customer data.**
- **Any tasks normally attributed to the 'developer' role such as:-**
 - **Creating or modifying Views, Functions, Triggers or Assemblies.**
 - **Creating modify or troubleshoot Stored Procedures or Microsoft SQL Server™ Integration Services packages other than those required for administrative tasks.**
 - **Creating or maintaining reports in Microsoft SQL Server™ Reporting services.**

- **Creating modify or troubleshoot PowerShell scripts, Net based applications or any other non SQL code.**
- **Query tuning or indexing strategy which would impact non Daisy Intellectual property rights (IPR).**
- **All applications that use Microsoft SQL Server™ as its 'back end' are not; in themselves covered as part of this module. For example SharePoint, Sage, Internet Information Server.**

Please note that anything not explicitly detailed within this document should be considered out of scope.

Cost Optimisation

Cost Optimisation Review Summary

The Cost Optimisation review service is a regular, scheduled cost focussed audit of the use of your Cloud services from one of our technical specialists.

As regular professional services engagement, on regular basis our specialist engineer will spend up to two working days reviewing your Cloud services and a further day constructing a report into their usage with recommendations on how you could make savings through adjusting how you utilise your Cloud services.

Service Transition for Managed Service

Transition Methodology

Our workstream approach to transition has been developed as a result of years' of experience of managing complex and high risk service transfers for our partners and customers. Using the workstream approach allows specific resources to be concentrated in key areas running in parallel whilst sharing the same governance model and schedule which results in a more focused transition in a shorter duration.

Governed under a Prince 2 Framework the Service Transition process will:

- 1) Ensure all Service Processes are agreed and documented in a Service Operations Manual**
- 2) Manage the handover into support processes for the services in built including:**
 - a. Confirmation all monitoring, and management services are configured**
 - b. Reviewing and placing all design documents and configuration information into the support knowledge base and CMDB**

- c. Handover calls with the support team and agreement around acceptance into service such that the offering becomes owned as part of the ongoing service and operational management function.

Supporting Services

Service Desk

For all tiers of service, Daisy will provide a Service Desk function for incident management and the handling of problem tickets, requests for change and service requests.

Daisy will provide the Insolvency services SIAM provider with primary contact information, such as telephone number and web portal URL. The SIAM will use this primary contact point to log Insolvency Service Customer requests for all contracted Services. The Daisy Service Desk will manage tickets on a priority basis (in accordance with service level agreements), provide diagnosis of incidents and resolution where appropriate, liaise with Customer & SIAM provider resolver(s) as required, manage ticket updates and closures, administer all service requests, and manage agreed third party resolver groups (e.g. vendors).

The Daisy Service Desk will in conjunction with the Insolvency Services SIAM provider:

- Receive calls/tickets from the SIAM provider, respond to contact via the web portal, respond to tickets and investigate and resolve alerts as necessary within the agreed support hours including on a 24x7 basis for P1 incidents;
- Maintain an authorisation process with the SIAM provider to validate the Customer contact and the rights of each contact in relation to incidents, problems, changes and service requests.
- Act as a primary point of hierarchical escalation for all tickets types in scope of the service and logged by the SIAM provider.

Remedy Integration with ServiceNow

The DCS Business Systems Team will design, develop, and deploy integration between our service now toolset and that used by InsS and their Siam advanced Remedy.

The work carried out by the DCS Business Systems Team to process this integration is normally chargeable, however both Union Street & DCS have agreed internally to cover the cost of this resource.

Neither organisation would be responsible for any costs incurred by Advanced or InsS to complete the integration on the Remedy system

The initial stage is to set up a requirement meeting with technical representatives on both sides to scope out the works needed to initiate the integration.

It is advised that this resource is either a developer or Business Analyst with technical knowledge of the Remedy system. In this requirements session we would set out the communication plan and expected outcomes from the initial integration including a low-level design.

Once the integration between Remedy and ServiceNow has been completed the following ticket types will be able to process between the two platforms as intended:

- Incident & Request
- Problem
- Change

DCS business systems team advise to a phased approach to the project and set up integrations as steps

With the requirements gathered, work can start on integration, with regular updates between the project team.

When ready, a staging environment is created where testing can be undertaken. Once all parties are satisfied that the development of that phase meets requirements, then that phase can be scheduled for deployment

Once this work is completed all; incidents, requests, change or problem tickets raised by InsS or Advanced in Remedy for the DCS solution will raise a ticket within DCS SNOW instance automatically via the integration API.

DCS will monitor and be responsible for the integration within the ServiceNow system only.

As the integration with Remedy will take time, and whilst the technical discussions are ongoing with Advanced, tickets raised by InsS will need to be processed via the DCS CSM portal in the same way they are logged currently.

<https://daisygroup.service-now.com/csm>

Customer Web Portal

The Daisy web portal has been implemented to provide Customers with a simple online real-time interface with Daisy resolver groups. Incidents and service requests can be raised, monitored, updated and reviewed in this instance by the SIAM provider.

Unique logins for the portal are emailed directly to the key account holders on commencement of the maintenance contract. Additional logins are available on request. The portal is encrypted with SSL certificates for data protection and authentication.

1.1.3 Service Management

Daisy will provide a named Service Manager who will act as a key point of contact in relation to the Services. The Service Manager will work collaboratively with the SIAM

provider, the Insolvency Services, and any Daisy nominated Third Parties, to establish high levels of engagement, remaining strongly focused on delivery of the Service, and to continually enhance the experience for Insolvency Services.

The key accountabilities of the Service Manager, in line with the Governance Schedule set out in section Governance Schedule are as follows:

1.1.4 Relationship Management

- **Establish and maintain key relationships between Daisy, the SIAM provider and Insolvency Services;**
- **Operate as the Customer advocate within Daisy, whilst protecting Daisy's interests in the relationship; and**
- **Facilitate meetings between Daisy's, the SIAM provider and as needed the Insolvency Services as required.**

1.1.5 Operational Management

- **Maintain the Operations Manual, ensuring that all required processes, workflows, contacts etc. are reviewed on a regular basis;**
- **Manage the resolution of escalated issues, engaging the appropriate resource to perform technical root cause analysis and reporting to the SIAM provider as agreed and necessary and completing follow up actions to avoid repeat issues;**
- **Engage with Daisy's technical operations teams in relation to any Planned Service Outages or planned maintenance as required to facilitate scheduling and impact assessment; and**
- **Define, manage and deliver Lifecycle Management in line with the lifecycle governance.**

1.1.6 Reporting and Review Meetings

- **Organise, manage and run review meetings with the SIAM provider and the Insolvency Services as needed.**
- **Provide Service performance reporting, including Service Level reporting, trend analysis and active identification of service improvement opportunities;**
- **Within reason, provide ad hoc reports when required by the SIAM provider ; and**
- **Where appropriate suggest improvements and additional possible Service Level measurement approaches which improve and add value to Insolvency Services and/or the services.**

1.1.7 Customer Satisfaction

- **Take ownership for acting on feedback received from SIAM provider,**

1.1.8 Governance Schedule

Daisy will implement an account governance structure for Insolvency Services working with the SIAM provider. The frequency of meetings and elements of that governance structure are described in the table below

	Standard
Meeting Frequency	
Service Review Meeting / Quarterly Account Performance review	Monthly
Strategic Review Meeting	Annually
CAB meeting – Mandatory attendance.	Weekly
Problem Meeting – attendance as required	Weekly
SIAM Meeting	Monthly x 2
Service Elements	
Service Reporting	Monthly
Lifecycle Management	Yes
Continual Service Improvement	Yes
Service Improvement Plan	As required
Service Operations Manual	Yes
Escalation Management	Inclusive

1.1.9 Service Management Meetings

Meeting	Daisy Attendees	SIAM Provider Attendees	Objectives
Service Review	Service Manager Account Manager – DCS Account Manager - Wisdom	Service Manager / Operations Manager	<ul style="list-style-type: none"> • Business update from Daisy • Business update from the SIAM provider • Performance review • Action Log (SIP) review

Meeting	Daisy Attendees	SIAM Provider Attendees	Objectives
			<ul style="list-style-type: none"> • Lifecycle Management • AOB

Daisy's Field Based Service Management will be able to conduct customer meetings via phone as a minimum –utilising collaboration tools such as Microsoft Teams where possible and appropriate to participate in video calls and share presentations –or face to face in either Daisy's or the Customer's premises as required and agreed.

1.1.10 Service Levels

Underpinning the Services are Service Levels, which are measured and reported against as part of the quarterly reports provided by the Daisy Service Manager. The Service Levels are designed to allow measurement in terms of how the Service Provider (Daisy) are performing against the expectations from Insolvency Services. It is imperative that the Service levels agreed are measurable, achievable and are relevant to the Insolvency Services Business. Daisy has included suggested Service Levels.

The Daisy Service Manager will be responsible for the Services delivered to Insolvency Services in line with the agreed SLA's.

The commercials for the service are based on the standard SLA's below.

1.1.10.1 Incident Response

"Incident Response Time" is that time taken for Daisy to pick up an Incident via alerting or phone call from the Customer, raise an Incident ticket and begin triage of the Incident.

Priority Level		Examples	Response Times	Resolution Times	Support Hours	KPI
1	Critical	<p>Significant revenue, operational or safety impact on the Customer.</p> <p>A total loss of Service affecting a single Customer Premises or multiple departments or business functions of the Customer.</p> <p>A Service is significantly degraded affecting the entire</p>	15 minutes*	Within 4 hours	24x7	90%

		Customer organisation.				
2	High	A total loss of a Service affecting a single department or business function of the Customer. A Service is degraded or impacted affecting multiple departments or a single Customer Premises.	Within 4 Support hours	Within 8 support hours	Mon-Fri 09:00-17:30 (excl. Public Holidays)	90%
3	Normal	A Service is degraded or impacted affecting a single department or business function of the Customer. A Service is degraded or a total loss of Service for an individual End User.	Within 8 support hours	Within 16 support hours	Mon-Fri 09:00-17:30 (excl. Public Holidays)	90%
4	Minor	Any incident not classified as a P3 or above.	Within 24 support hours	Within 40 support hours	Mon-Fri 09:00-17:30 (excl. Public Holidays)	90%

Note: *P1 Incidents must be raised by telephone into the service desk for the 15 minutes response SLA to apply.

Whilst Daisy will work towards and report on resolution times, due to the complexities of the software no resolution guarantees can be given, and no financial penalties can be applied for failure to meet them.

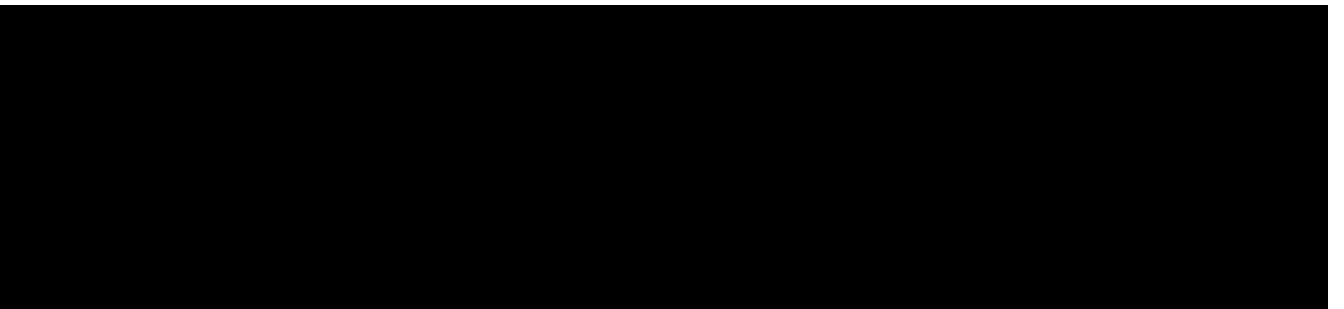
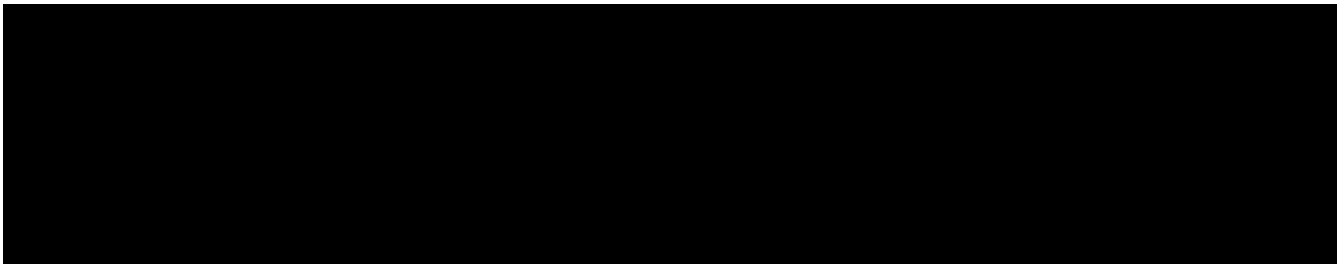
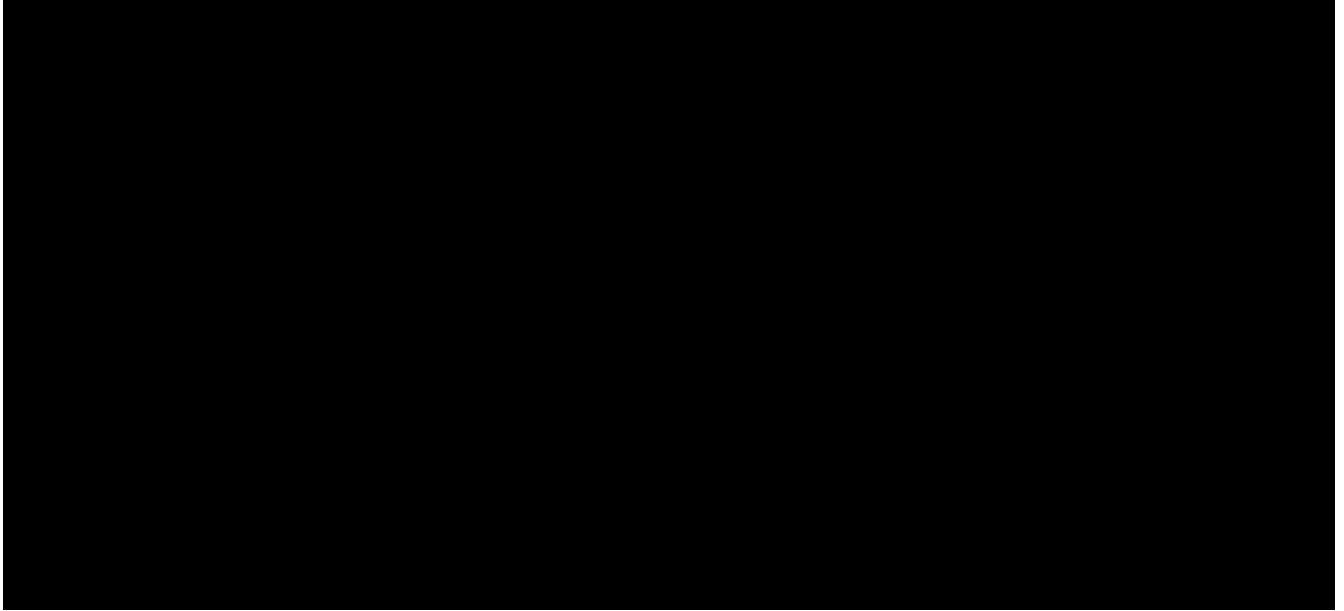
1.1.11 In-Scope

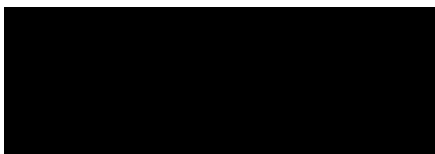
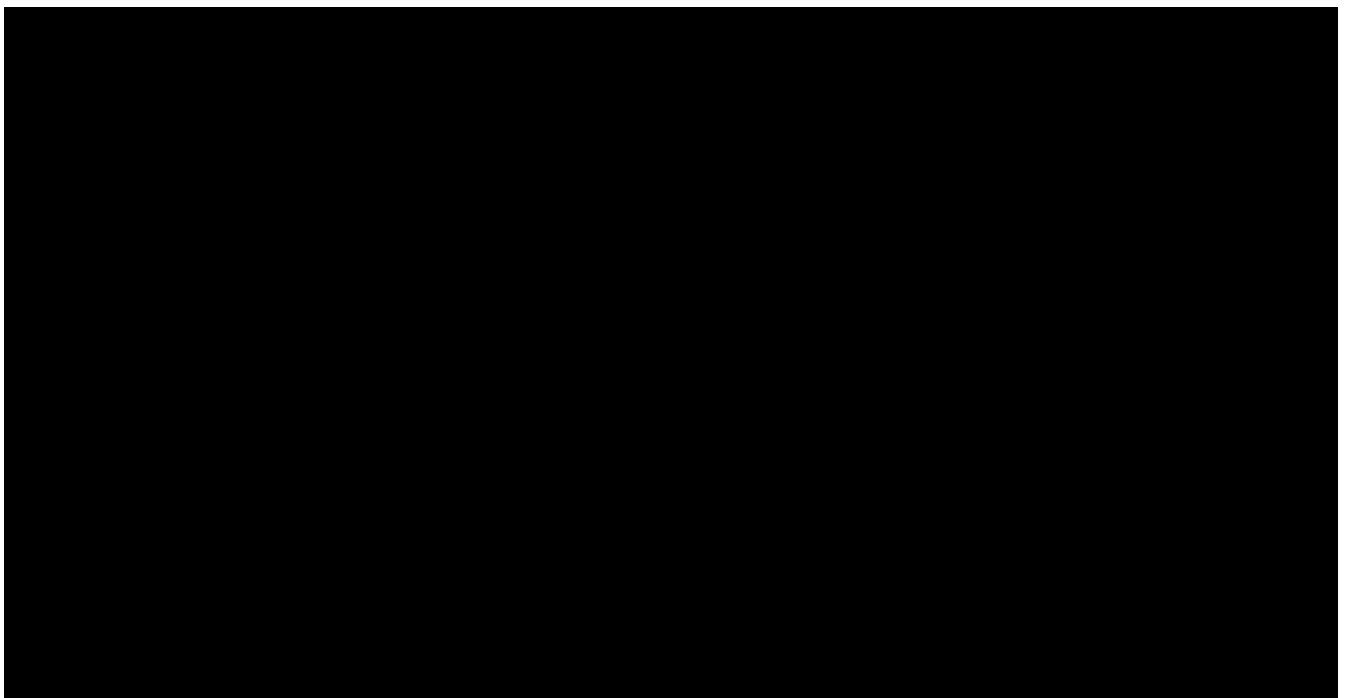
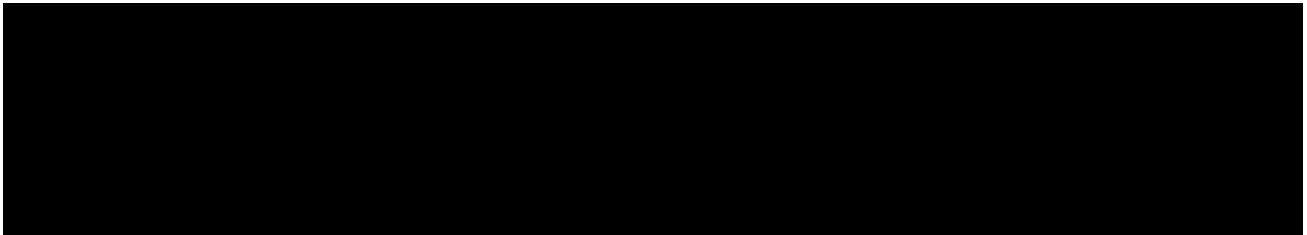
Daisy is responsible for the SQL server and its function, Insolvency Services is responsible for their data content and its usage.

All database changes will be applied to the test database environment for Insolvency Services testing & sign-off prior to implementing the change on the Production database. A single change release is defined as the application of one set of changes to both database environments. Database change releases will be delivered in the form of a Daisy Customer Change Request.

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace pricing document) can't be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:





Customer Benefits

For each Call-Off Contract please complete a customer benefits record, by following this link;

[G-Cloud 12 Customer Benefits Record](#)

Part B: Terms and conditions

1. Call-Off Contract Start date and length

- 1.1 The Supplier must start providing the Services on the date specified in the Order Form.
- 1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.
- 1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.
- 1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

2. Incorporation of terms

- 2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 4.1 (Warranties and representations)
- 4.2 to 4.7 (Liability)
- 4.11 to 4.12 (IR35)
- 5.4 to 5.5 (Force majeure)
- 5.8 (Continuing rights)
- 5.9 to 5.11 (Change of control)
- 5.12 (Fraud)
- 5.13 (Notice of fraud)
- 7.1 to 7.2 (Transparency)
- 8.3 (Order of precedence)
- 8.6 (Relationship)
- 8.9 to 8.11 (Entire agreement)
- 8.12 (Law and jurisdiction)
- 8.13 to 8.14 (Legislative change)
- 8.15 to 8.19 (Bribery and corruption)
- 8.20 to 8.29 (Freedom of Information Act)
- 8.30 to 8.31 (Promoting tax compliance)
- 8.32 to 8.33 (Official Secrets Act)
- 8.34 to 8.37 (Transfer and subcontracting)
- 8.40 to 8.43 (Complaints handling and resolution)
- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.51 to 8.53 (Publicity and branding)
- 8.54 to 8.56 (Equality and diversity)
- 8.59 to 8.60 (Data protection)

- 8.64 to 8.65 (Severability)
- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

- 2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'
- 2.2.2 a reference to 'CCS' will be a reference to 'the Buyer'
- 2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

4. Supplier staff

4.1 The Supplier Staff must:

4.1.1 be appropriately experienced, qualified and trained to supply the Services

4.1.2 apply all due skill, care and diligence in faithfully performing those duties

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer

4.1.4 respond to any enquiries about the Services as soon as reasonably possible

4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on its own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.

- 6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.
- 6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.
- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

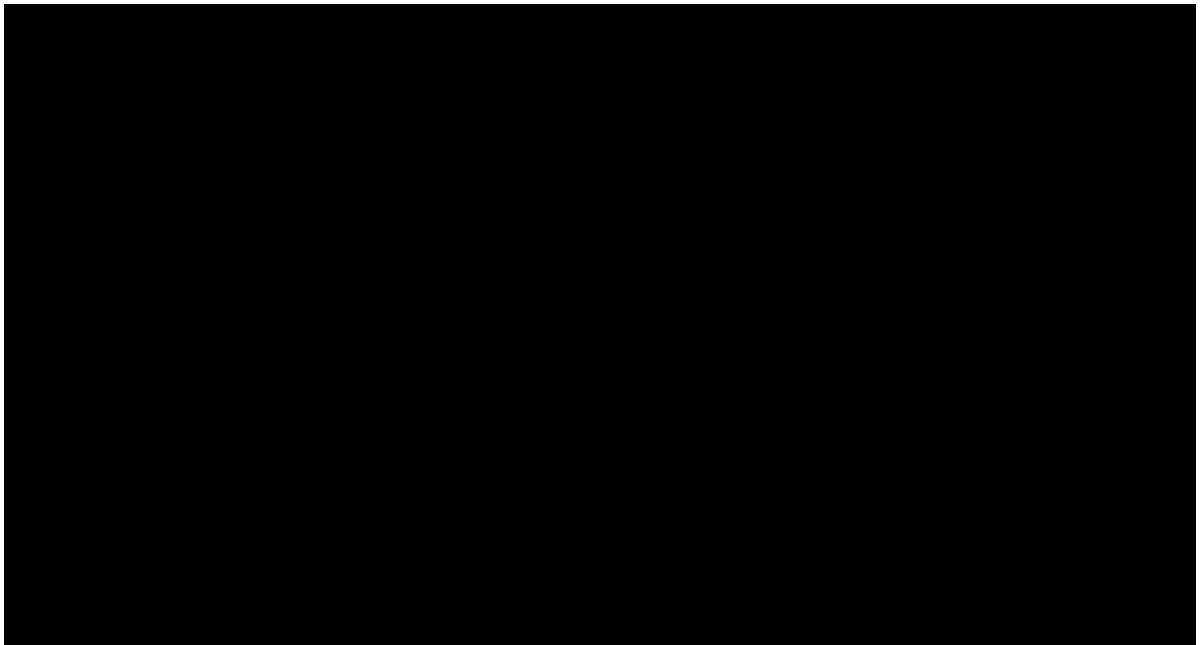
8. Recovery of sums due and right of set-off

- 8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

- 9.2 The Supplier will ensure that:



- 9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

- 9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

- 9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

- 9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
- 9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances
- 9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance
- 9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
- 9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.
- 9.8 The Supplier will be liable for the payment of any:
 - 9.8.1 premiums, which it will pay promptly
 - 9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

- 10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

11. Intellectual Property Rights

- 11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its Licensors.
- 11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.
- 11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.
- 11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.

11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

11.5.1 rights granted to the Buyer under this Call-Off Contract

11.5.2 Supplier's performance of the Services

11.5.3 use by the Buyer of the Services

11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

11.6.1 modify the relevant part of the Services without reducing its functionality or performance

11.6.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer

11.6.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.7 Clause 11.5 will not apply if the IPR Claim is from:

11.7.2 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract

11.7.3 other material provided by the Buyer necessary for the Services

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

- 12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:
 - 12.2.1 providing the Buyer with full details of the complaint or request
 - 12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions
 - 12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)
 - 12.2.4 providing the Buyer with any information requested by the Data Subject
- 12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

- 13.1 The Supplier must not remove any proprietary notices in the Buyer Data.
- 13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.
- 13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.
- 13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.
- 13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.
- 13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:
 - 13.6.1 the principles in the Security Policy Framework:
<https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy:
<https://www.gov.uk/government/publications/government-security-classifications>
 - 13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management:
<https://www.cpni.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets:
<https://www.cpni.gov.uk/protection-sensitive-information-and-assets>

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance:

<https://www.ncsc.gov.uk/collection/risk-management-collection>

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint:

<https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance:

<https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

13.6.6 buyer requirements in respect of AI ethical standards.

13.7 The Buyer will specify any security requirements for this project in the Order Form.

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at:

<https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

- 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

- 15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.
- 15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
- 16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
- 16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control
- 16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.

- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:
<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

- 17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:
- 17.1.1 an executed Guarantee in the form at Schedule 5
- 17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

- 18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.
- 18.2 The Parties agree that the:
- 18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
- 18.2.2 Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses
- 18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.
- 18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:
- 18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied
- 18.4.2 any fraud
- 18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

18.5.2 an Insolvency Event of the other Party happens

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date (whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability)

- 8.44 to 8.50 (Conflicts of interest and ethical walls)
- 8.89 to 8.90 (Waiver and cumulative remedies)

19.4.4 any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

19.5.5 work with the Buyer on any ongoing work

19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

- 20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:
- 21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
- 21.6.2 there will be no adverse impact on service continuity
- 21.6.3 there is no vendor lock-in to the Supplier's Service at exit
- 21.6.4 it enables the Buyer to meet its obligations under the Technology Code Of Practice
- 21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
- 21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

- 21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
- 21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
- 21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
- 21.8.4 the testing and assurance strategy for exported Buyer Data
- 21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations
- 21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

- 22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:
 - 22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control
 - 22.1.2 other information reasonably requested by the Buyer
- 22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.
- 22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

- 23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

24.1.1 Property: for all Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form

24.1.2 Buyer Data: for all Defaults by the Supplier resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data, will not exceed the amount in the Order Form

24.1.3 Other Defaults: for all other Defaults by either party, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

- 29.2.1 the activities they perform
- 29.2.2 age
- 29.2.3 start date
- 29.2.4 place of work
- 29.2.5 notice period
- 29.2.6 redundancy payment entitlement
- 29.2.7 salary, benefits and pension entitlements

- 29.2.8 employment status
- 29.2.9 identity of employer
- 29.2.10 working arrangements
- 29.2.11 outstanding liabilities
- 29.2.12 sickness absence
- 29.2.13 copies of all relevant employment contracts and related documents
- 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

- 29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.
- 29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.
- 29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.
- 29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
 - 29.6.1 its failure to comply with the provisions of this clause
 - 29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer
- 29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
- 29.8 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

- 30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.
- 30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

- 31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.
- 31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:
 - 31.2.1 work proactively and in good faith with each of the Buyer's contractors
 - 31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

- 32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.
- 32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.
- 32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

- 33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with clauses 8.59 and 8.60 are reproduced in this Call-Off Contract document at schedule 7.

Schedule 3: Collaboration agreement

Not Applicable

Schedule 4: Alternative clauses

Not Applicable

Schedule 5: Guarantee

Not Applicable

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
Audit	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).
Background IPRs	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes created by the Party independently of this Call-Off Contract, or <p>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.</p>
Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.

Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
Controller	Takes the meaning given in the GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy (iii) all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
Data Subject	Takes the meaning given in the GDPR
Default	<p>Default is any:</p> <ul style="list-style-type: none"> • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
Deliverable(s)	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.
Digital Marketplace	The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
End	Means to terminate; and Ended and Ending are construed accordingly.

Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-for-tax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.
Force Majeure	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> • acts, events or omissions beyond the reasonable control of the affected Party • riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare • acts of government, local government or Regulatory Bodies • fire, flood or disaster and any failure or shortage of power or fuel • industrial dispute affecting a third party for which a substitute third party isn't reasonably available <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> • any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain • any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure • the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into • any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also

	includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.12 together with the Framework Schedules.
Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.

Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.
Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.
Insolvency event	<p>Can be:</p> <ul style="list-style-type: none"> • a voluntary arrangement • a winding-up petition • the appointment of a receiver or administrator • an unresolved statutory demand • a Schedule A1 moratorium
Intellectual Property Rights or IPR	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> • copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information • applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction • all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> • the supplier's own limited company • a service or a personal service company • a partnership <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>

IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
LED	Law Enforcement Directive (EU) 2016/680.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' Losses ' will be interpreted accordingly.
Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.

Management Information	The management information specified in Framework Agreement section 6 (What you report to CCS).
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.
New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: "Fair Deal for staff pensions: staff transfer from central government" issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and 'Parties' will be interpreted accordingly.
Personal Data	Takes the meaning given in the GDPR.
Personal Data Breach	Takes the meaning given in the GDPR.
Processing	Takes the meaning given in the GDPR.
Processor	Takes the meaning given in the GDPR.

Prohibited act	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> • induce that person to perform improperly a relevant function or activity • reward that person for improper performance of a relevant function or activity • commit any offence: <ul style="list-style-type: none"> ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud
Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
PSN or Public Services Network	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.

Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Digital Marketplace.
Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.

Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier staff	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
Term	The term of this Call-Off Contract as set out in the Order Form.
Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

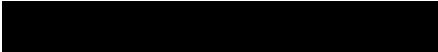
Schedule 7: GDPR Information

This schedule reproduces the annexes to the GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract.

Annex 1: Processing Personal Data

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

1.1 The contact details of the Buyer’s Data Protection Officer are:



1.2 The contact details of the Supplier’s Data Protection Officer are:



1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Descriptions	Details
Identity of Controller for each Category of Personal Data	<p>The Buyer is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with paragraph 2-15 Framework Agreement Schedule 4 (Where the Party is a Controller and the other Party is Processor) and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:</p> <p>Under GDPR Articles. Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</p> <p>In the case of the Insolvency Service, Daisy do not have access to Personal Date of current or past InsS employees, their agents and suppliers, however we hold and have access to data held by companies that had gone into</p>

	<p>insolvency and those employees who worked for those companies. However, a number of details are removed by The Insolvency Service at the point they come into the business such as sickness and disciplinary records of those employed.</p> <p>Below is a list of items that would come under Personal Data with the scope of this agreement:</p> <p>Name Date of Birth Address Bank Details Financial Information such as Loans, Credit Cards, Payment History, Credit Rating etc. Salary Details Gender Nationality NI Number Phone & Mobile Numbers Tax Code & Other Tax History Details Marital Status Work History Medical History Driving Licence Passport Criminal Records & DBS Checks</p>
Duration of the Processing	11/08/2022-10/08/2024 plus any contract extension granted.
Nature and purposes of the Processing	<p>Storage, retrieval and use for the purpose of ticketing, provisioning and account management. GDPR only applies to personal data processed in one of two ways: <input type="checkbox"/> Personal data processed wholly or partly by automated means (or, information in electronic form); and <input type="checkbox"/> Personal data processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (or, written records in a manual filing system).</p> <p>The scope of the contract which will be between the Insolvency Service and Daisy is Personal Data processed wholly by automated means (or, information in electronic form).</p>
Type of Personal Data	<p>Name Date of Birth Address Bank Details Financial Information such as Loans, Credit Cards, Payment History, Credit Rating etc. Salary Details Gender Nationality</p>

	<p>NI Number Phone & Mobile Numbers Tax Code & Other Tax History Details Marital Status Work History Medical History Driving Licence Passport Criminal Records & DBS Checks</p>
Categories of Data Subject	<p>There are numerous Data Subject types within the general population were GDPR would come into force, however if we are being specific to the Insolvency Service and the data that we will be holding and processing this will reduce quite significantly as most Data Subjects will not apply. As we are not holding personal data on InsS staff as we are not managing HR, Financial and Supplier Databases and Business Functions these will not be applicable.</p> <p>The data we hold would be the Data Subjects of the businesses that have fallen into insolvency and liquidation and the data they hold, however some of this may have been removed by InsS at the time the case has come into the organisation, and these would include:</p> <p>All Staff (Full Time, Part Time, Temporary/Agency Staff, Potentially Volunteers, including staff that have left and Retired including Directors)</p> <p>Customers including Patients (including lapsed customers)</p> <p>Suppliers and Contractors (including lapsed suppliers)</p> <p>Governmental Departments (such as HMRC, HSE, FSA, Local Authority etc.)</p> <p>Banking and Financial Providers including Consultants and Advisors</p> <p>Users of the Company Websites</p>
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	<p>Most Financial Data has a recommended Retention Period of Current Year plus 6 Years before destruction, however as the Insolvency Service may be holding data where Legal Action may still be on-going with the cases it manages this may be much longer, so suggest that a Case Review of Data is undertaken, to understand those cases that are closed and no further action will be taken can be destroyed if they pass that 6 + 1 year threshold.</p> <p>All electronic data held will be destroyed and deleted from our servers and those servers/hard drives are then decommissioned and securely destroyed.</p>

	<p>We use Blancco whose software is certified by the National Cyber Security Centre (NCSC), the UK Government's National Technical Authority for Information Assurance. The Blancco product meets the highest security specifications detailed in the HMG InfoSec Standard No: 5. Data Erasure Software.</p> <p>Data can be returned either by a Secure FTP Transfer, once the data has been received and verified as complete by the Insolvency then the above statement will be enacted. Alternatively, we can return the data on Hard Drives, (e.g. Microsoft Databox etc.), back to you.</p>
--	--